Guía para desarrolladores

Amazon CloudFront

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon CloudFront: Guía para desarrolladores

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Amazon CloudFront? ... 1
Cómo configurar CloudFront para entregar contenido ... 2
Elija entre distribución estándar o distribución de varios inquilinos ... 5
Precios ... 5
Formas de utilizar CloudFront ... 6
Acelerar la entrega de contenidos de sitios web estáticos ... 6
Distribuir vídeo bajo demanda o en streaming ... 6
Cifrar campos específicos a través del procesamiento del sistema ... 7
Personalizar en el borde ... 7
Distribuir contenido privado mediante personalizaciones de Lambda@Edge ... 7
Cómo CloudFront entrega el contenido ... 8
Cómo CloudFront entrega contenido a sus usuarios ... 9
Cómo funciona CloudFront con las cachés de borde regionales ... 10
Servidores periféricos de CloudFront ... 12
Utilizar la lista de prefijos administrados de CloudFront ... 13
Cómo utilizar los AWS SDK ... 14
Recursos técnicos de CloudFront ... 15
Introducción ... 16
Configuración de su Cuenta de AWS ... 16
Cómo crear una Cuenta de AWS ... 16
Creación de un usuario con acceso administrativo ... 17
Elección de cómo acceder a CloudFront ... 18
Introducción a una distribución estándar ... 19
Requisitos previos ... 20
Creación de un bucket ... 20
Carga de contenido ... 21
Creación de una distribución ... 21
Acceso al contenido ... 22
Limpieza ... 23
Mejora de la distribución básica ... 23
Introducción (AWS CLI) ... 24
Requisitos previos ... 24
Crear un bucket de Amazon S3 ... 24
Carga del contenido en el bucket ... 25

Creación de un control de acceso de origen (OAC) ... 25
Creación de una distribución estándar ... 26
Actualización de la política de bucket de S3 ... 27
Confirmación de la implementación de la distribución ... 28
Acceso al contenido a través de CloudFront ... 28
Limpieza ... 29
Introducción a un sitio web seguro estático ... 30
Información general de la solución ... 31
Implementación de la solución ... 32
Planes de precios de tarifa fija de CloudFront ... 38
Beneficios de los planes de precios de tarifa fija de CloudFront ... 39
Características por plan de precios ... 40
Características del plan de precios ... 40
Asignaciones de uso mensuales ... 85
La elegibilidad se basa en el uso histórico ... 86
Costos cubiertos por el plan ... 86
La administración de DNS de Route 53 y su plan ... 87
Reducción de los costos de AWS generales con planes de precios ... 89
Administración de los planes de precios de tarifa fija ... 89
Suscripción de una nueva distribución a un plan de precios ... 89
Suscripción de una distribución existente a un plan de precios ... 90
Actualización de un plan de precios ... 91
Bajada de categoría de un plan de precios ... 91
Cancelación de un plan de precios ... 92
Cancelación de un cambio de plan pendiente ... 92
Eliminación de una distribución con un plan de precios ... 93
Permisos ... 93
Cuotas de planes de precios de tarifa fija ... 93
Características no admitidas ... 94
Características no admitidas ... 94
Asociaciones no compatibles ... 96
Restricciones por cuenta ... 97
Restricciones por recursos ... 97
Características adicionales que pueden afectar al plan de precios ... 97
Planes de precios frente a precios de pago por uso ... 99
Configuración de distribuciones ... 100

Introducción al funcionamiento de las distribuciones de varios inquilinos 102
Funcionamiento 103
Términos 105
Características no admitidas 107
Personalizaciones de inquilinos de distribución 108
Solicitud de certificados (inquilino de distribución) 112
Creación de un grupo de conexiones personalizado (opcional) 119
Migración a una distribución de varios inquilinos 121
Creación de una distribución 122
Creación de una distribución de CloudFront en la consola 124
Valores que se muestran 130
Enlaces adicionales 131
Adición de un dominio a la distribución estándar de CloudFront 131
Configuración de distribución preconfigurada 134
Origen de Amazon S3 134
Origen de API Gateway 135
Origen personalizado e instancia de EC2 137
Origen de Elastic Load Balancing 138
Origen de MediaPackage v1 140
Origen de MediaPackage v2 141
Origen de MediaTailor 143
Toda la configuración de distribución 144
Configuración de origen 144
Configuración del comportamiento de la caché 156
Ajustes de la distribución 172
Páginas de error personalizadas y almacenamiento de errores en caché 182
Restricciones geográficas 183
Prueba de una distribución 183
Creación de enlaces a sus objetos 184
Actualizar una distribución 185
Actualización de una distribución en la consola 185
Etiquetado de una distribución 188
Restricciones de las etiquetas 189
Adición, edición y eliminación de etiquetas para distribuciones 189
Etiquetado programático 190
Eliminar una distribución 190

Uso de varios orígenes ... 193
Uso de un bucket de Amazon S3 ... 194
Uso de un contenedor de MediaStore o un canal de MediaPackage ... 206
Uso de un equilibrador de carga de aplicación ... 207
Uso de un equilibrador de carga de red ... 207
Uso de una URL de función de Lambda ... 208
Uso de Amazon EC2 (u otro origen personalizado) ... 209
Uso de los grupos de origen de CloudFront ... 211
Uso de Amazon API Gateway ... 211
Habilitar IPv6 ... 211
Solicitudes de espectadores de IPv6 ... 212
Solicitudes de origen de IPv6 ... 213
Uso de la implementación continua para probar de forma segura los cambios ... 213
Flujo de trabajo de implementación continua de CloudFront ... 216
Trabajo con una distribución provisional y una política de implementación continua ... 217
Supervisión de una distribución provisional ... 228
Información sobre cómo funciona la implementación continua ... 228
Cuotas y otras consideraciones de la implementación continua ... 230
Uso de URL personalizadas ... 232
Requisitos para el uso de nombres de dominio alternativos ... 232
Restricciones de uso de nombres de dominio alternativos ... 234
Adición de un nombre de dominio alternativo ... 237
Desplazamiento de un nombre de dominio alternativo ... 240
Eliminación de un nombre de dominio alternativo ... 254
Uso de comodines en nombres de dominio alternativos ... 255
Uso de WebSockets ... 256
Cómo funciona el protocolo WebSocket ... 256
Requisitos de WebSocket ... 257
Encabezados de WebSocket recomendados ... 257
Solicitud de direcciones IP estáticas de anycast para utilizarlas en las listas de permitidos ... 258
Requisitos previos ... 258
Solicitud de una lista de direcciones IP estáticas de anycast ... 259
Creación de una lista de direcciones IP estáticas de anycast ... 259
Asociación de una lista de direcciones IP estáticas de anycast a una distribución existente ... 260
Asociación de una lista de direcciones IP estáticas de anycast a una nueva distribución ... 261

Asociación de una lista de direcciones IP estáticas de anycast a un grupo de conexión 261
Actualización de una lista de direcciones IP estáticas de Anycast 262
Incorporación de su propia IP a CloudFront mediante IPAM 263
Uso de gRPC 267
Cómo funciona gRPC en CloudFront 267
Trabajo con recursos compartidos en CloudFront 270
Requisitos previos para compartir recursos 270
Uso compartido de un origen de la VPC 271
Uso de un origen de VPC compartido 274
Identificación de un origen de la VPC compartido 275
Desactivación de un origen de la VPC compartido 275
Responsabilidades y permisos de orígenes de la VPC compartidos 276
Permisos de los propietarios 276
Permisos de los consumidores 276
AWSRAMDefaultPermissionCloudFront 276
Facturación y medición 277
Cuotas de recursos compartidos 277
Almacenamiento en caché y disponibilidad 278
Mejora de la tasa de aciertos de caché 279
Especificación de cuánto tiempo CloudFront almacena en caché los objetos 279
Uso del escudo de origen 279
Almacenamiento en caché en función de parámetros de cadenas de consulta 280
Almacenamiento en caché en función de valores de cookies 280
Almacenamiento en caché en función de encabezados de solicitud 282
Eliminación del encabezado `Accept-Encoding` cuando no sea necesario comprimir 283
Distribución de contenido multimedia a través de HTTP 283
Uso del escudo de origen 283
Casos de uso para el escudo de origen 285
Elección de la región de AWS para Origin Shield 290
Habilitar Origin Shield 292
Estimación de los costos de Origin Shield 294
Alta disponibilidad del escudo de origen 295
Cómo interactúa Origin Shield con otras características de CloudFront 296
Aumento de alta disponibilidad con conmutación por error 297
Creación de un grupo de origen 299
Control de tiempos de espera e intentos de origen 300

Utilizar la conmutación por error de origen con funciones de Lambda@Edge 301
Utilizar páginas de error personalizadas con conmutación por error de origen 302
Administración de vencimiento de caché 303
Uso de encabezados para controlar la duración del almacenamiento en caché de objetos individuales 304
Distribución de contenido obsoleto (caducado) 306
Especificación de cuánto tiempo CloudFront almacena objetos en caché 309
Agregación de encabezados a los objetos con la consola de Amazon S3 316
Almacenamiento en caché y parámetros de cadenas de consulta 316
Configuración de la consola y de la API para el reenvío de cadenas de consulta y almacenamiento en caché 319
Optimización del almacenamiento en caché 319
Parámetros de cadena de consulta y registros estándar de CloudFront (registros de acceso) 321
Almacenamiento en caché de contenido en función de cookies 321
Almacenamiento en caché de contenido en función de encabezados de solicitud 325
Encabezados y distribuciones: información general 325
Selección de los encabezados para basar el almacenamiento en caché 327
Configuración de CloudFront para que respete la configuración de CORS 328
Configuración del almacenamiento en caché en función del tipo de dispositivo 329
Configuración del almacenamiento en caché en función del idioma del lector 329
Configuración del almacenamiento en caché en función de la ubicación del lector 329
Configuración del almacenamiento en caché en función del protocolo de la solicitud 330
Configuración del almacenamiento en caché para archivos comprimidos 330
Cómo afecta al rendimiento el almacenamiento en caché en función de los encabezados ... 330
Cómo afectan al almacenamiento en caché las mayúsculas o minúsculas de los encabezados y sus valores 330
Encabezados que CloudFront devuelve al lector 331
Control de la clave de caché con una política 332
Descripción de las políticas de caché 333
Información de políticas 333
Configuración del tiempo de vida (TTL) 333
Configuración de la clave de caché 334
Creación de políticas de caché 341
Uso de políticas de caché administradas 345
Amplify 346

CachingDisabled ... 348
CachingOptimized ... 348
CachingOptimizedForUncompressedObjects ... 349
Elemental-MediaPackage ... 350
UseOriginCacheControlHeaders ... 351
UseOriginCacheControlHeaders-QueryStrings ... 352
Descripción de la clave de caché ... 353
Clave de caché predeterminada ... 353
Personalización de la clave de caché ... 355
Control de las solicitudes de origen con una política ... 357
Descripción de políticas de solicitud de origen ... 358
Información de políticas ... 358
Configuración de solicitud de origen ... 358
Creación de políticas de solicitud de origen ... 361
Uso de políticas de solicitudes de origen administradas ... 366
AllViewer ... 366
AllViewerAndCloudFrontHeaders-2022-06 ... 367
AllViewerExceptHostHeader ... 368
CORS-CustomOrigin ... 369
CORS-S3Origin ... 369
Elemental-MediaTailor-PersonalizedManifests ... 370
HostHeaderOnly ... 370
UserAgentRefererHeaders ... 371
Añadido de encabezados de solicitudes de CloudFront ... 371
Encabezados de tipo de dispositivo ... 372
Encabezados de ubicación del espectador ... 373
Encabezados para determinar la estructura de los encabezados del espectador ... 374
Encabezados relacionados con TLS ... 375
Otros encabezados de CloudFront ... 376
Descripción de cómo funcionan juntas las políticas de solicitud de origen y las políticas de caché ... 377
Añadido o eliminación de encabezados de respuestas con una política ... 382
Descripción de las políticas de encabezados de respuesta ... 383
Detalles de la política (metadatos) ... 384
Encabezados de CORS ... 384
Encabezados de seguridad ... 388

Encabezados personalizados ... 390
Eliminar encabezados ... 391
Encabezado Server-Timing ... 393
Creación de políticas de encabezados de respuesta ... 398
Uso de las políticas de encabezados de respuesta administradas ... 405
CORS-and-SecurityHeadersPolicy ... 406
CORS-With-Preflight ... 407
CORS-with-preflight-and-SecurityHeadersPolicy ... 407
SecurityHeadersPolicy ... 408
SimpleCORS ... 409
Comportamiento de solicitudes y respuestas ... 411
Cómo procesa CloudFront las solicitudes HTTP y HTTPS ... 411
Comportamiento de solicitudes y respuestas para orígenes de Amazon S3 ... 412
Cómo CloudFront procesa y reenvía solicitudes a su origen de Amazon S3 ... 412
Cómo procesa CloudFront las respuestas de su origen de Amazon S3 ... 419
Comportamiento de solicitudes y respuestas para orígenes personalizados ... 422
Cómo procesa y reenvía CloudFront solicitudes a su origen personalizado ... 422
Cómo procesa CloudFront las respuestas de su origen personalizado ... 442
Comportamiento de solicitudes y respuestas para grupos de origen ... 446
Añadido de encabezados personalizados a solicitudes de origen ... 447
Casos de uso ... 448
Configuración de CloudFront para agregar encabezados personalizados a solicitudes de origen ... 449
Encabezados personalizados que CloudFront no puede agregar a solicitudes de origen ... 449
Configuración de CloudFront para reenviar el encabezado de `Authorization` ... 450
Procesamiento de CloudFront de Range GET ... 451
Uso de solicitudes de rango para almacenar en caché objetos grandes ... 452
Cómo CloudFront procesa los códigos de estado HTTP 3xx desde el origen ... 453
Procesamiento de CloudFront de los códigos de estado HTTP 4xx y 5xx desde el origen ... 454
Cómo CloudFront procesa los errores cuando las páginas de error personalizadas están configuradas ... 455
Cómo CloudFront procesa los errores si no ha configurado las páginas de error personalizadas ... 458
Códigos de estado HTTP 4xx y 5xx que CloudFront almacena en caché ... 460
Generación de respuestas de error personalizadas ... 462
Configuración del comportamiento de respuestas de error ... 462

Creación de una página de error personalizada para códigos de estado HTTP específicos . 464
Almacenamiento de objetos y páginas de error personalizadas en diferentes lugares 466
Cambio de códigos de respuesta devueltos por CloudFront 467
Control de cuánto tiempo CloudFront almacena los errores en caché 468
Agregación, eliminación o sustitución de contenido 471
Agregación de contenido y acceso al mismo 471
Uso del control de versiones de archivos para actualizar o eliminar el contenido existente 472
Actualización de archivos existentes con versiones de nombres de archivos 472
Eliminación de contenido para que CloudFront no lo distribuya 473
Personalización de URL de archivo 473
Uso de su propio nombre de dominio (example.com) 474
Uso de un delimitador final (/) en las URL 474
Creación de URL firmadas para contenido restringido 475
Especificación de un objeto raíz predeterminado 475
Cómo especificar un objeto raíz predeterminado 475
Cómo funciona el objeto raíz predeterminado 477
Cómo funciona CloudFront si no define un objeto raíz 479
Invalidación de archivos para eliminar el contenido 479
Elección entre invalidar archivos y utilizar nombres de archivo con versiones 480
Determinación de qué archivos invalidar 481
Qué se debe saber al invalidar archivos 481
Invalidación de archivos 485
Máximo de solicitud de invalidación simultánea 489
Cargos por invalidación de archivo 489
Ofrecimiento de archivos comprimidos 490
Configuración de CloudFront para comprimir objetos 490
Cómo funciona la compresión de CloudFront 491
Condiciones para la compresión 492
Tipos de archivos que CloudFront comprime 494
`ETag`Conversión de encabezado 496
Uso de protecciones de AWS WAF 498
Habilitación de AWS WAF para distribuciones 499
Habilitación de AWS WAF para una nueva distribución 499
Utilizar una ACL web existente 500
Habilitación del control de bots 501
Configuración de la protección por categoría de bots 502

Administración de las protecciones de seguridad de AWS WAF para CloudFront 503
Requisitos previos 504
Habilitación de registros de AWS WAF 504
Configuración del límite de velocidad 505
Habilitación de protecciones de seguridad de AWS WAF 506
Configuración de acceso seguro y restricción de acceso a contenido 508
Uso de HTTPS con CloudFront 509
Exigencia de HTTPS entre lectores y CloudFront 510
Exigencia de HTTPS en un origen personalizado 513
Exigencia de HTTPS en un origen de Amazon S3 516
Protocolos y cifrados admitidos entre lectores y CloudFront 518
Protocolos y cifrados admitidos entre CloudFront y el origen 527
Uso de nombres de dominio alternativos y HTTPS 529
Elección de la forma en que CloudFront atiende las solicitudes HTTPS 530
Requisitos para la utilización de certificados SSL/TLS con CloudFront 533
Cuotas al usar certificados SSL/TLS con CloudFront (solo HTTPS entre lectores y CloudFront) 538
Configuración de nombres de dominio alternativos y HTTPS 540
Determinación del tamaño de la clave pública en un certificado SSL/TLS RSA 544
Aumento de las cuotas de certificados SSL/TLS 545
Rotación de certificados SSL/TLS 546
Reversión de un certificado SSL/TLS personalizado al certificado de CloudFront predeterminado 547
Cambio de un certificado SSL/TLS personalizado con direcciones IP dedicadas a SNI 549
Autenticación TLS mutua con CloudFront (mTLS de espectador) 550
Funcionamiento 550
Casos de uso 550
Almacenes de confianza y administración de certificados 551
Habilitación de TLS mutua para las distribuciones de CloudFront 558
Asociación de una función de conexión de CloudFront 562
Configuración adicional 568
Encabezados de mTLS del espectador para las políticas de caché y reenvío al origen 571
Revocación mediante la función de conexión de CloudFront y KVS 575
Observabilidad mediante registros de conexión 579
TLS mutua (origen) con CloudFront 584
mTLS de espectador frente a mTLS de origen 584

Funcionamiento ... 585
Casos de uso ... 585
Importante: requisitos del servidor de origen ... 586
Introducción ... 586
Administración de certificados con AWS Certificate Manager ... 587
Habilitación de TLS mutua (origen) para las distribuciones de CloudFront ... 591
Uso de CloudFront Functions con TLS mutua (origen) ... 594
Restricción de contenido con URL firmadas y cookies firmadas ... 597
Distribución de contenido privado ... 597
Restricción del acceso a archivos ... 598
Especificación de firmantes de confianza ... 601
Decisión de utilizar URL firmadas o cookies firmadas ... 611
Uso de URL firmadas ... 612
Uso de cookies firmadas ... 635
Comandos de Linux y OpenSSL para codificación y cifrado base64 ... 664
Ejemplos de código para URL firmadas ... 664
Restricción del acceso a un origen de AWS ... 694
Restricción del acceso a un origen de AWS Elemental MediaPackage v2 ... 694
Restricción del acceso a un origen de AWS Elemental MediaStore ... 702
Restricción del acceso a un origen de URL de función de AWS Lambda ... 710
Restricción del acceso a un origen de Amazon S3 ... 721
Restricción del acceso con orígenes de la VPC ... 737
Restricción del acceso a Application Load Balancer ... 745
Configuración de CloudFront para agregar un encabezado HTTP personalizado a solicitudes ... 746
Configuración de un equilibrador de carga de aplicaciones para que solo reenvíe solicitudes que contengan un encabezado específico ... 748
(Opcional) Mejore la seguridad de esta solución ... 749
(Opcional) Limitación del acceso al origen mediante la lista de prefijos administrados por AWS para CloudFront ... 751
Restricción geográfica ... 751
Uso de restricciones geográficas de CloudFront ... 752
Uso de un servicio de geolocalización de terceros ... 754
Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial ... 756
Información general del cifrado en el nivel de campo ... 758
Configuración del cifrado en el nivel de campo ... 758

Descifrado de campos de datos en el origen ... 764
Vídeo bajo demanda y en streaming en directo ... 768
Acerca del streaming de vídeo ... 768
Distribución de vídeo bajo demanda ... 769
Configuración de vídeo bajo demanda para Microsoft Smooth Streaming ... 770
Distribución de video en streaming ... 772
Distribución de vídeo utilizando AWS Elemental MediaStore como origen ... 773
Distribución de vídeo en directo formateado con AWS Elemental MediaPackage ... 774
Distribución de contenido de video bajo demanda con AWS Elemental MediaPackage ... 780
Resiliencia basada en la calidad multimedia ... 786
Campos de registro de MQAR ... 789
Uso de funciones para personalizar en la periferia ... 790
Diferencias entre CloudFront Functions y Lambda@Edge ... 791
Personalización con CloudFront Functions ... 793
Tutorial: creación de una función simple de CloudFront ... 794
Tutorial: creación de una función de CloudFront que incluya pares clave-valor ... 797
Escritura de código de función ... 800
Creación de funciones ... 901
Prueba de funciones ... 904
Actualización de funciones ... 909
Publicación de funciones ... 912
Asociación de funciones con distribuciones ... 913
CloudFront KeyValueStore ... 917
Personalización con funciones de conexión de CloudFront ... 939
Información general y flujo de trabajo ... 940
Configuración y límites ... 942
Creación de funciones de conexión de CloudFront para la validación de TLS mutua (espectador) ... 943
Escritura de código de función de conexión de CloudFront para la validación de TLS mutua (espectador) ... 947
Prueba de las funciones de conexión de CloudFront antes de la implementación ... 956
Asociación de funciones de conexión con distribuciones ... 958
Implementación de la revocación de certificados para TLS mutua (espectador) con CloudFront Functions y KeyValueStore ... 959
Personalización con Lambda@Edge ... 966
Cómo funciona Lambda@Edge con las solicitudes y las respuestas ... 967

Formas de utilizar Lambda@Edge ... 968
Introducción a Lambda@Edge ... 969
Configuración de permisos y roles de IAM ... 977
Escritura y creación de una función de Lambda@Edge ... 984
Adición de desencadenadores para una función de Lambda@Edge ... 989
Prueba y depuración ... 997
Eliminación de funciones y réplicas ... 1005
Estructura de evento ... 1006
Trabajo con solicitudes y respuestas ... 1024
Funciones de ejemplo ... 1030
Restricciones en funciones de borde ... 1069
Restricciones en todas las funciones de borde ... 1070
Restricciones en CloudFront Functions ... 1076
Restricciones de Lambda @Edge ... 1078
Informes, métricas y registros ... 1084
Informes de uso y facturación de AWS para CloudFront ... 1084
Visualización del informe de facturación de AWS para CloudFront ... 1085
Visualización del informe de uso de AWS para CloudFront ... 1086
Interpretación de la factura de AWS y de los informes de uso de CloudFront ... 1088
Visualización de informes de la consola de CloudFront ... 1095
Visualización de informes estadísticos de la caché de CloudFront ... 1095
Visualización de informes de objetos populares de CloudFront ... 1102
Visualización de informes de remitentes principales de CloudFront ... 1108
Visualización de informes de uso de CloudFront ... 1112
Visualización de informes de espectadores de CloudFront ... 1121
Supervisión de métricas de CloudFront con Amazon CloudWatch ... 1133
Visualización de métricas de funciones periféricas y de CloudFront ... 1134
Creación de alarmas ... 1142
Descarga de datos de métricas ... 1143
Métricas de CloudFront ... 1146
Registro de funciones de CloudFront y perimetrales ... 1152
Solicitudes de registro ... 1153
Registro de las funciones perimetrales ... 1154
Registro de la actividad del servicio ... 1154
Registros de acceso (registros estándar) ... 1155
Uso de registros de acceso en tiempo real ... 1204

Registros de funciones perimetrales ... 1227
Registros de AWS CloudTrail ... 1231
Realización de un seguimiento de los cambios en la configuración con AWS Config ... 1245
Configurar AWS Config con CloudFront ... 1245
Consultar historial de configuración de CloudFront ... 1247
Evaluación de las configuraciones de CloudFront con reglas de AWS Config ... 1248
Seguridad ... 1249
Protección de datos ... 1250
Cifrado en tránsito ... 1251
Cifrado en reposo ... 1252
Restricción del acceso a contenido ... 1252
Gestión de identidad y acceso ... 1253
Público ... 1254
Autenticación con identidades ... 1254
Administración del acceso con políticas ... 1256
Cómo funciona Amazon CloudFront con IAM ... 1258
Ejemplos de políticas basadas en identidades ... 1263
Políticas gestionadas por AWS ... 1274
Uso de roles vinculados a servicios ... 1284
Resolución de problemas de identidad y acceso de CloudFront ... 1288
Registro y supervisión ... 1290
Validación de conformidad ... 1292
Prácticas recomendadas de conformidad de CloudFront ... 1293
Resiliencia ... 1294
Conmutación por error de CloudFront ... 1294
Seguridad de la infraestructura ... 1295
Solución de problemas ... 1296
Solucionar problemas de distribuciones ... 1296
CloudFront devuelve un error Access Denied ... 1296
CloudFront devuelve un error InvalidViewerCertificate al intentar agregar un nombre de dominio alternativo ... 1299
CloudFront devuelve un error de registro DNS mal configurado al intentar agregar un nuevo CNAME ... 1300
No puedo ver los archivos de mi distribución ... 1301
Mensaje de error: Certificate: <id-certificado> is being used by CloudFront ... 1303
Solución de problemas de códigos de estado de respuesta a errores ... 1303

Código de estado HTTP 400 (Solicitud errónea) ... 1304
Código de estado HTTP 401 (sin autorización) ... 1305
Código de estado HTTP 403 (método no válido) ... 1306
Código de estado HTTP 403 (permiso denegado) ... 1306
Código de estado HTTP 404 (no encontrado) ... 1309
Código de estado HTTP 412 (condición previa con error) ... 1310
Código de estado HTTP 500 (error de servidor interno) ... 1310
Código de estado HTTP 502 (Puerta de enlace incorrecta) ... 1311
Código de estado HTTP 503 (Servicio no disponible) ... 1316
Código de estado HTTP 504 (Tiempo de espera de puerta de enlace agotado) ... 1318
Pruebas de carga de CloudFront ... 1324
Cuotas ... 1325
Cuotas generales ... 1326
Cuotas generales de distribuciones ... 1327
Cuotas generales de políticas ... 1329
Cuotas en mTLS y almacenes de confianza ... 1331
Cuotas en CloudFront Functions ... 1332
Cuotas en funciones de conexión ... 1332
Cuotas en almacenes de clave-valor ... 1333
Cuotas de Lambda@Edge ... 1334
Cuotas en certificados SSL ... 1336
Cuotas de invalidaciones ... 1337
Cuotas en grupos de claves ... 1337
Cuotas de conexiones WebSocket ... 1338
Cuotas de cifrado en el nivel de campo ... 1338
Cuotas en cookies (configuración de caché heredada) ... 1339
Cuotas en cadenas de consulta (configuración de caché heredada) ... 1340
Cuotas en encabezados ... 1340
Cuotas en distribuciones de varios inquilinos ... 1341
Información relacionada ... 1342
Ejemplos de código ... 1343
Conceptos básicos ... 1344
Acciones ... 1345
Escenarios ... 1415
Creación de una distribución de varios inquilinos y un inquilino de distribución ... 1415
Eliminar recursos de firma ... 1427

Introducción a CloudFront 1429
Firmar URL y cookies 1437
Ejemplos de CloudFront Functions 1441
Añadir encabezados de seguridad HTTP 1442
Añada un encabezado CORS 1443
Añadir un encabezado de control de caché 1444
Agregar un encabezado True-Client-IP 1445
Agregue un encabezado de origen 1445
Agregar index.html a las URL de solicitud 1446
Normalizar parámetros de cadena de consulta 1447
Redirección a una nueva URL 1448
Reescribir el URI de una solicitud 1450
Selección del origen más cercano al espectador 1452
Uso de pares clave-valor 1454
Validar un token simple 1455
Historial de documentos 1460

¿Qué es Amazon CloudFront?

Amazon CloudFront es un servicio web que agiliza la distribución de contenido web estático y dinámico como archivos .html, .css, .js y archivos de imágenes a los usuarios. CloudFront entrega el contenido a través de una red mundial de centros de datos que reciben el nombre de ubicaciones de borde. Cuando un usuario solicita contenido que se distribuye con CloudFront, la solicitud se redirige a la ubicación de borde que ofrece la mínima latencia (retraso de tiempo), de modo que el contenido se entregue con el mejor rendimiento posible.

- Si el contenido ya se encuentra en la ubicación de borde con menor latencia, CloudFront lo entrega inmediatamente.
- Si el contenido no se encuentra en dicha ubicación de borde, CloudFront lo recupera de un origen que haya definido como, por ejemplo, un bucket de Amazon S3, un canal de MediaPackage o un servidor HTTP (por ejemplo, un servidor web) que se haya definido como origen de la versión definitiva del contenido.

Por ejemplo, supongamos que distribuye una imagen desde un servidor web tradicional, en lugar de hacerlo desde CloudFront. Por ejemplo, puede distribuir una imagen, sunsetphoto.png, utilizando la URL `https://example.com/sunsetphoto.png`.

Sus usuarios podrían navegar fácilmente a esta URL y ver la imagen. Pero probablemente no sepan que su solicitud se dirige de una red a otra (a través de la compleja colección de redes interconectadas que componen Internet) hasta que se encuentra la imagen.

CloudFront agiliza la distribución de su contenido al dirigir cada solicitud de usuario mediante la red troncal de AWS a la ubicación de borde que mejor ofrezca su contenido. Por lo general, se trata de un servidor de borde de CloudFront que proporciona la entrega más rápida al lector. Utilizando la red de AWS se reduce drásticamente la cantidad de redes que tienen que atravesar las solicitudes de los usuarios, lo que mejora el desempeño. Los usuarios experimentan una menor latencia (el tiempo que se tarda en cargar el primer byte del archivo) y una mayor velocidad de transferencia de datos.

También logra mayor confiabilidad y disponibilidad, ya que las copias de los archivos (también conocidos como objetos) ahora se guardan (o se almacenan en caché) en varias ubicaciones de borde en todo el mundo.

Temas

- Cómo configurar CloudFront para entregar contenido

- Elija entre distribución estándar o distribución de varios inquilinos
- Precios
- Formas de utilizar CloudFront
- Cómo CloudFront entrega el contenido
- Ubicaciones e intervalos de direcciones IP de servidores de borde de CloudFront
- Uso de CloudFront con AWS SDK
- Recursos técnicos de CloudFront

Cómo configurar CloudFront para entregar contenido

Debe crear una distribución de CloudFront para indicar a CloudFront desde dónde desea enviar el contenido y los detalles acerca de cómo realizar un seguimiento y administrar la entrega de contenido. A continuación, CloudFront utiliza equipos (servidores perimetrales) que se encuentran próximos a los lectores para entregar dicho contenido rápidamente cuando alguien quiere verlo o utilizarlo.

Cómo configurar CloudFront para entregar su contenido

1. Debe especificar los servidores de origen, como un bucket de Amazon S3 o su propio servidor HTTP, desde el que CloudFront obtiene sus archivos que después se distribuirán desde ubicaciones de borde de CloudFront de todo el mundo.

   Un servidor de origen almacena la versión original y definitiva de sus objetos. Si ofrece contenido a través de HTTP, su servidor de origen es un bucket de Amazon S3 o un servidor HTTP, como un servidor web. Su servidor HTTP puede ejecutarse en una instancia Amazon Elastic Compute Cloud (Amazon EC2) o en un servidor que usted administre; estos servidores también reciben el nombre de orígenes personalizados.

2. Cargue sus archivos en sus servidores de origen. Los archivos, también conocidos como objetos, suelen incluir páginas web, imágenes y archivos multimedia, pero pueden ser cualquier cosa que se pueda servir a través de HTTP.

Si utiliza un bucket de Amazon S3 como servidor de origen, puede hacer que los objetos del bucket sean legibles públicamente para que cualquiera que conozca la URL de CloudFront de sus objetos pueda obtener acceso a ellos. También puede mantener los objetos privados y controlar quién obtiene acceso a ellos. Consulte Distribución de contenido privado con URL firmadas y cookies firmadas.

3. Cree una distribución de CloudFront que le indique al mismo CloudFront desde qué servidores de origen obtener los archivos cuando los usuarios los soliciten archivos a través de su aplicación o sitio web. También debe especificar detalles como si desea que CloudFront registre todas las solicitudes y que la distribución se habilite en cuanto se cree.
4. CloudFront asigna un nombre de dominio a su nueva distribución que puede ver en la consola de CloudFront o que se devuelve en respuesta a una solicitud programada, por ejemplo, una solicitud de la API. Si lo desea, puede añadir un nombre de dominio alternativo para usarlo en su lugar.
5. CloudFront envía la configuración de su distribución (pero no el contenido) a todas las ubicaciones de borde o puntos de presencia (POP): conjuntos de servidores en centros de datos dispersos geográficamente, en los que CloudFront almacena en caché las copias de los archivos.

Cuando desarrolle su sitio web o aplicación, utilice el nombre de dominio que CloudFront ofrece para sus URL. Por ejemplo, si CloudFront devuelve `d111111abcdef8.cloudfront.net` como el nombre de dominio de la distribución, la URL de logo.jpg en su bucket de Amazon S3 (o en el directorio raíz de un servidor HTTP) sería `https://d111111abcdef8.cloudfront.net/logo.jpg`.

O bien puede configurar CloudFront para usar su propio nombre de dominio con su distribución. En ese caso, la URL sería `https://www.example.com/logo.jpg`.

También puede configurar su servidor de origen para agregar encabezados a los archivos, para indicar el tiempo durante el que desea que los archivos se mantengan en la caché en las ubicaciones de borde de CloudFront. De forma predeterminada, cada uno de los archivos permanece en una ubicación de borde durante 24 horas antes de caducar. El tiempo de vencimiento mínimo es de 0 segundos y no hay un tiempo máximo. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Elija entre distribución estándar o distribución de varios inquilinos

CloudFront ofrece opciones de distribución para sitios web o aplicaciones individuales y para escenarios de varios inquilinos.

Distribución estándar

Diseñada para configuraciones únicas por sitio web o aplicación. Elija esta opción en los siguientes casos de uso:

- Necesita una distribución de CloudFront independiente
- Cada sitio o aplicación requiere una configuración personalizada propia

La mayoría de las personas comienzan con una distribución estándar.

Distribución de varios inquilinos e inquilinos de distribución (administrador de SaaS de CloudFront)

Diseñada específicamente para proveedores de SaaS y escenarios de varios inquilinos. Elija esta opción en los siguientes casos de uso:

- Va a crear una plataforma SaaS para dar servicio a varios sitios web o aplicaciones de clientes
- Necesita administrar varias distribuciones similares de manera eficiente
- Desea un control centralizado de las configuraciones compartidas

Para obtener más información, consulte Introducción al funcionamiento de las distribuciones de varios inquilinos.

Precios

CloudFront cobra por las transferencias de datos desde sus ubicaciones periféricas, junto con las solicitudes HTTP o HTTPS. Los precios varían según el tipo de uso, la región geográfica y la selección de características.

La transferencia de datos desde su origen a CloudFront siempre es gratuita si emplea orígenes de AWS como Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing o Amazon API Gateway. Solo se le factura la transferencia de datos salientes de CloudFront al lector cuando se utilizan orígenes de AWS.

Para obtener más información, consulte los precios de CloudFront y las preguntas frecuentes sobre el paquete de facturación y ahorros.

Formas de utilizar CloudFront

El uso de CloudFront puede ayudarle a lograr diferentes objetivos. En esta sección se enumeran algunos, junto con enlaces para obtener más información, para que tenga una idea de las posibilidades.

Temas

- Acelerar la entrega de contenidos de sitios web estáticos
- Distribuir vídeo bajo demanda o en streaming
- Cifrar campos específicos a través del procesamiento del sistema
- Personalizar en el borde
- Distribuir contenido privado mediante personalizaciones de Lambda@Edge

Acelerar la entrega de contenidos de sitios web estáticos

CloudFront puede acelerar la entrega de su contenido estático (por ejemplo, imágenes, hojas de estilo, JavaScript, etc.) para lectores de todo el mundo. Mediante el uso de CloudFront, puede aprovechar la red troncal de AWS y los servidores de CloudFront en el borde para ofrecer a los lectores una experiencia rápida, segura y fiable a la hora de visitar el sitio web.

Un enfoque sencillo para almacenar y entregar contenido estático consiste en utilizar un bucket de Amazon S3. El uso de S3 junto con CloudFront presenta una serie de ventajas, entre las que se incluye la opción de usar el control de acceso de origen para restringir fácilmente el acceso al contenido de Amazon S3.

Para obtener más información acerca de cómo utilizar Amazon S3 junto con CloudFront, incluida una plantilla de CloudFormation para ayudarle a empezar rápidamente, consulte Introducción a un sitio web seguro estático.

Distribuir vídeo bajo demanda o en streaming

CloudFront ofrece varias opciones para el streaming de archivos multimedia a lectores de todo el mundo, tanto de archivos grabados y como de eventos en directo.

- Para el streaming de vídeo bajo demanda (VOD), puede usar CloudFront para transmitir formatos comunes tales como MPEG DASH, Apple HLS, Microsoft Smooth Streaming y CMAF a cualquier dispositivo.

- Para difusión de una transmisión en directo, puede almacenar en caché fragmentos multimedia en el borde, de forma que varias solicitudes para el archivo de manifiesto que envía los fragmentos en el orden correcto se puedan combinar, con el fin de reducir la carga en su servidor de origen.

Para obtener más información acerca de cómo entregar contenido en streaming con CloudFront, consulte Video bajo demanda y streaming de video en directo con CloudFront.

Cifrar campos específicos a través del procesamiento del sistema

Cuando se configura HTTPS con CloudFront, ya tiene conexiones integrales seguras a servidores de origen. Cuando se añade el cifrado en el nivel de campo, puede proteger datos específicos durante su procesamiento en el sistema además de la seguridad HTTPS, de forma que solo determinadas aplicaciones en el origen puedan ver los datos.

Para configurar el cifrado en el nivel de campo, agregue una clave pública a CloudFront y, a continuación, especifique el conjunto de campos que desee cifrar con la clave. Para obtener más información, consulte Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial.

Personalizar en el borde

La ejecución de código sin servidor en el borde abre una serie de posibilidades para personalizar los contenidos y la experiencia para los espectadores, con una latencia reducida. Por ejemplo, puede devolver un mensaje de error personalizado cuando el servidor de origen está desactivado por motivos de mantenimiento, por lo que los espectadores no reciben un mensaje de error HTTP genérico. O puede utilizar una función para ayudar a autorizar a los usuarios y controlar el acceso al contenido, antes de que CloudFront reenvíe una solicitud a su origen.

El uso de Lambda@Edge con CloudFront permite distintas formas de personalizar el contenido que ofrece CloudFront. Para obtener más información acerca de Lambda@Edge y cómo crear e implementar funciones con CloudFront, consulte Personalización en la periferia con Lambda@Edge. Para ver una serie de ejemplos de código que puede personalizar para sus propias soluciones, consulte Funciones de ejemplo de Lambda@Edge.

Distribuir contenido privado mediante personalizaciones de Lambda@Edge

El uso de Lambda@Edge puede ayudarle a configurar su distribución de CloudFront para ofrecer contenidos privados desde su origen personalizado, además de usar URL o cookies firmadas.

Para ofrecer este contenido privado mediante CloudFront, haga lo siguiente:

- Exija a los usuarios (lectores) que accedan al contenido mediante URL o cookies firmadas.
- Restrinja el acceso a su origen para que solo esté disponible desde los servidores orientados al origen de CloudFront. Para ello, puede hacer una de las siguientes acciones:
  - Para un origen de Amazon S3, puede utilizar un control de acceso de origen (OAC).
  - Para un origen personalizado, puede hacer lo siguiente:
    - Si el origen personalizado está protegido por un grupo de seguridad de Amazon VPC o AWS Firewall Manager, puede utilizar la lista de prefijos administrados de CloudFront para permitir el tráfico entrante a su origen desde solo las direcciones IP orientadas al origen de CloudFront.
    - Utilice un encabezado HTTP personalizado para restringir el acceso solo a las solicitudes de CloudFront. Para obtener más información, consulte the section called “Restricción del acceso a archivos en orígenes personalizados” y the section called “Añadido de encabezados personalizados a solicitudes de origen”. Para obtener un ejemplo que utiliza un encabezado personalizado para restringir el acceso a un origen de Application Load Balancer, consulte the section called “Restricción del acceso a Application Load Balancer”.
    - Si el origen personalizado requiere una lógica de control de acceso personalizada, puede utilizar Lambda@Edge para implementarla, como se describe en esta publicación de blog: Serving Private Content Using Amazon CloudFront & Lambda@Edge (Servir contenido privado mediante Amazon CloudFront y Lambda@Edge).

Cómo CloudFront entrega el contenido

Después de una configuración inicial, CloudFront funciona conjuntamente con el sitio web o aplicación y acelera la entrega de su contenido. En esta sección se explica cómo distribuye CloudFront su contenido cuando los lectores lo solicitan.

Temas

- Cómo CloudFront entrega contenido a sus usuarios
- Cómo funciona CloudFront con las cachés de borde regionales

Cómo CloudFront entrega contenido a sus usuarios

Después de configurar CloudFront para distribuir su contenido, esto es lo que ocurre cuando los usuarios solicitan sus objetos:

1. Un usuario obtiene acceso a su sitio web o aplicación y solicita un objeto, como un archivo de imagen o un archivo HTML.
2. DNS enruta la solicitud al POP de CloudFront (ubicación periférica) que mejor puede atender la solicitud, normalmente el POP de CloudFront más cercano en términos de latencia.
3. CloudFront comprueba su caché en busca del objeto solicitado. Si el objeto está en la caché, CloudFront lo devuelve al usuario. Si el objeto no está en la caché, CloudFront hace lo siguiente:
   a. CloudFront compara la solicitud con las especificaciones de su distribución y reenvía la solicitud a su servidor de origen para el objeto correspondiente, por ejemplo, a su bucket de Amazon S3 o a su servidor HTTP.
   b. El servidor de origen devuelve el objeto a la ubicación de borde.
   c. En cuanto llega el primer byte desde el origen, CloudFront comienza a reenviar el objeto al usuario. CloudFront también agrega el objeto a la caché para la próxima vez que alguien lo solicite.

Cómo funciona CloudFront con las cachés de borde regionales

Los puntos de presencia de CloudFront (también conocidos como POP o ubicaciones de borde) garantizan que los contenidos populares puedan servirse rápidamente a los lectores. CloudFront dispone también de cachés de borde regionales que acercan más su contenido a los lectores, incluso cuando el contenido no es tan popular como para permanecer en un punto de presencia, para ayudar a mejorar el rendimiento de dicho contenido.

Las cachés perimetrales regionales ayudan con todo tipo de contenidos, especialmente los que pierden popularidad con el tiempo. Entre los ejemplos se incluyen contenido generado por usuarios como videos, fotos o ilustraciones; recursos de e-commerce como fotos y videos de productos, así como noticias y contenido relacionado con eventos que podrían hacerse populares de repente.

Cómo funcionan las cachés regionales

Las cachés de borde regionales son ubicaciones de CloudFront implementadas en todo el mundo y cercanas a sus lectores. Están ubicadas entre el servidor de origen y los puntos de presencia: ubicaciones de borde globales que distribuyen contenido directamente a los lectores. A medida que los objetos se hacen menos populares, los puntos de presencia individuales podrían quitar

dichos objetos para dejar espacio a contenido más popular. Las cachés perimetrales regionales tienen una caché mayor que un punto de presencia individual, de modo que los objetos permanecen más tiempo en la ubicación de caché perimetral regional más cercana. De esta manera, es posible conservar un mayor volumen de contenido más cerca de los lectores, lo que reduce la necesidad de que CloudFront regrese al servidor de origen y mejora el rendimiento general para los lectores.

Cuando un espectador realiza una solicitud a su sitio web o mediante su aplicación, DNS dirige la solicitud al punto de presencia que puede distribuir mejor la solicitud del usuario. Esta ubicación suele ser la ubicación de borde de CloudFront más cercana en términos de latencia. En el punto de presencia, CloudFront busca el objeto solicitado en su caché. Si el objeto está en la caché, CloudFront lo devuelve al usuario. Si el objeto no se encuentra en la caché, el POP suele dirigirse a la caché de borde regional más cercana para recuperarlo. Para obtener más información sobre cuándo el POP omite la caché de borde regional y va directamente al origen, consulte la siguiente nota.

En la caché de borde regional, CloudFront vuelve a buscar el objeto solicitado en su caché. Si el objeto se encuentra en la caché, CloudFront lo reenvía al POP que lo solicitó. En cuanto el primer byte llega desde la caché de borde regional, CloudFront comienza a reenviar el objeto al usuario. CloudFront también agrega el objeto a la caché en el POP para la próxima vez que alguien lo solicite.

En el caso de los objetos que no están almacenados en caché ni en el POP ni en la ubicación de caché de borde regional, CloudFront compara la solicitud con las especificaciones de sus distribuciones y reenvía la solicitud al servidor de origen. Después de que su servidor de origen devuelva el objeto a la ubicación de borde regional de la caché, este se reenvía al POP y, a continuación, CloudFront lo reenvía al usuario. En este caso, CloudFront también agrega el objeto a la caché en la ubicación de caché de borde regional, además de agregarlos al punto de presencia para la próxima vez que un lector lo solicite. Esto garantiza que todos los puntos de presencia de una región compartan una caché local, con lo que no es necesario realizar varias solicitudes a los servidores de origen. CloudFront mantiene además conexiones permanentes con los servidores de origen, de modo que los objetos se obtengan desde los orígenes lo antes posible.

> **Note**
>
> - Las cachés perimetrales regionales tienen paridad de características con los puntos de presencia. Por ejemplo, una solicitud de invalidación de la caché elimina un objeto tanto de las cachés de los puntos de presencia como de las cachés perimetrales regionales antes de caducar. La próxima vez que un lector solicite el objeto, CloudFront volverá al origen para recuperar la última versión.

- Los métodos HTTP proxy (`PUT`, `POST`, `PATCH`, `OPTIONS` y `DELETE`) van directamente al origen desde los puntos de presencia sin pasar por las cachés de borde regionales.
- Las solicitudes dinámicas, según se determinan en el momento de la solicitud, no fluyen a través de las cachés de borde regionales, sino que van directamente al origen.
- Cuando el origen es un bucket de Amazon S3 y la caché de borde regional óptima de la solicitud está en el mismo Región de AWS que el bucket de S3, el punto de presencia omite la caché de borde regional y va directamente al bucket de S3.

El siguiente diagrama ilustra cómo fluyen las solicitudes y las respuestas a través de las ubicaciones de borde de CloudFront y las cachés de borde regionales.

Ubicaciones e intervalos de direcciones IP de servidores de borde de CloudFront

Para obtener una lista de las ubicaciones de los servidores de borde de CloudFront, consulte la página Amazon CloudFront Global Edge Network.

Amazon Web Services (AWS) publica sus rangos de direcciones IP actuales en formato JSON. Para ver los rangos actuales, descargue ip-ranges.json. Para obtener más información, consulte Rangos de direcciones IP de AWS en la Referencia general de Amazon Web Services.

Para encontrar los intervalos de direcciones IP asociadas a servidores de borde de CloudFront, busque la siguiente cadena en ip-ranges.json:

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

También puede ver sólo los intervalos de IP de CloudFront en https://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips.

Utilizar la lista de prefijos administrados de CloudFront

La lista de prefijos administrados de CloudFront contiene los intervalos de direcciones IP de todos los servidores orientados a origen distribuidos globalmente de CloudFront. Si su origen está alojado en AWS y protegido por un grupo de seguridad de Amazon VPC, puede utilizar la lista de prefijos administrados de CloudFront para permitir el tráfico entrante a su origen solo desde los servidores orientados al origen de CloudFront, lo que impide que cualquier tráfico que no sea de CloudFront llegue a su origen. CloudFront mantiene la lista de prefijos administrados para que esté siempre actualizada con las direcciones IP de todos los servidores de origen globales de CloudFront. Con la lista de prefijos administrados de CloudFront, no es necesario la lectura o el mantenimiento de una lista de intervalos de direcciones IP.

Por ejemplo, imagine que su origen es una instancia de Amazon EC2 en la región Europa (Londres) (`eu-west-2`). Si la instancia se encuentra en una VPC, puede crear una regla de grupo de seguridad que permita el acceso HTTPS entrante desde la lista de prefijos administrados de CloudFront. Esto permite que todos los servidores orientados al origen global de CloudFront lleguen a la instancia. Si elimina todas las demás reglas entrantes del grupo de seguridad, evitará que cualquier tráfico que no sea de CloudFront llegue a la instancia.

Las listas de prefijos administrados de CloudFront son las siguientes:

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

Para obtener más información, consulte Utilizar una lista de prefijos administrados por AWS en la Guía del usuario de Amazon VPC.

> **Important**
>
> La lista de prefijos administrados de CloudFront es única en cuanto a cómo se aplica a las cuotas de Amazon VPC. Para obtener más información, consulte el peso de la lista de prefijos administrados de AWS en la Guía del usuario de Amazon VPC.

Uso de CloudFront con AWS SDK

Los kits de desarrollo de software (SDK) de AWS se encuentran disponibles en muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK para C++	AWS SDK para C++ Ejemplos de código de la
AWS CLI	AWS CLI Ejemplos de código de la
AWS SDK para Go	AWS SDK para Go Ejemplos de código de la
AWS SDK para Java	AWS SDK para Java Ejemplos de código de la
AWS SDK para JavaScript	AWS SDK para JavaScript Ejemplos de código de la
AWS SDK para Kotlin	AWS SDK para Kotlin Ejemplos de código de la
AWS SDK para .NET	AWS SDK para .NET Ejemplos de código de la
AWS SDK para PHP	AWS SDK para PHP Ejemplos de código de la
Herramientas de AWS para PowerShell	Herramientas de AWS para PowerShell Ejemplos de código de la
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) Ejemplos de código de la

Documentación de SDK	Ejemplos de código
AWS SDK para Ruby	AWS SDK para Ruby Ejemplos de código de la
AWS SDK para Rust	AWS SDK para Rust Ejemplos de código de la
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP Ejemplos de código de la
AWS SDK para Swift	AWS SDK para Swift Ejemplos de código de la

Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Recursos técnicos de CloudFront

Utilice los siguientes recursos para obtener respuestas a preguntas técnicas sobre CloudFront:

- AWS re:Post: un sitio de preguntas y respuestas de la comunidad en el que los desarrolladores pueden debatir aspectos técnicos relacionados con CloudFront.
- Soporte Center: este sitio incluye información sobre sus casos de soporte recientes, así como los resultados de AWS Trusted Advisor y las comprobaciones de estado. También contiene enlaces a foros de debate, preguntas frecuentes técnicas, el panel de estado del servicio e información sobre los planes de Soporte.
- AWS Premium Support: información sobre AWS Premium Support, un canal de soporte individualizado y de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en AWS.
- AWS IQ: obtenga ayuda de profesionales y expertos certificados de AWS.

Introducción a CloudFront

Los temas de esta sección muestran cómo comenzar a entregar su contenido con Amazon CloudFront.

El tema Configuración de su Cuenta de AWS describe los requisitos previos de los siguientes tutoriales, como la creación de una Cuenta de AWS y la creación de un usuario con acceso administrativo.

El tutorial de distribución básica muestra cómo configurar el control de acceso de origen (OAC) para enviar solicitudes autenticadas a un origen de Amazon S3.

El tutorial de sitios web estáticos seguros muestra cómo crear un sitio web estático seguro para su nombre de dominio utilizando OAC con un origen de Amazon S3. El tutorial utiliza una plantilla de Amazon CloudFront (CloudFront) para la configuración y la implementación.

Temas

- Configuración de su Cuenta de AWS
- Introducción a una distribución estándar de CloudFront
- Introducción a una distribución estándar (AWS CLI)
- Introducción a un sitio web seguro estático

Configuración de su Cuenta de AWS

En este tema se describen los pasos preliminares, como la creación de una Cuenta de AWS, para prepararle para el uso de Amazon CloudFront.

Temas

- Cómo crear una Cuenta de AWS
- Creación de un usuario con acceso administrativo
- Elección de cómo acceder a CloudFront

Cómo crear una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Procedimiento para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS le enviará un correo electrónico de confirmación cuando complete el proceso de registro. Se puede ver la actividad de la cuenta y administrarla en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no usar el usuario raíz en las tareas cotidianas.

Protección de Usuario raíz de la cuenta de AWS

1. Inicie sesión en Consola de administración de AWS como propietario de la cuenta; para ello, elija Usuario raíz e introduzca el correo electrónico de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitación de un dispositivo MFA virtual para su usuario raíz de la Cuenta de AWS (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre cómo usar Directorio de IAM Identity Center como origen de identidad, consulte Configuración del acceso de los usuarios con el Directorio de IAM Identity Center predeterminado en la Guía del usuario de AWS IAM Identity Center.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, consulte Inicio de sesión en el portal de acceso de AWS en la Guía del usuario de AWS Sign-In.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center.

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center.

Elección de cómo acceder a CloudFront

Puede acceder a Amazon CloudFront de las siguientes maneras:

- Consola de administración de AWS: los procedimientos a lo largo de esta guía explican cómo utilizar la Consola de administración de AWS para realizar tareas.
- SDK de AWS: si utiliza un lenguaje de programación para el que AWS proporciona un SDK, puede usar un SDK para obtener acceso a CloudFront. Los SDK simplifican la autenticación, se integran

fácilmente con su entorno de desarrollo y proporcionan acceso a los comandos de CloudFront. Para obtener más información, consulte Uso de CloudFront con AWS SDK.

- API de CloudFront: si utiliza un lenguaje de programación para el que no exista un SDK, consulte la Referencia de la API de Amazon CloudFront para obtener información acerca de las acciones de API y cómo realizar solicitudes de API.
- AWS CLI: la AWS Command Line Interface (AWS CLI) es una herramienta unificada para administrar los Servicios de AWS. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte Instalar o actualizar a la última versión de la AWS CLI en la Guía del usuario de la AWS Command Line Interface.
- Heramientas para Windows PowerShell: si tiene experiencia con Windows PowerShell, es posible que prefiera utilizar AWS Tools for Windows PowerShell. Para obtener más información, consulte Installing the AWS Tools for Windows PowerShell en la Guía del usuario de Herramientas de AWS para PowerShell.

Introducción a una distribución estándar de CloudFront

Los procedimientos de esta sección le muestran cómo utilizar CloudFront para configurar una distribución estándar que realiza lo siguiente:

- Crea un bucket de S3 para utilizarlo como origen de la distribución.
- Almacena las versiones originales de los objetos en un solo bucket de Amazon Simple Storage Service (Amazon S3).
- Utiliza el control de acceso de origen (OAC) para enviar solicitudes autenticadas al origen de Amazon S3. El OAC envía las solicitudes a través de CloudFront para evitar que los lectores accedan directamente al bucket de S3. Para obtener más información sobre OAC, consulte Restricción del acceso a un origen de Amazon S3.
- Utiliza el nombre de dominio de CloudFront en las URL de los objetos (por ejemplo, `https://d111111abcdef8.cloudfront.net/index.html`).
- Mantiene los objetos en ubicaciones periféricas de CloudFront durante el período predeterminado de 24 horas (la duración mínima es de 0 segundos).

La mayor parte de esto se configura automáticamente al crear una distribución de CloudFront.

Temas

- Requisitos previos

- Crear un bucket de Amazon S3
- Carga del contenido en el bucket
- Creación de una distribución de CloudFront que usa un origen de Amazon S3 con OAC
- Acceso al contenido a través de CloudFront
- Limpieza
- Mejora de la distribución básica

Requisitos previos

Antes de comenzar, asegúrese de que ha completado los pasos que se detallan en Configuración de su Cuenta de AWS.

Crear un bucket de Amazon S3

Un bucket de Amazon S3 es un contenedor para archivos (objetos) o carpetas. CloudFront puede distribuir casi cualquier tipo de archivo por usted cuando un bucket de S3 es el origen. Por ejemplo, CloudFront puede distribuir texto, imágenes y vídeos. No hay un máximo para la cantidad de datos que puede almacenar en Amazon S3.

En este tutorial, va a crear un bucket de S3 con los archivos `hello world` de ejemplo proporcionados que utilizará para crear una página web básica.

Creación de un bucket

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Le recomendamos que utilice nuestro ejemplo “Hello World” para esta introducción. Descargue la página web hello world: hello-world-html.zip. Descomprímala y guarde la carpeta `css` y el archivo `index` en un lugar adecuado, como el escritorio donde esté ejecutando el navegador.
3. Elija Crear bucket.
4. Introduzca un Nombre de bucket único que cumpla con a las reglas de nomenclatura de los buckets de uso general de la Guía del usuario de Amazon Simple Storage Service.
5. En Región, le recomendamos que elija una Región de AWS que esté geográficamente cerca de usted. (Esto reduce la latencia y los costos).
    - Elegir otra región también funciona. Puede hacerlo para cumplir con los requisitos reglamentarios, por ejemplo.

6. Deje todas las demás configuraciones en sus valores predeterminados y, a continuación, elija Crear bucket.

Carga del contenido en el bucket

Después de haber creado el bucket de Amazon S3, cargue el contenido del archivo `hello world` descomprimido en él. (Ha descargado y descomprimido este archivo en Crear un bucket de Amazon S3).

Para cargar el contenido a Amazon S3

1. En la sección Buckets de uso general, elija el nombre del nuevo bucket.
2. Seleccione Cargar.
3. En la página Cargar, arrastre la carpeta `css` y el archivo `index` al área para soltar elementos.
4. Deje todas las demás configuraciones en sus valores predeterminados y, a continuación, elija Cargar.

Creación de una distribución de CloudFront que usa un origen de Amazon S3 con OAC

En este tutorial, creará una distribución de CloudFront que utilice un origen de Amazon S3 con control de acceso de origen (OAC). OAC lo ayuda a enviar solicitudes autenticadas de forma segura al origen de Amazon S3. Para obtener más información sobre OAC, consulte Restricción del acceso a un origen de Amazon S3.

Creación de una distribución de CloudFront con un origen de Amazon S3 que usa OAC

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Crear distribución.
3. Introduzca un Nombre de distribución para la distribución estándar. El nombre aparecerá como el valor de la clave `Name` como una etiqueta. Puede cambiar este valor posteriormente. Puede agregar hasta 50 etiquetas a la distribución estándar. Para obtener más información, consulte Etiquetado de una distribución.
4. Elija Sitio web o aplicación únicos, Siguiente.
5. Elija Siguiente.

6. En la página Tipo de origen, seleccione Amazon S3.
7. En Origen de S3, elija Examinar S3 y seleccione el bucket de S3 que ha creado para este tutorial.
8. En Configuración, elija Utilizar la configuración de origen recomendada. CloudFront utilizará la configuración de caché y origen recomendada de forma predeterminada para el origen de Amazon S3, incluida la configuración del control de acceso de origen (OAC). Para obtener más información sobre los ajustes recomendados, consulte Referencia de la configuración de distribución preconfigurada.
9. Elija Siguiente.
10. En la página Habilitar las protecciones de seguridad, elija si desea habilitar las protecciones de seguridad de AWS WAF.
11. Elija Siguiente.
12. Elija Crear distribución. CloudFront actualiza la política de bucket de S3 por usted.
13. Revise la sección Detalles de la nueva distribución. Cuando la distribución termine de implementarse, el campo Última modificación cambiará de Implementando a una fecha y hora.
14. Registre el nombre de dominio que CloudFront asigna a su distribución. Tendrá un aspecto similar al siguiente: `d111111abcdef8.cloudfront.net`.

Antes de usar la distribución y el bucket de S3 de este tutorial en un entorno de producción, asegúrese de configurarlos para que se ajusten a sus necesidades específicas. Para obtener información sobre cómo configurar el acceso en un entorno de producción, consulte Configuración de acceso seguro y restricción de acceso a contenido.

Acceso al contenido a través de CloudFront

Para acceder a su contenido a través de CloudFront, combine el nombre de dominio de la distribución de CloudFront con la página principal de su contenido. (Ha registrado el nombre de dominio de distribución en Creación de una distribución de CloudFront que usa un origen de Amazon S3 con OAC).

- Su nombre de dominio de distribución podría tener este aspecto: `d111111abcdef8.cloudfront.net`.
- La ruta a la página principal de un sitio web suele ser `/index.html`.

Por lo tanto, la URL para acceder a su contenido a través de CloudFront podría tener este aspecto:

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

Si ha seguido los pasos anteriores y ha utilizado la página web hola mundo, debería ver una página web que diga ¡Hola mundo!

Cuando carga más contenido en el bucket de S3, puede acceder al contenido a través de CloudFront combinando el nombre de dominio de distribución de CloudFront con la ruta al objeto en el bucket de S3. Por ejemplo, si carga un nuevo archivo llamado `new-page.html` a la raíz de su bucket de S3, la URL tendrá el siguiente aspecto:

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

Limpieza

Si creó la distribución y el bucket de S3 solo como ejercicio de aprendizaje, elimínelos para no seguir acumulando cargos. Elimine primero la distribución. Para obtener más información, consulte los enlaces siguientes:

- Eliminar una distribución
- Eliminación de un bucket

Mejora de la distribución básica

En este tutorial de introducción se proporciona un marco mínimo para crear una distribución. Le recomendamos que explore las siguientes mejoras:

- Puede utilizar la característica de contenido privado de CloudFront para restringir el acceso al contenido de los buckets de Amazon S3. Para obtener más información acerca de la distribución de contenido privado, consulte Distribución de contenido privado con URL firmadas y cookies firmadas.
- Puede configurar su distribución de CloudFront para que use un nombre de dominio personalizado (por ejemplo, `www.example.com` en lugar de `d111111abcdef8.cloudfront.net`). Para obtener más información, consulte Uso de URL personalizadas.
- En este tutorial se utiliza un origen de Amazon S3 con control de acceso de origen (OAC). No obstante, no puede utilizar OAC si el origen es un bucket de S3 configurado como un punto de conexión de sitio web. En ese caso, debe configurar el bucket con CloudFront como un origen personalizado. Para obtener más información, consulte Uso de un bucket de Amazon S3

configurado como punto de conexión del sitio web. Para obtener más información sobre OAC, consulte Restricción del acceso a un origen de Amazon S3.

Introducción a una distribución estándar (AWS CLI)

Los procedimientos de esta sección le muestran cómo utilizar AWS CLI con CloudFront para definir una configuración básica que incluye lo siguiente:

- Creación de un bucket de Amazon S3 para utilizarlo como origen de la distribución.
- Almacenamiento de las versiones originales de los objetos en el bucket de S3.
- Uso del control de acceso de origen (OAC) para enviar solicitudes autenticadas al origen de Amazon S3. El OAC envía las solicitudes a través de CloudFront para evitar que los lectores accedan directamente al bucket de S3. Para obtener más información sobre OAC, consulte Restricción del acceso a un origen de Amazon S3.
- Uso del nombre de dominio de CloudFront en las URL de los objetos (por ejemplo, `https://d111111abcdef8.cloudfront.net/index.html`).
- Mantenimiento de los objetos en ubicaciones periféricas de CloudFront durante el período predeterminado de 24 horas (la duración mínima es de 0 segundos).

La mayoría de estas opciones pueden personalizarse. Para obtener información acerca de cómo personalizar sus opciones de distribución de CloudFront, consulte Creación de una distribución.

Requisitos previos

Antes de comenzar, asegúrese de que ha completado los pasos que se detallan en Configuración de su Cuenta de AWS.

Instale la AWS CLI y configúrela con las credenciales. Para obtener más información, consulte Cómo empezar a trabajar con AWS CLI en la Guía del usuario de AWS CLI.

Crear un bucket de Amazon S3

Un bucket de Amazon S3 es un contenedor para archivos (objetos) o carpetas. CloudFront puede distribuir casi cualquier tipo de archivo por usted cuando un bucket de S3 es el origen. Por ejemplo, CloudFront puede distribuir texto, imágenes y vídeos. No hay un máximo para la cantidad de datos que puede almacenar en Amazon S3.

En este tutorial, creará un bucket de S3 y cargará un archivo HTML que utilizará para crear una página web básica.

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

Reemplace *amzn-s3-demo-bucket* por un nombre de bucket único globalmente. En la Región de AWS, le recomendamos que elija una región que esté geográficamente cerca de usted. Esto reduce la latencia y los costos, pero también puede elegir una región diferente. Por ejemplo, puede hacerlo para cumplir los requisitos normativos.

Carga del contenido en el bucket

En este tutorial, descargue y extraiga los archivos de contenido de muestra para una página web básica “Hello World”.

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

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

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

Esto crea un directorio con un archivo `index.html` y una carpeta `css`. Cargue estos archivos en el bucket de S3.

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

Creación de un control de acceso de origen (OAC)

En este tutorial, creará un control de acceso de origen (OAC). OAC lo ayuda a enviar solicitudes autenticadas de forma segura al origen de Amazon S3. Para obtener más información sobre OAC, consulte Restricción del acceso a un origen de Amazon S3.

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

Guarde el ID de OAC de la salida como una variable de entorno. Reemplace el valor de ejemplo por un ID de OAC propio. Lo utilizará en el siguiente paso.

```
OAC_ID="E1ABCD2EFGHIJ"
```

Creación de una distribución estándar

Cree un archivo de configuración de distribución denominado `distribution-config.json`. Reemplace el nombre del bucket de ejemplo con el nombre del bucket para los valores `Id`, `DomainName` y `TargetOriginId`.

```
cat > distribution-config.json << EOF
{
    "CallerReference": "cli-example-$(date +%s)",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "S3-amzn-s3-demo-bucket",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                },
                "OriginAccessControlId": "$OAC_ID"
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "S3-amzn-s3-demo-bucket",
        "ViewerProtocolPolicy": "redirect-to-https",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["GET", "HEAD"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["GET", "HEAD"]
            }
        },
        "DefaultTTL": 86400,
        "MinTTL": 0,
        "MaxTTL": 31536000,
        "Compress": true,
```

```
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            }
        }
    },
    "Comment": "CloudFront distribution for S3 bucket",
    "Enabled": true
}
EOF
```

Cree la distribución estándar.

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

Guarde el ID de distribución y el nombre de dominio de la salida como variables de entorno. Sustituya los valores de ejemplo por sus propios valores. Los utilizará más adelante en este tutorial.

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

Antes de usar la distribución y el bucket de S3 de este tutorial en un entorno de producción, asegúrese de configurarlos para que se ajusten a sus necesidades específicas. Para obtener información sobre cómo configurar el acceso en un entorno de producción, consulte Configuración de acceso seguro y restricción de acceso a contenido.

Actualización de la política de bucket de S3

Actualice la política de bucket de S3 para permitir que CloudFront acceda a los objetos. Reemplace el nombre de bucket de ejemplo por el nombre del bucket.

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

# Create the bucket policy
cat > bucket-policy.json << EOF
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudfront::$ACCOUNT_ID:distribution/
$DISTRIBUTION_ID"
                }
            }
        }
    ]
}
EOF

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

Confirmación de la implementación de la distribución

Después de crear la distribución, la implementación tardará un tiempo en completarse. Cuando el estado de la distribución cambie de `InProgress` a `Deployed`, continúe con el siguiente paso.

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

De forma alternativa, puede utilizar el comando `wait` para esperar a que se implemente la distribución.

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

Acceso al contenido a través de CloudFront

Para acceder a su contenido a través de CloudFront, combine el nombre de dominio de la distribución de CloudFront con la página principal de su contenido. Reemplace el nombre de dominio de CloudFront de ejemplo por el suyo propio.

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

Si ha seguido los pasos anteriores y ha creado el archivo HTML, debería ver una página web donde se muestre Hello world!

Cuando carga más contenido en el bucket de S3, puede acceder al contenido a través de CloudFront combinando el nombre de dominio de distribución de CloudFront con la ruta al objeto en el bucket de S3. Por ejemplo, si carga un nuevo archivo llamado `new-page.html` a la raíz de su bucket de S3, la URL tendrá el siguiente aspecto:

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

Limpieza

Si creó la distribución y el bucket de S3 solo como ejercicio de aprendizaje, elimínelos para no seguir acumulando cargos. Desactive y elimine primero la distribución.

Desactivación y eliminación de una distribución estándar (AWS CLI)

1. En primer lugar, desactive la distribución.

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

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

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

2. Espere a que se desactive la distribución.

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

3. Elimine la distribución.

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

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

Eliminación de un bucket de S3 (AWS CLI)

- Elimine el bucket de S3 y el contenido. Reemplace el nombre del bucket de ejemplo por el suyo.

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

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

Para limpiar los archivos locales creados para este tutorial, ejecute los siguientes comandos:

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

Si lo desea, puede eliminar el OAC que ha creado para este tutorial.

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

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

Introducción a un sitio web seguro estático

Puede comenzar a usar Amazon CloudFront con la solución descrita en este tema para crear un sitio web estático seguro para su nombre de dominio. Un sitio web estático solo utiliza archivos estáticos,

como HTML, CSS, JavaScript, imágenes y vídeos, y no necesita servidores ni procesamiento del lado del servidor. Con esta solución, su sitio web obtiene los siguientes beneficios:

- Utiliza el almacenamiento duradero de Amazon Simple Storage Service (Amazon S3): esta solución crea un bucket de Amazon S3 para alojar el contenido de su sitio web estático. Para actualizar el sitio web, solo tiene que cargar los archivos nuevos en el bucket de S3.
- Está acelerado por la red de entrega de contenido de Amazon CloudFront: esta solución crea una distribución de CloudFront para servir su sitio web a los lectores con baja latencia. La distribución está configurada con un control de acceso de origen (OAC) para asegurarse de que solo se pueda acceder al sitio web mediante CloudFront, no directamente desde S3.
- Está protegido por HTTPS y encabezados de seguridad: esta solución crea un certificado SSL/TLS en AWS Certificate Manager (ACM) y lo asocia a la distribución de CloudFront. Este certificado permite que la distribución sirva el sitio web de su dominio de forma segura con HTTPS.
- Se configura e implementa con AWS CloudFormation: esta solución utiliza una plantilla de CloudFormation para configurar todos los componentes, de modo que pueda centrarse más en el contenido de su sitio web y menos en la configuración de componentes.

Esta solución es de código abierto en GitHub. Para ver el código, enviar una solicitud de extracción o abrir una incidencia, vaya a https://github.com/aws-samples/amazon-cloudfront-secure-static-site.

Temas

- Información general de la solución
- Implementación de la solución

Información general de la solución

En el siguiente diagrama se muestra información general de cómo funciona esta solución de sitio web estático:

1. El lector solicita el sitio web en www.example.com.
2. Si el objeto solicitado está en caché, CloudFront devuelve el objeto de su caché al lector.
3. Si el objeto no está en la caché de CloudFront, CloudFront solicita el objeto desde el origen (un bucket de S3).
4. S3 devuelve el objeto a CloudFront.
5. CloudFront almacena el objeto en caché.
6. Los objetos se devuelven al espectador. Las solicitudes posteriores del objeto que llegan a la misma ubicación de borde de CloudFront se sirven desde la memoria caché de CloudFront.

Implementación de la solución

Para implementar esta solución de sitio web estático seguro, puede elegir una de las siguientes opciones:

- Utilice la consola de CloudFormation para implementar la solución con contenido predeterminado y, a continuación, cargue el contenido del sitio web en Amazon S3.
- Clone la solución en su equipo para agregar contenido de su sitio web. A continuación, implemente la solución con AWS Command Line Interface (AWS CLI).

> **Note**
>
> Debe usar la región Este de EE. UU. (Norte de Virginia) para implementar la plantilla de CloudFormation.

Temas

- Requisitos previos
- Uso de la consola de CloudFormation
- Clonación local de la solución
- Búsqueda de registros de acceso

Requisitos previos

Para utilizar esta solución, debe cumplir los siguientes requisitos previos:

- Un nombre de dominio registrado, como example.com, que apunte a una zona alojada por Amazon Route 53. La zona alojada debe estar en la misma Cuenta de AWS en la que implementa esta solución. Si no tiene un nombre de dominio registrado, puede registrarlo con Route 53. Si tiene un nombre de dominio registrado pero no apunta a una zona alojada por Route 53, configure Route 53 como su servicio de DNS.
- Permisos de AWS Identity and Access Management (IAM) para iniciar plantillas de CloudFormation que crean roles de IAM y permisos para crear todos los recursos de AWS en la solución. Para obtener más información, consulte Controlar el acceso con AWS Identity and Access Management en la Guía del usuario de AWS CloudFormation.

Usted es responsable de los costos generados durante el uso de esta solución. Para obtener más información sobre los costos, consulte las páginas de precios de cada Servicio de AWS.

Uso de la consola de CloudFormation

Para efectuar la implementación mediante la consola de CloudFormation

1. Inicie esta solución en la consola de CloudFormation. Si es necesario, inicie sesión en la Cuenta de AWS.
2. Se abre el asistente Crear pila en la consola de CloudFormation, con campos ya rellenados que especifican la plantilla de CloudFormation de esta solución.

   En la parte inferior de la página, elija Next.
3. En la página Especificar los detalles de la pila, escriba valores para los siguientes campos:
   - SubDomain (SubDominio): escriba el subdominio que se va a utilizar para su sitio web. Por ejemplo, si el subdominio es www, el sitio web está disponible en *www*.example.com. (Reemplace example.com por su nombre de dominio, como se explica en el siguiente punto).
   - DomainName (NombreDominio): escriba su nombre de dominio, como *example.com*. Este dominio debe apuntar a una zona alojada por Route 53.
   - HostedZoneID: el ID de zona alojada de Route 53 del nombre de dominio.
   - CreateApex: (opcional) cree un alias para el ápex del dominio (example.com) en la configuración de CloudFront.
4. Cuando haya terminado, elija Next (Siguiente).
5. (Opcional) En la página Configure stack options (Configurar las opciones la de pila), agregue etiquetas y otras opciones de pila.

6. Cuando haya terminado, elija Next (Siguiente).
7. En la página Revisar, desplácese hasta la parte inferior de la página y, a continuación, seleccione los dos cuadros de la sección Capacidades. Estas capacidades permiten a CloudFormation crear un rol de IAM que permite el acceso a los recursos de la pila y asignar nombres a los recursos dinámicamente.
8. Elija Create stack.
9. Espere a que termine la creación de la pila. La pila crea algunas pilas anidadas y puede tardar varios minutos en terminar. Cuando termine, el estado cambia a CREATE_COMPLETE.

   Cuando el estado sea CREATE_COMPLETE, vaya a https://*www.example.com* para ver su sitio web (reemplace www.example.com por el subdominio y el nombre de dominio especificados en el paso 3). Debería ver el contenido predeterminado del sitio web:

Para reemplazar el contenido predeterminado del sitio web por el suyo propio

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Elija el bucket cuyo nombre comienza por amazon-cloudfront-secure-static-site-s3bucketroot-.

   > **Note**
   > Asegúrese de elegir el bucket que tiene s3bucketroot en el nombre, no s3bucketlogs. El bucket con s3bucketroot en el nombre incluye el contenido del sitio web. El que tiene s3bucketlogs solo contiene archivos de registro.

3. Elimine el contenido predeterminado del sitio web y, a continuación, cargue el suyo propio.

   > **Note**
   > Si ha visto su sitio web con el contenido predeterminado de esta solución, es probable que parte del contenido predeterminado se almacene en caché en una ubicación de borde de CloudFront. Para asegurarse de que los lectores vean el contenido actualizado del sitio web, invalide los archivos para quitar las copias almacenadas en caché de

las ubicaciones de borde de CloudFront. Para obtener más información, consulte Invalidación de archivos para eliminar el contenido.

Clonación local de la solución

Requisitos previos

Para agregar contenido de su sitio web antes de implementar esta solución, debe empaquetar localmente los artefactos de la solución, lo que requiere Node.js y npm. Para obtener más información, consulte https://www.npmjs.com/get-npm.

Para agregar contenido de su sitio web e implementar la solución

1. Clone o descargue la solución desde https://github.com/aws-samples/amazon-cloudfront-secure-static-site. Después de clonarla o descargarla, abra un símbolo del sistema o terminal y navegue hasta la carpeta `amazon-cloudfront-secure-static-site`.
2. Ejecute el siguiente comando para instalar y empaquetar los artefactos de la solución:

```
make package-static
```

3. Copie el contenido de su sitio web en la carpeta `www`, con lo que se sobrescribe el contenido predeterminado del sitio web.
4. Ejecute el siguiente comando de AWS CLI para crear un bucket de Amazon S3 a fin de almacenar los artefactos de la solución. Reemplace *`amzn-s3-demo-bucket-for-artifacts`* por el nombre de bucket propio.

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

5. Ejecute el siguiente comando de la AWS CLI para empaquetar los artefactos de la solución como una plantilla de CloudFormation. Reemplace *`amzn-s3-demo-bucket-for-artifacts`* por el nombre del bucket que ha creado en el paso anterior.

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

6. Ejecute el siguiente comando para implementar la solución con CloudFormation; para ello, reemplace los siguientes valores:

   - *your-CloudFormation-stack-name*: reemplácelo por un nombre para la pila de CloudFormation.
   - *example.com*: reemplácelo por el nombre de su dominio. Este dominio debe apuntar a una zona alojada de Route 53 en la misma Cuenta de AWS.
   - *www*: reemplácelo por el subdominio que se usará para su sitio web. Por ejemplo, si el subdominio es www, el sitio web está disponible en www.example.com.
   - *hosted-zone-ID*: reemplácelo por el ID de zona alojada de Route 53 del nombre de 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
```

   - (Opcional) Para implementar la pila con un ápex de dominio, ejecute el siguiente comando en su lugar.

```
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. Espere a que se termine de crear la pila de CloudFormation. La pila crea algunas pilas anidadas y puede tardar varios minutos en terminar. Cuando termine, el estado cambia a CREATE_COMPLETE.

   Cuando el estado cambie a CREATE_COMPLETE, vaya a https://www.example.com para ver su sitio web (reemplace www.example.com por el subdominio y el nombre de dominio especificados en el paso anterior). Debería ver el contenido de su sitio web.

Búsqueda de registros de acceso

Esta solución habilita los registros de acceso para la distribución de CloudFront. Complete los siguientes pasos para localizar los registros de acceso de la distribución.

Para localizar los registros de acceso de la distribución

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Elija el bucket cuyo nombre comience por amazon-cloudfront-secure-static-site-s3bucketlogs-.

> **Note**
>
> Asegúrese de elegir el bucket que tiene s3bucketlogs en el nombre, no s3bucketroot. El bucket con s3bucketlogs en el nombre contiene los archivos de registro. El que tiene s3bucketroot incluye el contenido del sitio web.

3. La carpeta denominada cdn contiene los registros de acceso de CloudFront.

Planes de precios de tarifa fija de CloudFront

Los planes de precios de tarifa fija de CloudFront combinan la red de entrega de contenido (CDN) global de Amazon CloudFront con múltiples Servicios de AWS y características en un precio mensual sin cargos por exceso, independientemente de los picos de tráfico o los ataques.

Los planes de precios de tarifa fija incluyen las siguientes características por un precio mensual sencillo:

- CloudFront CDN
- AWS WAF y protección contra ataques DDoS
- Administración y análisis de bots
- DNS de Amazon Route 53
- Ingesta de registros de Amazon CloudWatch
- Certificado TLS
- Computación de periferia sin servidor
- Créditos de almacenamiento de Amazon S3 cada mes

Los planes están disponibles en los niveles Free, Pro, Business y Premium para adaptarse a las necesidades de la aplicación. Los planes no requieren un compromiso anual para obtener las mejores tarifas disponibles. Comience con el plan gratuito y actualícelo para acceder a más capacidades y mayores límites de uso.

Temas

- Beneficios de los planes de precios de tarifa fija de CloudFront
- Características por plan de precios
- Asignaciones de uso mensuales
- Costos cubiertos por el plan
- Reducción de los costos de AWS generales con planes de precios
- Administración de los planes de precios de tarifa fija
- Permisos
- Cuotas de planes de precios de tarifa fija
- Características no admitidas

Beneficios de los planes de precios de tarifa fija de CloudFront

El plan de precios de CloudFront proporciona varios beneficios clave:

- Servicios y precios consolidados

  Combine múltiples Servicios de AWS y características en un solo plan por una tarifa fija. Se ha diseñado para eliminar las compras de servicios independientes y los cálculos de precios por adelantado.

- Sin excedentes

  No se cobran cargos por exceso de tráfico, independientemente de los picos de tráfico o los ataques.

- Asignaciones de uso claras

  Cada plan incluye las asignaciones de uso publicadas diseñadas para un rendimiento óptimo en ese nivel. Supervise su uso, reciba notificaciones proactivas y actualice en función de las necesidades de la aplicación, sin compromisos a largo plazo.

- Protección contra los ataques DDoS

  CloudFront y AWS WAF absorben y bloquean los ataques antes de que lleguen a la infraestructura. Reserva el uso informático, de la base de datos y la infraestructura solo para el tráfico legítimo. Los ataques DDoS bloqueados y las solicitudes bloqueadas por AWS WAF nunca se descontarán de la asignación de uso.

- Reducción de los costos de AWS generales

  La transferencia de datos desde las aplicaciones de AWS que se ejecutan en servicios como Amazon S3, equilibrador de carga de aplicación (ALB) de AWS o Amazon API Gateway a CloudFront sigue siendo gratuita. Si entrega las aplicaciones de AWS a través de CloudFront en lugar de hacerlo directamente a Internet, el plan de tarifa fija cubre los costos de transferencia de datos entre las aplicaciones y los espectadores por un simple precio mensual sin preocuparse por los excedentes. El menor número de solicitudes que llegan al lugar de origen también reduce los costos de los servicios, que se cobran en función del uso.

Características por plan de precios

Cada plan de precios cubre una distribución de CloudFront con hasta un dominio Apex (raíz) que combina características y servicios esenciales en un solo precio mensual. Cada plan también incluye créditos de almacenamiento de S3 adicionales.

Los planes de niveles superiores incluyen todas las características de los planes de niveles inferiores, así como características adicionales.

- Gratis: para aficionados, estudiantes y desarrolladores que estén empezando.
- Pro: lance y desarrolle sitios web, blogs y aplicaciones pequeños.
- Business: proteja y acelere las aplicaciones empresariales.
- Premium: escale y proteja las aplicaciones empresariales y de misión crítica.

Seleccione un nivel de plan que incluya las características y configuraciones que necesita para las aplicaciones. Consulte las siguientes características por plan de precios.

Características del plan de precios

En la siguiente tabla se muestran las características de CloudFront, AWS WAF y DDoS, Amazon Route 53, Amazon CloudWatch y Amazon S3 incluidas en cada nivel del plan de precios.

Rendimiento y entrega	Free	Pro	Usuarios	Premium
CDN global	Sí	Sí	Sí	Sí
Utilice las más de 750 ubicaciones periféricas globales de CloudFront como un punto de entrada masivo, distribuido y único para la aplicación	✓	✓	✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
web. Acelere las aplicaciones estáticas, dinámicas y que no se pueden almacenar en caché.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Almacenamiento de contenido en caché Almacene copias del contenido en las más de 750 ubicacion es periféricas de CloudFront en todo el mundo y envíelas a los usuarios desde la ubicación más cercana. Reduce los tiempos de carga, protege la aplicación de los picos de tráfico y ahorra costos al atender las solicitud es repetidas de forma local en lugar de hacerlo desde los servidores de aplicaciones.	Sí	Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Invalidaciones de caché instantáneas Elimine o actualice el contenido almacenado en caché en todas las ubicaciones periféricas en cuestión de segundos.	Sí	Sí	Sí	Sí
Enrutamiento inteligente Dirige a los usuarios de forma inteligente a la ubicación periférica óptima mediante datos de red en tiempo real y se conecta al origen de AWS a través de la red privada de AWS para mejorar el rendimiento.	Sí	Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Almacenamiento en caché por niveles Las cachés periféricas regionales se ubican entre las ubicaciones periféricas y la aplicación para almacenar el contenido durante más tiempo, lo que reduce la carga de la aplicación y permite una entrega rápida.	Sí	Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Reglas de almacenamiento en caché predeterminadas	Sí	Sí	Sí	Sí
Toma decisiones de almacenamiento en caché eficaces para almacenar en caché la mayoría de las aplicaciones web sin una configuración personalizada.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Reglas de almacenamiento en caché personalizadas			Sí	Sí
Controle la forma en que CloudFront almacena en caché el contenido especificando qué valores de solicitud utilizar y optimizándolos según las necesidades de rendimiento, personalización y actualización de la aplicación mediante políticas de caché.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Enrutamiento de origen de alta velocidad Con Origin Shield, las solicitudes dinámicas se enrutan desde las ubicacion es periféricas hasta el origen mediante la red privada de CloudFront para una ruta de alto rendimiento hacia el origen.				Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Reducción de la carga de origen				Sí
Agrega una capa de almacenamiento en caché adicional cerca de la aplicación web mediante Origin Shield. Origin Shield consolida las solicitudes de todas las ubicaciones periféricas, lo que reduce la carga de la aplicación, especialmente durante los picos de tráfico.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Conmutación por error de origen automática Si el origen principal produce un error, dirige automáticamente el tráfico a un origen de copia de seguridad, lo que permite mantener una alta disponibilidad sin interrumpir a los usuarios.				Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Reglas de solicitud de origen predeterminadas	Sí	Sí	Sí	Sí
Controle qué información de las solicitudes de los espectadores se incluye automáticamente en las solicitudes que se envíen al origen mediante políticas de solicitudes de origen administradas por AWS optimizadas para situaciones habituales.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Reglas de encabezado de respuesta predeterminadas Utilice políticas de encabezados de respuesta administradas por AWS para agregar o eliminar encabezados HTTP en las respuestas a los espectadores, preconfiguradas para los encabezados de seguridad comunes, la configuración de CORS y otros casos de uso estándar.	Sí	Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Reglas de solicitud de origen personalizadas			Sí	Sí
Cree sus propias políticas de solicitudes de origen para especificar exactamente qué cadenas de consulta de URL, encabezados y cookies se reenvían al origen, lo que permite personalizar el análisis y la gestión de las solicitudes.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Reglas personalizadas para los encabezados de respuesta			Sí	Sí
Cree sus propias políticas de encabezados de respuesta para controlar exactamente qué encabezados HTTP agrega o quita CloudFront en las respuestas a los espectadores, como los encabezados de seguridad, la política de seguridad de contenido (CSP), la configuración de CORS y los encabezados de aplicaciones personalizados.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Número de comportamientos de la memoria caché	5	10	50	100
Configure los comportamientos de la caché para controlar la forma en que CloudFront gestiona las solicitudes de patrones de URL específicos, incluido el origen que proporciona el contenido, la forma en que se almacena el contenido en caché y si se requieren HTTPS o URL firmadas.				
Seguridad y protección				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Protección contra DDoS permanente Protéjase contra los ataques DDoS dirigidos a los sitios web o aplicaciones.	Sí	Sí	Sí	Sí
Protección contra DDoS avanzada Identifique y bloquee los ataques DDoS en cuestión de segundos con el AntiDDoS AMR. AWS aprende los patrones únicos de las aplicaciones para distinguir entre los ataques y las oleadas naturales de usuarios legítimos.			Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Web Application Firewall (WAF) Protéjase contra las vulnerabilidades comunes de las aplicaciones y las posibles amenazas en función de la inteligencia de amenazas internas de Amazon. Las solicitudes se bloquean antes de que lleguen a los servidores.	Sí	Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Número de reglas de WAF	5	25	50	75
Número total de reglas de seguridad que puede crear y habilitar en la configura ción de WAF, incluidas las reglas personali zadas y las reglas administr adas por AWS.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Protecciones para bases de datos de WordPress, PHP y SQL		Sí	Sí	Sí
Reglas de seguridad basadas en casos de uso para proteger aplicaciones y sistemas operativos comunes como WordPress, PHP, bases de datos SQL, Linux y Windows.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Limitación de velocidad basada en IP Bloquee automáticamente las direcciones IP que superen un número configurable de solicitud es durante un periodo de 5 minutos, protegiéndolas contra los ataques de inundación HTTP y los intentos de denegación de servicio (DoS).	Sí	Sí	Sí	Sí
Bloqueo geográfico del tráfico Bloquee las solicitudes de países o regiones seleccionados.	Sí	Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Filtrado de amenazas basado en encabezados		Sí	Sí	Sí
Cree reglas de seguridad de WAF que filtren las amenazas en función de los encabezados de las solicitudes HTTP.				
Filtrado de amenazas basado en expresiones regulares			Sí	Sí
Cree reglas de seguridad de WAF utilizando expresiones regulares para hacer coincidir las rutas de URI y los atributos de las solicitudes HTTP.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Desafío de JavaScript			Sí	Sí
Bloquee las amenazas automatizadas exigiendo a los navegadores que completen los desafíos de JavaScrip t que verifican a los usuarios legítimos.			✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Administración y análisis de bots			Sí	Sí
Detecte y analice el tráfico de bots con Control de bots de AWS WAF para los bots habituales. Proporciona controles para bloquear, desafiar o permitir la entrada de bots no verificados, al tiempo que identifica y distingue a los bots verificados, como ocurre en los motores de búsqueda.			✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Respuesta de WAF personalizada Establezca un código de estado HTTP específico y una respuesta HTML, de texto sin formato o JSON personalizada opcional cuando una regla bloquee las solicitudes.		Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Inserción de encabezados	Sí	Sí	Sí	Sí
Agregue encabezados HTTP personalizados a las solicitudes que pasen la inspección de WAF, lo que permitirá a las aplicaciones posteriores procesar las solicitudes de forma diferente o marcarlas para su análisis.	✓	✓	✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Solicitud de inspección del cuerpo	16 KB	16 KB	64 KB	64 KB
Tamaño máximo del contenido del cuerpo de la solicitud HTTP que puede inspeccionar AWS WAF para detectar amenazas y patrones maliciosos.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Orígenes privados dentro de la VPC			Sí	Sí
Mejore la seguridad manteniendo la aplicación en una subred privada de VPC, accesible solo a través de las distribuciones de CloudFront y oculta del Internet público, mediante orígenes de la VPC.			✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
TLS mutua (origen)			Sí	Sí
Restrinja el acceso no autorizado a la aplicación (origen) mediante certificados de cliente basados en TLS y asegúrese de que solo las distribuciones de CloudFront autorizadas puedan establecer conexiones con la aplicación.			✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Control de acceso de origen (OAC) Mantenga un bucket de S3 privado y permita el acceso solo a través de la distribución de CloudFront designada, lo que garantiza que el contenido esté protegido por las reglas de WAF, los límites de velocidad y otros controles de seguridad configurados en la distribución de CloudFront.	Sí	Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Certificado TLS gratuito	Sí	Sí	Sí	Sí
Certificado TLS gratuito para el dominio con renovación automática mediante AWS Certificate Manager.	✓	✓	✓	✓
URL firmadas	Sí	Sí	Sí	Sí
Cree URL seguras que proporcionen acceso temporal a contenido privado para usuarios específicos. Suele utilizarse para compartir documentos privados con usuarios autorizados o para conceder acceso seguro a contenido protegido tras la verificación del pago.	✓	✓	✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
TLS mutuo (mTLS)				Sí
Restrinja el acceso a la aplicación mediante la autenticación mTLS, asegurándose de que solo los clientes de confianza con certificados válidos puedan conectarse.				✓
Computación de periferia				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Computación de periferia sin servidor Ejecute JavaScript ligero en la periferia para modificar las URL, los encabezados HTTP y los elementos de solicitud/respuesta en milisegundos mediante CloudFront Functions.	Sí	Sí	Sí	Sí
Almacén clave-valor de periferia Almacene los datos en la periferia mediante KeyValueStore para personalizar el contenido de forma rápida y dinámica con CloudFront Functions.		Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Soporte de redes y protocolos				
IPv6	Sí	Sí	Sí	Sí
Entregue contenido a través de conexiones IPv6 modernas e IPv4 tradicionales desde CloudFront a los espectadores y a los orígenes. Habilita el soporte integral de IPv6 para las aplicaciones.	✓	✓	✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
HTTP/2	Sí	Sí	Sí	Sí
Permita que las páginas se carguen más rápidamente mediante características de protocolo modernas, como la multiplexación, la compresión de encabezados y la priorización de flujos. Se utiliza automáticamente cuando los navegadores y los clientes lo admiten.	✓	✓	✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
HTTP/3	Sí	Sí	Sí	Sí
Entregue contenido mediante QUIC a los navegadores y clientes compatibles, lo que permite conexiones más rápidas y un rendimiento mejorado. Beneficia especialmente a los usuarios móviles y mantiene las conexiones cuando cambian las condiciones de la red.	✓	✓	✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
TLS 1.3	Sí	Sí	Sí	Sí
Ofrezca conexiones HTTPS más rápidas mediante un proceso de establecimiento de comunicación que requiere un viaje de ida y vuelta, en comparación con dos en TLS 1.2. Reduce la latencia del primer byte hasta un 33 % en comparación con las versiones anteriores de TLS. Habilitado de extremo a extremo para las aplicaciones.	✓	✓	✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
WebSockets	Sí	Sí	Sí	Sí
Permita una comunicación bidireccional persistente y en tiempo real entre navegadores y servidores. Ideal para aplicaciones de chat de IA, juegos de varios jugadores, espacios de trabajo de colaboración y fuentes de distribución de datos en tiempo real como las plataformas de comercio financiero.	✓	✓	✓	✓
Registro y supervisión				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Registros de acceso de		Sí	Sí	Sí
Acceda a los registros de solicitudes detallados de CloudFront para comprender los patrones de tráfico de seguridad y entrega, ya que registros de Amazon CloudWatch incluye la ingesta sin costo adicional.		✓	✓	✓

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Registros de solicitudes de WAF Acceda a los registros de solicitudes de AWS WAF detallados para comprender los patrones de tráfico de seguridad y entrega. La ingesta de registros de Amazon CloudWatch está incluida sin costo adicional.		Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Panel de seguridad	Sí	Sí	Sí	Sí
Supervise los eventos de seguridad, investigue las amenazas y tome medidas de bloqueo inmediatas mediante el análisis visual sin necesidad de escribir reglas de seguridad. La versión Pro y las versiones posteriores incluyen un analizador visual de registros para comprender rápidamente los patrones de tráfico sin consultar los registros.	✓	✓	✓	✓
DNS				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
DNS de Amazon Route	Sí	Sí	Sí	Sí
Servicio de DNS autorizado público rápido y fiable que utiliza Route 53.	✓	✓	✓	✓
Registros por zona alojada	50	100	1000	5000
El número máximo de registros de DNS permitidos en la zona alojada.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
DNSSEC	Sí	Sí	Sí	Sí
Proteja su dominio contra la suplantación de DNS y los ataques de intermediarios, en los que los atacantes interceptan las consultas de DNS y redirigen a los visitantes a sitios web falsos. Protege el tráfico de DNS firmando criptográficamente los registros de DNS.	✓	✓	✓	✓
Almacenamiento				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Almacenamiento de Amazon S	5 GB	50 GB	1 TB	5 TB
Créditos de almacenamiento de Amazon S3 que compensan cualquier costo de almacenamiento estándar de S3 en la Cuenta de AWS. No se limita al contenido de CloudFront ni está sujeto a las asignaciones de uso del plan.				
Compatibilidad y fiabilidad				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
24Soporte de cuentas y facturación en cualquier momento	Sí	Sí	Sí	Sí
Respuestas personalizadas a preguntas relacionadas con cuentas y facturación.				
Si tiene un plan de asistencia pagado, es elegible para recibir asistencia en todos los planes de tarifa fija.				

Rendimiento y entrega	Free	Pro	Usuarios	Premium
Documentación y foros de AWS Support Acceda a la documentación del producto, los documentos técnicos, las guías de prácticas recomendadas, los foros comunitarios de AWS re:Post y la información sobre el estado de los servicios para planificar y solucionar problemas.	Sí	Sí	Sí	Sí

Rendimiento y entrega	Free	Pro	Usuarios	Premium
SLA de tiempo de actividad			Sí	Sí
Los acuerdos de nivel de servicio (SLA) para Amazon CloudFront, AWS WAF, Amazon Route 53 y Amazon CloudWatch incluyen compromisos de disponibilidad del servicio. En caso de que AWS no cumpla con el compromiso del SLA asociado, tendrá derecho a recibir un crédito de servicio.			✓	✓

Asignaciones de uso mensuales

Cada plan de tarifa plana incluye una asignación de uso mensual diseñada para un rendimiento óptimo en ese nivel. Puede realizar un seguimiento de la asignación de uso en la consola de CloudFront en cualquier momento. También recibirá notificaciones automáticas por correo electrónico cuando alcance el 50 %, el 80 % y el 100 % de la asignación, aunque es posible que las notificaciones se retrasen.

Seleccione un plan en el que la asignación de uso mensual se adapte al tráfico de referencia, tanto en las solicitudes como en las transferencias de datos. Si supera la asignación, no incurrirá en ningún cargo por exceso de uso. Esto permite operar la aplicación sin preocuparse por los costos derivados de picos de tráfico o ataques inesperados. Si se acaban las características del plan o cambia el tráfico de referencia, pase al siguiente nivel para acceder a más características y aumentar la asignación de uso mensual. Si el uso supera las asignaciones en el plan de precios de tarifa fija de CloudFront, AWS puede tomar las medidas adecuadas, que pueden incluir reducir el rendimiento (por ejemplo, atender el tráfico desde ubicaciones periféricas menos o más distantes, reducir el rendimiento o limitar) o solicitar un cambio en la estructura de precios.

Si el uso base de la aplicación supera los 500 millones de solicitudes o los 50 TB al mes, contacte con nosotros para conocer los precios personalizados.

Asignaciones de uso mensuales por nivel del plan

	Free	Pro	Usuarios	Premium
Solicitudes	1 millón	10 millones	125 millones	500 millones
Transferencia de datos	100 GB	50 TB	50 TB	50 TB

> **Note**
>
> Los ataques DDoS bloqueados y las solicitudes bloqueadas por AWS WAF nunca se descontarán de la asignación de uso.

La elegibilidad se basa en el uso histórico

Su uso histórico de CloudFront puede afectar a su aptitud para suscribirse a niveles de plan específicos o pasarse a un plan específico. Si el uso reciente supera las asignaciones de uso de un nivel del plan, es posible que deba seleccionar un nivel superior que se adapte mejor a la carga de trabajo.

Costos cubiertos por el plan

El plan cubre los costos de:

- La distribución de CloudFront
- La ACL web de AWS WAF asociada a la distribución.
- Ingesta de registros de CloudWatch para los registros de acceso a CloudFront de la distribución y los registros de WAF asociados
- La zona alojada de Route 53, los registros de DNS y las consultas de DNS cuando se adjuntan al plan de distribución

También recibirá créditos de S3 para compensar el uso de almacenamiento estándar de S3 en la cuenta de pagador, independientemente de que se utilice o no un bucket de S3 como origen para su distribución de CloudFront.

La administración de DNS de Route 53 y su plan

Si usa Route 53 para DNS y adjunta la zona al plan, el plan de tarifa fija puede incluir los costos de la zona alojada de Route 53. Puede adjuntar la zona al plan en la sección Administrar plan de la distribución de CloudFront. Cuando la zona esté asociada al plan, el plan cubrirá los costos estándar de la zona alojada, incluida la cuota mensual de la zona alojada, los registros de DNS y las tarifas de consulta de DNS, con sujeción a las asignaciones respectivas por nivel, que se indican a continuación. La zona alojada debe cumplir los siguientes requisitos:

- Existir en la misma cuenta de AWS que la distribución de CloudFront
- Mantener la cantidad de registros permitidos por zona alojada para el nivel del plan
- Cubrir el dominio utilizado por la distribución de CloudFront

Si la zona alojada no está vinculada al plan, seguirá teniendo un precio de pago por uso, en el que usted correrá con todos los costos estándar de Route 53.

Cómo entender las asignaciones mensuales de consultas de DNS

Cuando la zona alojada se vincula al plan, obtiene:

1. Consultas de DNS a registros ALIAS que apuntan a la distribución de CloudFront y a otros Servicios de AWS compatibles
2. Una asignación mensual adicional para otros tipos de registros de DNS

	Free	Pro	Usuarios	Premium
Consultas de DNS a registros ALIAS (CloudFront y otros Servicios de AWS compatibles) por mes	Sin límite	Sin límite	Sin límite	Sin límite
Asignación de consultas de DNS adicional por mes	1 millón	5 millones	20 millones	100 millones

> **Note**
>
> Para maximizar los beneficios del plan, utilice registros ALIAS para apuntar a la distribución de CloudFront. Los registros ALIAS que apuntan a CloudFront y a otros Servicios de AWS compatibles no se incluyen en la asignación mensual de consultas de DNS. Todas las demás consultas de DNS, incluidos los registros CNAME a CloudFront, se descontarán de la asignación de consultas de DNS.

Superación de las asignaciones de consulta de DNS

Si el uso de la consulta de DNS supera la asignación mensual del plan, AWS puede que se lo notifique. En ese momento, puede separar la zona alojada del plan en la sección Administrar plan de la distribución de CloudFront para que la zona alojada vuelva a tener un precio de pago por uso. Si no desconecta la zona alojada después de recibir esta notificación, AWS puede hacer la transición automática de la zona alojada a precios de pago por uso. Cuando una zona alojada pasa a los precios de pago por uso, usted es responsable de todos los costos estándar de Route 53. La distribución de CloudFront y todos los demás beneficios del plan permanecen inalterados.

Reducción de los costos de AWS generales con planes de precios

Los planes de precios de tarifa fija de CloudFront pueden reducir los costos de AWS generales de tres maneras:

Primero, los costos de la transferencia de datos entre CloudFront y las aplicaciones de AWS que se ejecutan en servicios como Amazon S3, equilibrador de carga de aplicación (ALB) de AWS o Amazon API Gateway se eximen automáticamente. Si entrega las aplicaciones de AWS a través de CloudFront en lugar de hacerlo directamente a Internet, el plan de tarifa fija cubre los costos de transferencia de datos entre las aplicaciones y los espectadores por un simple precio mensual sin preocuparse por los excedentes.

En segundo lugar, CloudFront reduce los costos informáticos y de bases de datos al proteger la infraestructura de aplicaciones y reducir la cantidad de solicitudes que llegan al origen. Sirve el contenido almacenado en caché desde ubicaciones periféricas o cachés periféricas regionales, reduce las solicitudes duplicadas y bloquea el tráfico malintencionado y no deseado antes de que llegue a los servicios de backend. Esto se traduce en menos solicitudes que lleguen a los servidores de aplicaciones, bases de datos y otros Servicios de AWS que se cobran en función del uso, lo que reduce los costos.

Por último, cada plan incluye créditos de almacenamiento de Amazon S3 Standard para compensar el uso de almacenamiento para la Cuenta de AWS.

Para maximizar estos ahorros, configure los orígenes de AWS para que solo acepten tráfico de CloudFront. Para S3, utilice Control de acceso de origen (OAC) con buckets privados para conceder acceso a la distribución de CloudFront designada. Para las instancias de equilibrador de carga de aplicación, equilibrador de carga de red y Amazon EC2 en subredes privadas, restrinja el acceso a la distribución de CloudFront designada mediante orígenes de VPC.

Administración de los planes de precios de tarifa fija

Siga estos procedimientos en la consola de CloudFront para suscribir, actualizar, degradar o cancelar un plan de precios para las distribuciones.

Suscripción de una nueva distribución a un plan de precios

Cuando crea una distribución nueva, puede suscribirse a un plan de precios.

Suscripción de una nueva distribución a un plan de precios

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, siga los pasos para crear una distribución.
3. Elija el plan de precios de distribución. Tenga en cuenta que algunas características no están disponibles por nivel del plan de precios. Revise las características de cada plan y elija el plan de precios que necesita para la aplicación.
4. Complete los pasos para crear la distribución.

Suscripción de una distribución existente a un plan de precios

Cuando actualiza una distribución, puede suscribirse a un plan de precios. Antes de elegir un plan de precios, asegúrese de que la configuración de distribución sea compatible con el plan que desee.

> **Tip**
>
> Si la distribución actual utiliza características no compatibles, debe desactivarlas antes de poder suscribirse al plan de precios. Esto incluye desactivar características como Lambda@Edge o los registros de acceso en tiempo real.

Una vez que la configuración de distribución sea compatible, podrá elegir el plan de precios que desee al actualizar una distribución.

Suscripción de una distribución existente a un plan de precios

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, siga los pasos para actualizar una distribución existente.
3. Elija el plan de precios de distribución. Tenga en cuenta que algunas características no están disponibles por nivel del plan de precios. Revise las características de cada plan y elija el plan de precios que necesita para la aplicación.
4. Complete los pasos para actualizar la distribución.

Actualización de un plan de precios

Recomendamos que actualice un plan si se acerca a la asignación de uso mensual o la ha superado, o si quiere habilitar una característica que esté disponible en el siguiente nivel.

Al actualizar a un plan de nivel superior, los cambios surtirán efecto de inmediato. La asignación de precio y uso se prorratea. La distribución y los recursos asociados tendrán acceso a las características disponibles y a la mayor asignación de uso del nuevo plan.

Actualización de un plan de precios

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Elija la distribución que esté suscrita a un plan de precios existente.
4. Siga las instrucciones para actualizar el plan de precios de la distribución.
5. Complete los pasos para actualizar una distribución existente.

Bajada de categoría de un plan de precios

Recomendamos que cambie de categoría a un nivel de plan inferior si no necesita las características adicionales del nivel actual. Por ejemplo, puede bajar de categoría si espera que la aplicación tenga menos tráfico.

Si cambia a un nivel inferior, los cambios en la facturación entrarán en vigor al principio del siguiente ciclo de facturación.

Si la distribución supera actualmente la asignación de uso de un plan, puede bajar de categoría una vez que el uso esté dentro de la asignación de uso del nivel deseado. Para evitar el cobro por el nivel del plan existente en el siguiente ciclo de facturación, baje la categoría antes de que acabe el mes.

Bajada de categoría de un plan de precios

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Elija la distribución que esté suscrita a un plan de precios existente.

4. Siga las instrucciones para bajar la categoría del plan de precios de la distribución. Si tiene características no compatibles, debe eliminar la característica o el recurso de la distribución.
5. Complete los pasos para actualizar una distribución existente.

Cancelación de un plan de precios

Cuando cancela un plan de precios, mantendrá el precio de tarifa fija hasta el final del ciclo de facturación actual. La distribución y todos los recursos del plan asociados pasarán entonces a precios de pago por uso al comienzo del siguiente ciclo de facturación.

Cancelación de un plan de precios

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Elija la distribución que esté suscrita a un plan de precios existente.
4. Siga las instrucciones para cancelar el plan de precios de la distribución. Si tiene características no compatibles, debe eliminar la característica o el recurso de la distribución.
5. Complete los pasos para actualizar una distribución existente.

Cancelación de un cambio de plan pendiente

Si bajó de categoría o canceló el plan de precios de tarifa fija, debe esperar hasta el final del ciclo de facturación actual para que los cambios entren en vigor. Para conservar el plan de precios de tarifa fija actual, volver a actualizarlo o bajarlo de categoría, primero debe cancelar el cambio de plan pendiente.

Cancelación de un cambio de plan de precios pendiente

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Elija la distribución que esté suscrita a un plan de precios existente.
4. Siga las instrucciones para cancelar el cambio del plan pendiente de la distribución.
5. Elija el plan de precios que desee para la distribución.

6. Complete los pasos para actualizar una distribución existente.

Eliminación de una distribución con un plan de precios

No puede eliminar una distribución que esté suscrita a un plan de precios. Primero debe cancelar el plan de precios y, después del ciclo de facturación actual, eliminar la distribución.

Eliminación de una distribución con un plan de precios

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Siga los pasos anteriores para cancelar el plan de precios de la distribución.
4. Siga los pasos para eliminar la distribución.

> **Note**
>
> Puede desactivar una distribución que esté suscrita a un plan de precios, pero seguirá incurriendo en cargos por ese plan. Para dejar de incurrir en cargos por el plan, primero debe cancelarlo.

Permisos

Para ver o administrar las suscripciones de un plan de precios para las distribuciones de CloudFront, debe contar con los permisos necesarios. Para obtener más información, consulte AWSPolítica administrada de : CloudFrontFullAccess y AWSPolítica administrada de : CloudFrontReadOnlyAccess.

Cuotas de planes de precios de tarifa fija

En la siguiente tabla se muestran las cuotas y restricciones para los planes de precios de tarifa fija de CloudFront.

> **Note**
>
> Estas cuotas no se pueden aumentar para la Cuenta de AWS.

Cuotas por cuenta	Cuotas
Planes de precios por Cuenta de AWS	100
Planes gratuitos por Cuenta de AWS	3
Dominios Apex por plan	1

Características no admitidas

Antes de poder asociar una distribución a un plan de precios, debe asegurarse de que determinadas características estén desactivadas y de que se eliminen las asociaciones.

> **Notas**
>
> - Si la distribución o cuenta tiene alguna de estas restricciones, debe resolverla antes de poder usar los planes de precios. Después de realizar los cambios en la distribución, espere a que los cambios se propaguen a todas las ubicaciones periféricas.
> - Debe tener una ACL web de AWS WAF asociada a su distribución si utiliza un plan de precios. Este recurso no puede eliminarse ni disociarse de la distribución a menos que cambie a un precio de pago por uso para esa distribución.

Características no admitidas

No puede suscribir distribuciones a un plan de precios si su configuración contiene las siguientes características no compatibles. Puede desactivar la característica no compatible y usar una opción alternativa o mantener el pago por uso para la distribución.

Características no admitidas	Opciones alternativas	Servicio de AWS
Distribuciones de varios inquilinos	Uso de una distribución estándar o precio de pago por uso	CloudFront
Implementación continua y Distribuciones provisionales	Uso del precio de pago por uso	CloudFront
Configuración de listas de IP de anycast	Uso del precio de pago por uso	CloudFront
Registros de acceso en tiempo real	Uso de registros de acceso estándar o precios de pago por uso	CloudFront
Funciones de Lambda@Edge	Uso de CloudFront Functions o precio de pago por uso	CloudFront
Bots específicos	Uso de bots comunes o precios de pago por uso	AWS WAF
CAPTCHA	Uso de un desafío o precios de pago por uso	AWS WAF
Reglas administradas por los socios	Uso del precio de pago por uso	AWS WAF
Prevención contra fraude en la creación de cuentas	Uso del precio de pago por uso	AWS WAF
Protección contra la apropiación de cuentas	Uso del precio de pago por uso	AWS WAF
Grupos de reglas		AWS WAF

Características no admitidas	Opciones alternativas	Servicio de AWS
	Cree reglas individuales (los grupos de reglas son reglas de AWS WAF compartidas que se pueden aplicar a una ACL web, de forma similar a las políticas de CloudFront)	
Características heredadas		
Configuración de Forwarded Values	Uso de las Políticas de solicitud de origen	CloudFront
IP/SSL dedicadas	Uso del precio de pago por uso	CloudFront
Cifrado por campo	Uso del precio de pago por uso	CloudFront
AWS Identity and Access Management (Certificados de servidor de (IAM	Uso de certificados de AWS Certificate Manager (ACM)	CloudFront
Identidad de acceso de origen (OAI)	Uso del Control de acceso de origen (OAC)	CloudFront
Configuración de la caché antigua	Use políticas de caché y políticas de solicitudes de origen.	CloudFront

Asociaciones no compatibles

No puede suscribir una distribución a un plan de precios si la distribución ya está asociada a alguno de los siguientes recursos que ya están asociados a otras distribuciones. Los recursos que están asociados a una distribución suscrita a un plan de precios solo se pueden usar para esa distribución.

Por ejemplo, si tiene una función de CloudFront que utiliza un almacén de valores clave, ni la función ni el almacén de valores clave se pueden compartir para una distribución que esté incluida en un plan de precios.

- CloudFront Functions
- CloudFront Functions asociadas a un almacén de valores clave
- AWS WAFACL web de

Para suscribir una distribución a un plan de precios, elimine el recurso asociado o sustitúyalo por otro.

Restricciones por cuenta

Las Cuentas de AWS no son elegibles para los planes de precios si cumplen alguna de las siguientes condiciones:

- Ha alcanzado el número máximo de suscripciones permitidas. Consulte Cuotas de planes de precios de tarifa fija.
- La cuenta está utilizando capa gratuita de AWS.

Restricciones por recursos

Las distribuciones no son elegibles para los planes de precios si cumplen alguna de las siguientes condiciones:

- La distribución ha habilitado AWS Shield Advanced
- La distribución ha habilitado el Servicio de Firewall Manager para la ACL web. Firewall Manager no administrará la WebACL de la distribución de CloudFront en un plan de precios.

Características adicionales que pueden afectar al plan de precios

Los planes de precios de tarifa fija permiten pagar una tarifa fija por la distribución de CloudFront y las características mostradas anteriormente, que están incluidas en el plan y asociadas a la distribución de CloudFront. Todas las demás características pueden conllevar cargos adicionales, incluidas, entre otras, las siguientes:

Route 53

- DNSSEC de Route 53 tiene un costo de AWS KMS
- Bloques de IP de Route 53 (CIDR) (los primeros 1000 son gratuitos por Cuenta de AWS)
- Las comprobaciones de estado de Route 53 (los primeros 50 son gratuitos por Cuenta de AWS)

Registro de características

- Registros de consultas de DNS de Route 53, registros de CloudFront Functions y registros de funciones de conexión de CloudFront
- Entrega de registros de AWS WAF en Amazon S3
- Entrega de registros de AWS WAF registros o CloudFront a Amazon Data Firehose
- Métricas de CloudWatch adicionales para CloudFront
- Registros de acceso de CloudFront en formato Parquet

> **Note**
>
> El plan incluye la ingesta de registros de Amazon CloudWatch para los registros estándar (registros de acceso) y los registros WAF de CloudFront sin costo adicional. El plan no cubre todos los demás costos de CloudWatch, como el almacenamiento y las consultas. Todos los demás registros también se facturan de forma independiente.

> **Note**
>
> El plan incluye el DNS público autorizado de Route 53. Cuando la zona alojada de Route 53 esté asociada al plan de precios, el plan cubrirá los costos estándar de la zona alojada, incluida la cuota mensual de la zona alojada, los registros de DNS y las tarifas de consulta de DNS, con sujeción a las asignaciones respectivas por nivel. El plan no cubre todos los demás costos del uso y las características de Route 53 que no se muestren anteriormente y estén incluidos en el plan.

Planes de precios frente a precios de pago por uso

Los planes de tarifa fija y los precios de pago por uso ofrecen diferentes ventajas en función de sus necesidades. Con los planes de tarifa fija, paga un precio que incluye varios Servicios de AWS como CloudFront, AWS WAF, Route 53 y registros de CloudWatch, y nunca se enfrenta a cargos por exceso de tráfico, ni siquiera durante picos de tráfico o ataques.

Con los precios de pago por uso, se le factura de forma independiente por cada servicio y característica en función del uso real. Aunque esto proporciona una flexibilidad total a la hora de seleccionar y configurar los servicios, los costos pueden variar de un mes a otro en función de los patrones de tráfico, por lo que tendrá que supervisar el uso de varios servicios para administrar los costos.

Los planes de tarifa fija son ideales si desea una facturación mensual combinada, una configuración de servicios simplificada y características de seguridad integradas sin tener que preocuparse por los cargos por exceso de uso. Los precios de pago por uso son una mejor opción si necesita tener un control total sobre las características individuales del servicio, las configuraciones personalizadas, el acceso a características que no están disponibles en los planes de tarifa fija o si espera gestionar picos de tráfico grandes y predecibles. Los planes de precios de tarifa fija de Amazon CloudFront no se pueden combinar con ninguna otra oferta, promoción o descuento.

Configuración de distribuciones

Debe crear una distribución de Amazon CloudFront para indicar a CloudFront desde dónde desea enviar el contenido y los detalles acerca de cómo realizar un seguimiento y administrar la entrega de contenido.

Al crear la distribución de CloudFront, CloudFront configura automáticamente gran parte de la configuración de distribución por usted, en función del tipo de origen del contenido. Para obtener más información sobre los ajustes preconfigurados, consulte Referencia de la configuración de distribución preconfigurada. Si lo desea, puede editar manualmente la configuración de la distribución. Para obtener más información, consulte Referencia de toda la configuración de distribución.

Se pueden configurar los siguientes ajustes:

- El origen de contenido: el bucket de Amazon S3, el canal AWS Elemental MediaPackage, el contenedor de AWS Elemental MediaStore, el equilibrador de carga de Elastic Load Balancing o el servidor HTTP desde el que CloudFront obtiene los archivos para distribuir. Puede especificar cualquier combinación de hasta 25 orígenes para una sola distribución.
- Acceso: si desea que los archivos estén disponibles para todos los usuarios o si prefiere restringir el acceso a algunos usuarios.
- Seguridad: si desea habilitar la protección de AWS WAF y exigir a los usuarios que utilicen HTTPS para acceder al contenido. Para las distribuciones de varios inquilinos, solo se admiten listas de control de acceso (ACL) web de AWS WAF V2.
- Clave de caché: qué valores, si los hay, desea incluir en la clave de caché. La clave de caché solo identifica cada archivo en la caché para una distribución determinada.
- Configuración de solicitud de origen: si se desea que CloudFront incluya encabezados HTTP, cookies o cadenas de consulta en las solicitudes que envía a su origen.
- Restricciones geográficas: si desea que CloudFront evite que los usuarios de ciertos países accedan a su contenido.
- Registros: si desea que CloudFront cree registros estándar o registros de acceso en tiempo real que muestren la actividad del espectador.

Para obtener más información, consulte Referencia de toda la configuración de distribución.

Para conocer la cantidad máxima actual de distribuciones que puede crear en cada Cuenta de AWS, consulte Cuotas generales de distribuciones. No hay un número máximo de archivos que se pueden entregar por cada distribución.

Puede utilizar distribuciones para distribuir el siguiente contenido a través de HTTP o HTTPS:

- Contenido estático y dinámico de descarga, como archivos HTML, CSS, JavaScript y de imagen, a través de HTTP o HTTPS.
- Video bajo demanda en distintos formatos, como Apple HTTP Live Streaming (HLS) y Microsoft Smooth Streaming. (Para las distribuciones de varios inquilinos, no se admite Smooth Streaming). Para obtener más información, consulte Distribución de vídeo bajo demanda con CloudFront.
- Un evento en directo, como una reunión, conferencia o concierto, en tiempo real. Para streaming en directo, puede crear la distribución automáticamente con un stack de CloudFormation. Para obtener más información, consulte Distribución de video en streaming con CloudFront y los servicios multimedia de AWS.

En los siguientes temas, se proporciona más información sobre las distribuciones de CloudFront y cómo configurarlas para ajustarse a sus necesidades empresariales. Para obtener más información sobre cómo crear una distribución, consulte Creación de una distribución.

Temas

- Introducción al funcionamiento de las distribuciones de varios inquilinos
- Creación de una distribución
- Referencia de la configuración de distribución preconfigurada
- Referencia de toda la configuración de distribución
- Prueba de una distribución
- Actualizar una distribución
- Etiquetado de una distribución
- Eliminar una distribución
- Uso de varios orígenes con distribuciones de CloudFront
- Habilitación de IPv6 para las distribuciones de CloudFront
- Uso de la implementación continua de CloudFront para probar de forma segura los cambios en la configuración de la CDN
- Uso de URL personalizadas añadiendo nombres de dominio alternativos (CNAME)

- Uso de WebSockets con distribuciones de CloudFront
- Solicitud de direcciones IP estáticas de anycast para utilizarlas en las listas de permitidos
- Uso de gRPC con distribuciones de CloudFront

Introducción al funcionamiento de las distribuciones de varios inquilinos

Puede crear distribuciones de varios inquilinos de CloudFront con configuraciones que se puedan reutilizar en varios inquilinos de distribución. Con una distribución de varios inquilinos, puede hacer que CloudFront configure los ajustes de distribución por usted en función del tipo de origen del contenido. Para obtener más información sobre los ajustes preconfigurados, consulte Referencia de la configuración de distribución preconfigurada.

Entre los beneficios de utilizar una distribución de varios inquilinos en lugar de una distribución estándar se incluyen los siguientes:

- Reducción de la carga operativa.
- Configuraciones reutilizables para que los administradores web y los proveedores de software administren la distribución de CloudFront para varias aplicaciones web que entregan contenido a los usuarios finales.
- Integraciones mejoradas con otros Servicios de AWS para ofrecer una administración de certificados automatizada, controles de seguridad unificados y un control de configuración sencillo y a escala.
- Mantenimiento de patrones de recursos coherentes en todas las implementaciones. Defina la configuración que se debe compartir y, a continuación, especifique las personalizaciones de la configuración que desee invalidar.
- Configuraciones de origen y seguridad personalizables para satisfacer necesidades específicas en nivel de inquilino de distribución.
- Organice los inquilinos de distribución en diferentes niveles. Por ejemplo, si algunos inquilinos de distribución requieren el escudo de origen y otros no, puede agrupar los inquilinos de distribución en distintas distribuciones de varios inquilinos.
- Compartir una configuración de DNS común en varios dominios.

A diferencia de una distribución estándar, no se puede acceder directamente a una distribución de varios inquilinos porque no tiene un punto de conexión de enrutamiento de CloudFront. Por lo tanto, se debe usar junto con un grupo de conexión y uno o más inquilinos de distribución. Aunque las distribuciones estándar tienen su propio punto de conexión de CloudFront y los usuarios finales pueden acceder a ellas directamente, no se pueden utilizar como plantilla para otras distribuciones.

Para obtener información acerca de las cuotas de distribución de varios inquilinos, consulte Cuotas en distribuciones de varios inquilinos.

Temas

- Funcionamiento
- Términos
- Características no admitidas
- Personalizaciones de inquilinos de distribución
- Solicitud de certificados para el inquilino de distribución de CloudFront
- Creación de un grupo de conexiones personalizado (opcional)
- Migración a una distribución de varios inquilinos

Funcionamiento

En una distribución estándar, la distribución contiene todos los ajustes que desea habilitar para su sitio web o aplicación, como las configuraciones de origen, los comportamientos de la memoria caché y los ajustes de seguridad. Si desea crear un sitio web independiente y utilizar muchos de los mismos ajustes, tendrá que crear una nueva distribución cada vez.

Las distribuciones de varios usuarios de CloudFront son diferentes en el sentido de que puede crear una distribución de varios inquilinos inicial. Para cada sitio web nuevo, debe crear un inquilino de distribución que hereda automáticamente los valores definidos de su distribución de origen. A continuación, personaliza la configuración específica del inquilino de distribución.

Descripción general

1. Para empezar, primero debe crear una distribución de varios inquilinos. CloudFront configura los ajustes de distribución automáticamente en función del tipo de origen del contenido. Puede personalizar la configuración de todos los orígenes, excepto los de la VPC. La configuración de orígenes de la VPC se personaliza en el propio recurso de origen de la VPC. Para obtener más

información acerca de la configuración de distribución de varios inquilinos que puede personalizar, consulte Referencia de la configuración de distribución preconfigurada.

- Los inquilinos de la distribución pueden heredar el certificado TLS que utilice para la distribución de varios inquilinos. La distribución de varios usuarios en sí misma no es enrutable, por lo que no tendrá un nombre de dominio asociado.

2. De forma predeterminada, CloudFront crea un grupo de conexiones para usted. El grupo de conexiones controla la forma en que las solicitudes de contenido de los lectores se conectan a CloudFront. Puede personalizar algunos ajustes de enrutamiento en el grupo de conexiones.

   Puede cambiarlo mediante la creación manual del propio grupo de conexiones. Para obtener más información, consulte Creación de un grupo de conexiones personalizado (opcional).

3. A continuación, debe crear uno o varios inquilinos de distribución. El inquilino de distribución es la “puerta principal” para que los lectores accedan al contenido. Cada inquilino de distribución hace referencia a la distribución de varios inquilinos y se asocia automáticamente al grupo de conexiones que CloudFront creó para usted. El inquilino de distribución admite un dominio o subdominio individual.
4. A continuación, puede personalizar algunos ajustes de los inquilinos de distribución, como los dominios personalizados y las rutas de origen. Para obtener más información, consulte Personalizaciones de inquilinos de distribución.
5. Por último, debe actualizar el registro de DNS en el host de DNS para enrutar el tráfico al inquilino de distribución. Para ello, obtenga el valor del punto de conexión de CloudFront del grupo de conexiones y cree un registro de CNAME que apunte al punto de conexión de CloudFront.

Example Ejemplo

El siguiente gráfico muestra cómo una distribución de varios inquilinos, los inquilinos de distribución y los grupos de conexión funcionan juntos para ofrecer contenido a los lectores en varios dominios.

1. La distribución de varios inquilinos define la configuración heredada para cada inquilino de distribución. Se utiliza la distribución de varios inquilinos como plantilla.
2. Cada inquilino de distribución creado a partir de la distribución de varios inquilinos tiene su propio dominio.
3. Los inquilinos de distribución se agregan automáticamente al grupo de conexiones que CloudFront creó para usted al crear la distribución de varios inquilinos. Los grupos de conexiones controlan la forma en que las solicitudes de contenido de los lectores se conectan a la red de CloudFront.

Para obtener instrucciones detalladas sobre la creación de distribuciones de varios inquilinos, consulte Creación de una distribución de CloudFront en la consola.

Términos

Los siguientes conceptos describen los componentes de las distribuciones de varios inquilinos:

Distribución de varios inquilinos

Un esquema de distribución de varios inquilinos que especifica todos los ajustes de configuración compartidos para cualquier inquilino de distribución, incluidos el comportamiento de la caché, las protecciones de seguridad y los orígenes. Las distribuciones de varios inquilinos no pueden atender el tráfico directamente. Se deben usar junto con grupos de conexión e inquilinos de distribución.

Distribución estándar

Una distribución que no tiene funcionalidad de varios inquilinos. Estas distribuciones son las mejores para admitir sitios web o aplicaciones individuales.

Inquilino de distribución

Un inquilino de distribución hereda la configuración de distribución de varios inquilinos. Algunos ajustes de configuración se pueden personalizar en nivel de inquilino de distribución. El inquilino de distribución debe tener un certificado TLS válido, que se puede heredar de la distribución de varios inquilinos siempre que cubra el dominio o subdominio del inquilino de distribución.

El inquilino de distribución debe estar asociado a un grupo de conexiones. CloudFront crea un grupo de conexiones para usted al crear un inquilino de distribución y asigna automáticamente los inquilinos de distribución a ese grupo de conexiones.

Tenencia múltiple

Puede usar la distribución de varios inquilinos para ofrecer contenido en varios dominios y, al mismo tiempo, compartir la configuración y la infraestructura. Este enfoque permite que los diferentes dominios (denominados inquilinos) compartan configuraciones comunes de la distribución de varios inquilinos y, al mismo tiempo, mantengan sus propias personalizaciones.

Grupos de conexiones

Proporciona el punto de conexión de enrutamiento de CloudFront que sirve contenido a los lectores. Debe asociar cada inquilino de distribución a un grupo de conexiones para obtener el punto de conexión de enrutamiento de CloudFront correspondiente para el registro de CNAME que cree para su dominio o subdominio del inquilino de distribución. Los grupos de conexiones se pueden compartir entre varios inquilinos de distribución. Los grupos de conexiones administran la configuración de enrutamiento para los inquilinos de distribución, como la configuración de las listas de IP de IPv6 y Anycast.

Parameters

Una lista de pares clave-valor para valores de marcador de posición, como rutas de origen y nombres de dominio. Puede definir parámetros en la distribución de varios inquilinos y proporcionar valores para esos parámetros en el nivel de inquilino de distribución. Usted elige si es necesario ingresar los valores de los parámetros para el inquilino de distribución.

Si no proporciona un valor para un parámetro opcional en un inquilino de distribución, se utilizará como valor el valor predeterminado de la distribución de varios inquilinos.

Punto de conexión de enrutamiento de CloudFront

DNS canónico para el grupo de conexiones, como `d123.cloudfront.net`. Se utiliza en el registro CNAME del dominio o subdominio de inquilino de distribución.

Personalizaciones

Puede personalizar los inquilinos de distribución para que usen configuraciones diferentes a las de la distribución de varios inquilinos. Para cada inquilino de distribución, puede especificar una lista de control de acceso (ACL) web de AWS WAF, certificados TLS y restricciones geográficas diferentes.

Características no admitidas

Las siguientes características no se pueden usar con una distribución de varios inquilinos. Si desea crear una nueva distribución de varios inquilinos con la misma configuración que la distribución estándar, tenga en cuenta que algunas configuraciones no están disponibles.

> **Notas**
>
> - Actualmente, las políticas de AWS Firewall Manager solo se aplican a las distribuciones estándar. Firewall Manager agregará compatibilidad con distribuciones de varios inquilinos en una versión futura.
> - A diferencia de las distribuciones estándar, usted especifica el nombre de dominio (alias) en el nivel de inquilino de distribución. Para obtener más información, consulte Solicitud de certificados para el inquilino de distribución de CloudFront y la operación de la API CreateDistributionTenant.

- Implementación continua
- Identidad de acceso de origen (OAI): utilice el control de acceso de origen (OAC) en su lugar.
- Soporte SSL personalizado con IP dedicada: solo se admite el método `sni-only`.
- ACL web clásica (V1) de AWS WAF: solo se admiten las ACL web de AWS WAF V2.
- Registro estándar (heredado)
- Tiempo de vida mínimo
- Tiempo de vida predeterminado
- Tiempo de vida máximo
- ForwardedValues
- PriceClass
- Firmantes de confianza

- Smooth Streaming
- AWS Identity and Access Management (Certificados de servidor de (IAM
- Direcciones IP dedicadas
- Versión mínima de protocolo SSLv3

Los siguientes ajustes no se pueden configurar en una distribución de varios inquilinos o inquilino de distribución. En su lugar, debe establecer los valores que desee en un grupo de conexión. Todos los inquilinos de distribución asociados al grupo de conexión utilizarán esta configuración. Para obtener más información, consulte Creación de un grupo de conexiones personalizado (opcional).

- Habilitación de IPv6 (solicitudes de espectadores)
- Lista de direcciones IP estáticas de Anycast

Personalizaciones de inquilinos de distribución

Cuando se utiliza una distribución de varios inquilinos, los inquilinos de la distribución heredan la configuración de distribución de varios inquilinos. Sin embargo, puede personalizar algunos ajustes en el nivel de inquilino de distribución.

Puede personalizar lo siguiente:

- Parámetros: los parámetros son pares clave-valor que se pueden utilizar para el dominio de origen o las rutas de origen. Consulte Funcionamiento de los parámetros con los inquilinos de distribución.
- ACL web de AWS WAF (V2): puede especificar una ACL web independiente para el inquilino de distribución, que invalidará la ACL web utilizada para la distribución de varios inquilinos. También puede desactivar esta configuración para un inquilino de distribución específico, lo que significa que el inquilino de distribución no heredará las protecciones de ACL web de la distribución de varios inquilinos. Para obtener más información, consulte ACL web de AWS WAF.
- Restricciones geográficas: las restricciones geográficas que especifique para un inquilino de distribución invalidarán cualquier restricción geográfica para la distribución de varios inquilinos. Por ejemplo, si bloquea Alemania (DE) en la distribución de varios inquilinos, todos los inquilinos de distribución asociados también bloquearán DE. Sin embargo, si permite DE para un inquilino de distribución específico, la configuración de ese inquilino de distribución invalidará la configuración de la distribución de varios inquilinos. Para obtener más información, consulte Restricción de la distribución geográfica de su contenido.

- Rutas de invalidación: especifique las rutas de archivo del contenido que desea invalidar para el inquilino de distribución. Para obtener más información, consulte Invalidación de archivos.
- Certificados TLS personalizados: los certificados de AWS Certificate Manager (ACM) que especifique para los inquilinos de distribución son complementarios al certificado proporcionado en la distribución de varios inquilinos. Sin embargo, si el certificado de distribución de varios inquilinos y el certificado de inquilino de distribución cubren el mismo dominio, se utilizará el certificado de inquilino. Para obtener más información, consulte Solicitud de certificados para el inquilino de distribución de CloudFront.
- Nombres de dominio: debe especificar al menos un nombre de dominio por inquilino de distribución.

Funcionamiento de los parámetros con los inquilinos de distribución

Un parámetro es un par clave-valor que puede utilizar como valores de marcador de posición. Defina los parámetros que desee usar en la distribución de varios inquilinos y especifique si son obligatorios.

Al definir los parámetros en la distribución de varios inquilinos, se decide si es necesario ingresar dichos parámetros en el nivel de inquilino de distribución.

- Si define los parámetros según sea necesario en la distribución de varios inquilinos, deben ingresarse en el nivel de inquilino de distribución. (No se heredan).
- Si los parámetros no son necesarios, puede proporcionar un valor predeterminado en la distribución multiusuario que herede el inquilino de distribución.

Puede utilizar parámetros en las siguientes propiedades:

- Nombre de dominio de origen
- Ruta de origen

En la distribución de varios inquilinos, puede definir hasta dos parámetros para cada una de las propiedades anteriores.

Parámetros de ejemplo

Consulte los siguientes ejemplos a fin de utilizar parámetros para el nombre de dominio y la ruta de origen.

Parámetros de nombre de dominio

En la configuración de distribución de varios inquilinos, puede definir un parámetro para el nombre de dominio de origen como en los siguientes ejemplos:

Amazon S3

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

Orígenes personalizados

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

Al crear un inquilino de distribución, especifique el valor que se utilizará para *parameter1*.

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

Según los ejemplos anteriores especificados en la distribución de varios inquilinos, el nombre de dominio de origen para el inquilino de distribución se resuelve de la siguiente manera:

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

Parámetros de ruta de origen

Del mismo modo, puede definir parámetros para la ruta de origen en la distribución de varios inquilinos como en los siguientes ejemplos:

- `/{{parameter2}}`

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

Al crear un inquilino de distribución, especifique el valor que se utilizará para *parameter2*.

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

Según los ejemplos anteriores especificados en la distribución de varios inquilinos, la ruta de origen para el inquilino de distribución se resuelve de la siguiente manera:

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

Example Ejemplo

Desea crear varios sitios web (inquilinos) para los clientes y debe asegurarse de que cada recurso de inquilino de distribución utilice los valores correctos.

1. Crea una distribución de varios inquilinos e incluye dos parámetros para la configuración del inquilino de distribución.
2. Para el nombre de dominio de origen, crea un parámetro denominado *customer-name* y especifica que es obligatorio. Introduce el parámetro antes del bucket de S3, de modo que aparezca como:

   {{*customer-name*}}.amzn-s3-demo-bucket3.s3.us-east-1.amazonaws.com.
3. Para la ruta de origen, crea un segundo parámetro denominado *my-theme* y especifica que es opcional, con el valor predeterminado de *basic*. La ruta de origen aparece como /{{*my-theme*}}

4. Al crear un inquilino de distribución:
   - En el nombre de dominio, debe especificar un valor para `customer-name`, ya que está marcado como obligatorio en la distribución de varios inquilinos.
   - Para la ruta de origen, puede especificar opcionalmente un valor para `my-theme` o utilizar el valor predeterminado.

Solicitud de certificados para el inquilino de distribución de CloudFront

Cuando crea un inquilino de distribución, el inquilino hereda el certificado compartido de AWS Certificate Manager (ACM) de la distribución de varios inquilinos. Este certificado compartido proporciona HTTPS para todos los inquilinos asociados a la distribución de varios inquilinos.

Al crear o actualizar un inquilino de distribución de CloudFront para agregar dominios, puede agregar un certificado de CloudFront administrado desde ACM. A continuación, CloudFront obtiene un certificado validado por HTTP de ACM en su nombre. Puede usar este certificado de ACM en el nivel de inquilino para configuraciones de dominio personalizadas. CloudFront optimiza el flujo de trabajo de renovación para ayudar a mantener los certificados actualizados y garantizar la entrega de contenido sin interrupciones.

> **Note**
>
> Posee el certificado, pero solo se puede usar con los recursos de CloudFront y la clave privada no se puede exportar.

Puede solicitar el certificado al crear o actualizar el inquilino de distribución.

Temas

- Agregación de un dominio y un certificado (inquilino de distribución)
- Configuración completa de dominio
- Dirección de dominios a CloudFront
- Consideraciones sobre el dominio (inquilino de distribución)
- Dominios comodín (inquilino de distribución)

Agregación de un dominio y un certificado (inquilino de distribución)

El siguiente procedimiento muestra cómo agregar un dominio y actualizar el certificado de un inquilino de distribución.

Agregación de un dominio y un certificado (inquilino de distribución)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En SaaS, elija Inquilinos de distribución.
3. Busque el inquilino de distribución. Utilice el menú desplegable de la barra de búsqueda para filtrar por dominio, nombre, ID de distribución, ID de certificado, ID de grupo de conexión o ID de ACL web.
4. Elija el nombre del inquilino de la distribución.
5. En Dominios, elija Administrar dominio.
6. En Certificado, elija si desea un certificado TLS personalizado para el inquilino de distribución. El certificado verifica si está autorizado a usar el nombre de dominio. El certificado debe existir en la región Este de EE. UU. (Norte de Virginia).
7. En Dominios, elija Agregar dominio e ingrese el nombre de dominio. Según el dominio, los siguientes mensajes aparecerán bajo el nombre de dominio que ingrese.
   - Este dominio está cubierto por el certificado.
   - Este dominio está cubierto por el certificado, pendiente de validación.
   - Este dominio está cubierto por el certificado. (Esto significa que debe verificar la propiedad del dominio).
8. Elija Actualizar inquilino de distribución.

   En la página de detalles del inquilino, en Dominios, puede ver los siguientes campos:

   - Propiedad del dominio: el estado de la propiedad del dominio. Antes de que CloudFront pueda ofrecer contenido, se debe verificar la propiedad del dominio mediante la validación del certificado TLS.
   - Estado de DNS: los registros de DNS del dominio deben apuntar a CloudFront para enrutar el tráfico correctamente.

9. Si no se ha verificado la propiedad del dominio, en la página de detalles del inquilino, en Dominios, elija Configuración completa del dominio y, a continuación, complete el siguiente procedimiento para apuntar el registro de DNS al nombre de dominio de CloudFront.

Configuración completa de dominio

Siga estos procedimientos para verificar que posee el dominio de los inquilinos de distribución. En función del dominio, elija uno de los procedimientos siguientes.

> **Note**
>
> Si el dominio ya apunta a CloudFront con un registro de alias de Amazon Route 53, debe agregar el registro TXT de DNS con `_cf-challenge.` delante del nombre de dominio. Este registro TXT verifica que el nombre de dominio esté vinculado a CloudFront. Repita este paso para cada dominio. A continuación, se muestra cómo actualizar el registro de TXT:
>
> - Nombre del registro: `_cf-challenge.`*`DomainName`*
> - Tipo del registro: `TXT`
> - Valor del registro: *`CloudFrontRoutingEndpoint`*
>
> Por ejemplo, el registro de TXT podría tener un aspecto similar al siguiente: `_cf-challenge.example.com TXT d111111abcdef8.cloudfront.net`
> Puede encontrar el punto de conexión de enrutamiento de CloudFront en la consola, en la página de detalles del arrendatario de distribución, o utilizar la acción de la API ListConnectionGroups en la Referencia de la API de Amazon CloudFront para encontrarlo.

> **Tip**
>
> Si es proveedor de SaaS y desea permitir la emisión de certificados sin necesidad de que los clientes (inquilinos) agreguen un registro TXT directamente al DNS, haga lo siguiente:
>
> 1. Si es propietario del dominio `example-saas-provider.com`, asigne subdominios a los inquilinos, como `customer-123.example-saas-provider.com`
> 2. En el DNS, agregue el registro TXT `_cf-challenge.customer-123.example-saas-provider.com TXT d111111abcdef8.cloudfront.net` a la configuración de DNS.

3. A continuación, los clientes (los inquilinos) pueden actualizar el registro de DNS propio para asignar el nombre de dominio al subdominio que ha proporcionado usted.

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

I have existing traffic

Seleccione esta opción si el dominio no puede tolerar el tiempo de inactividad. Debe tener acceso al servidor web o de origen. Utilice el siguiente procedimiento para validar la propiedad del dominio.

Cómo completar la configuración del dominio cuando hay tráfico

1. En Especificar el tráfico web, elija Tengo tráfico existente y, a continuación, elija Siguiente.
2. En Verificar la propiedad del dominio, elija una de las siguientes opciones:

   - Utilizar certificado existente: busque un certificado de ACM existente o ingrese el ARN del certificado que cubre los dominios mostrados.
   - Carga manual de archivos: elija esta opción si tiene acceso directo para cargar archivos al servidor web.

     Para cada dominio, cree un archivo de texto sin formato que contenga el token de validación desde la ubicación del token y cárguelo en el origen en la ruta de archivo especificada en el servidor actual. La ruta a este archivo podría tener un aspecto similar al siguiente: `/.well-known/pki-validation/acm_9c2a7b2ec0524d09fa6013efb73ad123.txt`. Tras completar ese paso, ACM verifica el token y, a continuación, emite el certificado TLS para el dominio.
   - Redirección HTTP: elija si no tiene acceso directo para cargar archivos al servidor web o si utiliza una CDN o un servicio proxy.

     Para cada dominio, se crea una redirección 301 en el servidor actual. Copie la ruta conocida en Redirigir desde y diríjala al punto de conexión del certificado especificado en Redirigir a. La redirección podría tener un aspecto similar al siguiente:

     ```
     If the URL matches: example.com/.well-known/pki-validation/
     leabe938a4fe077b31e1ff62b781c123.txt
     Then the settings are:Forwarding URL
     ```

```
Then 301 Permanent Redirect:To validation.us-east-1.acm-
validations.aws/123456789012/.well-known/pki-validation/
leabe938a4fe077b31e1ff62b781c123.txt
```

> **Note**
>
> Puede elegir Comprobar el estado del certificado para verificar cuándo ACM emite el certificado para el dominio.

3. Elija Siguiente.
4. Complete los pasos para Dirección de dominios a CloudFront.

I don't have traffic

Seleccione esta opción si va a agregar dominios nuevos. CloudFront administrará la validación de los certificados por usted.

Cómo completar la configuración del dominio si no tiene tráfico

1. En Especificar el tráfico web, elija Aún no tengo tráfico.
2. Para cada nombre de dominio, complete los pasos de Dirección de dominios a CloudFront.
3. Después de actualizar los registros de DNS de cada nombre de dominio, elija Siguiente.
4. Espere a que se emita el certificado.

> **Note**
>
> Puede elegir Comprobar el estado del certificado para verificar cuándo ACM emite el certificado para el dominio.

5. Elija Enviar.

Dirección de dominios a CloudFront

Actualice los registros de DNS para dirigir el tráfico de cada dominio al punto de conexión de enrutamiento de CloudFront. Puede tener varios nombres de dominio, pero todos deben resolverse a este punto de conexión.

Dirección de dominios a CloudFront

1. Copie el valor del punto de conexión de enrutamiento de CloudFront, como d111111abcdef8.cloudfront.net.
2. Actualice los registros de DNS para dirigir el tráfico de cada dominio al punto de conexión de enrutamiento de CloudFront.
   1. Inicie sesión en el registrador de dominios o en la consola de administración del proveedor de DNS.
   2. Vaya a la sección de administración de DNS del dominio.
      - Para subdominios: cree un registro CNAME. Por ejemplo:
        - Nombre: el subdominio (como `www` o `app`)
        - Valor/objetivo: el punto de conexión de enrutamiento de CloudFront
        - Tipo de registro: CNAME
        - TTL: 3600 (o lo que sea adecuado para el caso de uso)
      - Para dominios de vértice/raíz: esto requiere una configuración de DNS única, ya que los registros CNAME estándar no se pueden utilizar en el dominio raíz o de vértice. Como la mayoría de los proveedores de DNS no admiten los registros ALIAS, recomendamos crear un registro ALIAS en Route 53. Por ejemplo:
        - Nombre: el dominio de apex (por ejemplo, `example.com`)
        - Tipo de registro: A
        - Alias: sí
        - Destino de alias: el punto de conexión de enrutamiento de CloudFront
        - Política de enrutamiento: simple (o lo que sea apropiado para el caso de uso)
   3. Compruebe que el cambio de DNS se haya propagado. (Esto suele ocurrir cuando caduca TTL. A veces puede tardar entre 24 y 48 horas). Use una herramienta como `dig` o `nslookup`.

      ```
      dig www.example.com
      # Should eventually return a CNAME pointing to your CloudFront routing endpoint
      ```
3. Vuelva a la consola de CloudFront y elija Enviar. Cuando el dominio está activo, CloudFront actualiza el estado del dominio para indicar que el dominio está listo para atender el tráfico.

Para obtener más información, consulte la documentación del proveedor de DNS:

- Cloudflare
- ClouDNS
- DNSimple
- Gandi.net
- GoDaddy
- Google Cloud DNS
- Namecheap

Consideraciones sobre el dominio (inquilino de distribución)

Cuando un dominio está activo, se ha establecido el control del dominio y CloudFront responderá a todas las solicitudes de los lectores a este dominio. Una vez activado, un dominio no se puede desactivar ni cambiar a un estado inactivo. El dominio no se puede asociar a otro recurso de CloudFront mientras ya esté en uso. Para asociar el dominio a otra distribución, utilice la solicitud UpdateDomainAssociation para mover el dominio de un recurso de CloudFront a otro.

Cuando un dominio está inactivo, CloudFront no responderá a las solicitudes de los lectores al dominio. Mientras el dominio esté inactivo, tenga en cuenta lo siguiente:

- Si tiene una solicitud de certificado pendiente, CloudFront responderá a las solicitudes de la ruta conocida. Mientras la solicitud esté pendiente, el dominio no se puede asociar a ningún otro recurso de CloudFront.
- Si no tiene una solicitud de certificado pendiente, CloudFront no responderá a las solicitudes del dominio. Puede asociar el dominio a otros recursos de CloudFront.
- Solo puede tener una solicitud de certificado pendiente por inquilino de distribución. Antes de poder solicitar otro certificado para dominios adicionales, debe cancelar la solicitud pendiente existente. Cancelar una solicitud de certificado existente no elimina el certificado de ACM asociado. Puede eliminarlo mediante la API de ACM.
- Si aplica un nuevo certificado al inquilino de la distribución, se desasociará el certificado anterior. Puede reutilizar el certificado para cubrir el dominio de otro inquilino de distribución.

Al igual que ocurre con las renovaciones de certificados validados por DNS, se le notificará cuando la renovación del certificado se realice correctamente. Sin embargo, no tiene que hacer nada. CloudFront administrará automáticamente la renovación del certificado del dominio.

> **Note**
>
> No necesita llamar a las operaciones de la API de ACM para crear o actualizar los recursos de certificados. Puede administrar los certificados mediante las operaciones de la API CreateDistributionTenant y UpdateDistributionTenant para especificar los detalles de la solicitud de certificado administrado.

Dominios comodín (inquilino de distribución)

Los dominios comodín se admiten con los inquilinos de distribución en las siguientes situaciones:

- Cuando el comodín se incluye en el certificado compartido que se hereda de la distribución principal de varios inquilinos
- Cuando utiliza un certificado TLS personalizado existente y válido para el inquilino de distribución

Creación de un grupo de conexiones personalizado (opcional)

De forma predeterminada, CloudFront crea un grupo de conexiones para usted cuando crea una distribución de varios inquilinos. El grupo de conexiones controla la forma en que las solicitudes de contenido de los lectores se conectan a CloudFront.

Se recomienda usar el grupo de conexión predeterminado. Sin embargo, si necesita aislar aplicaciones empresariales o administrar grupos de inquilinos de distribución de forma independiente, puede optar por crear un grupo de conexiones personalizado. Por ejemplo, es posible que necesite mover un inquilino de distribución a un grupo de conexiones independiente si sufre un ataque DDoS. De esta forma, puede proteger a otros inquilinos de la distribución del impacto.

Creación de un grupo de conexiones personalizado (opcional)

Si lo desea, tiene la opción de elegir crear un grupo de conexiones personalizado para los inquilinos de distribución.

Creación de un grupo de conexiones personalizado (opcional)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, seleccione Configuración.

3. Active la configuración del Grupo de conexiones.
4. En el panel de navegación, elija Grupos de conexiones y, a continuación, elija Crear grupo de conexión.
5. En Nombre del grupo de conexiones, escriba un nombre para el grupo de conexiones. No puede actualizar este nombre después de haber creado el grupo de conexiones.
6. Para IPv6, especifique si desea habilitar este protocolo IP. Para obtener más información, consulte Habilitación de IPv6 (solicitudes de espectadores).
7. Para la lista de IP estáticas de Anycast, especifique si desea entregar tráfico a los inquilinos de distribución desde un conjunto de direcciones IP. Para obtener más información, consulte Lista de IP estática de Anycast.
8. (Opcional) Agregue etiquetas al grupo de conexiones.
9. Elija Crear grupo de conexiones.

Cuando se crea el grupo de conexiones, puede encontrar la configuración que especificó, así como el ARN y el punto de conexión.

- El ARN tiene el aspecto del siguiente ejemplo: `arn:aws:cloudfront::123456789012:connection-group/cg_2uVbA9KeWaADTbKzhj9lcKDoM25`
- El punto de conexión tiene el aspecto del siguiente ejemplo: d111111abcdef8.cloudfront.net

Puede editar o eliminar un grupo de conexión personalizado una vez que lo haya creado. Antes de eliminar un grupo de conexión, primero debe eliminar todos los inquilinos de distribución asociados. No puede eliminar el grupo de conexiones predeterminado que CloudFront creó para usted cuando creó la distribución de varios inquilinos.

> **Important**
>
> Si cambia el grupo de conexiones de un inquilino de distribución, CloudFront seguirá transportando tráfico para el inquilino de distribución, pero con una mayor latencia. Le recomendamos que actualice el registro de DNS del inquilino de distribución para que utilice el punto de conexión de enrutamiento de CloudFront del nuevo grupo de conexiones. Hasta que actualice el registro de DNS, CloudFront enrutará en función de la configuración definida para el punto de conexión de enrutamiento al que apunta actualmente el sitio web con DNS. Por ejemplo, supongamos que el grupo de conexiones predeterminado no

usa direcciones IP estáticas de Anycast, pero sí lo hace el nuevo grupo de conexiones personalizado. Debe actualizar el registro de DNS antes de que CloudFront utilice las IP estáticas de Anycast para los inquilinos de distribución del grupo de conexiones personalizado.

Migración a una distribución de varios inquilinos

Si tiene una distribución estándar de CloudFront y desea migrar a una distribución de varios inquilinos, siga estos pasos.

Migración de una distribución estándar a una distribución de varios inquilinos

1. Consulte el Características no admitidas.
2. Cree una distribución de varios inquilinos con la misma configuración que la distribución estándar, menos las características no compatibles. Para obtener más información, consulte Creación de una distribución de CloudFront en la consola.
3. Cree un inquilino de distribución y agregue un nombre de dominio alternativo que le pertenezca.

   > **Warning**
   >
   > No utilice el nombre de dominio actual que está asociado a la distribución estándar. Agregue un dominio de marcador de posición en su lugar. Trasladará el dominio más adelante. Para obtener más información sobre cómo crear un inquilino de distribución, consulte Creación de una distribución de CloudFront en la consola.

4. Proporcione un certificado existente para el dominio del inquilino de distribución. Este es el certificado que cubrirá el dominio de marcador de posición y el dominio que desea mover.
5. Copie el punto de conexión de enrutamiento de CloudFront desde la página de detalles del inquilino de distribución en la consola. Otra opción, encuéntrelo mediante la acción de la API ListConnectionGroups en la Referencia de la API de Amazon CloudFront.
6. Para verificar la propiedad del dominio, cree un registro TXT DCV con un prefijo de guion bajo (_) que apunte al punto de conexión de enrutamiento de CloudFront para el inquilino de distribución. Para obtener más información, consulte Dirección de dominios a CloudFront.
7. Cuando los cambios se hayan propagado, actualice el inquilino de la distribución para que utilice el dominio que utilizó anteriormente para la distribución estándar.

- Consola: para obtener instrucciones detalladas, consulte Agregación de un dominio y un certificado (inquilino de distribución).
- API: utilice la acción de la API UpdateDomainAssociation en la Referencia de la API de Amazon CloudFront.

> **Important**
>
> Esto restablece la clave de la caché del contenido. Después de esto, CloudFront comienza a almacenar en caché su contenido mediante la nueva clave de la caché. Para obtener más información, consulte Descripción de la clave de caché.

8. Actualice el registro de DNS para que apunte el dominio al punto de conexión de enrutamiento de CloudFront para el inquilino de distribución. Una vez completado este paso, el dominio estará listo para servir tráfico al inquilino de distribución. Para obtener más información, consulte Dirección de dominios a CloudFront.
9. (Opcional) Después de migrar correctamente el dominio a un inquilino de distribución, puede utilizar un certificado administrado por CloudFront diferente que cubra el nombre de dominio del inquilino de distribución. Para solicitar un certificado administrado, cree un registro TXT independiente para emitir el certificado y siga los pasos que se indican en Configuración completa de dominio.

Creación de una distribución

Este tema explica cómo usar la consola de CloudFront para crear una distribución.

Descripción general

1. Cree uno o más buckets de Amazon S3 o configure servidores HTTP como servidores de origen. Un origen es la ubicación en la que se almacena la versión original del contenido. Cuando CloudFront recibe una solicitud de archivos, se dirige al origen para obtener los archivos que distribuye en ubicaciones de borde. Puede utilizar cualquier combinación de buckets de Amazon S3 y servidores HTTP en sus servidores de origen.
   - Si utiliza Amazon S3, el nombre de su bucket debe estar todo en minúscula y no puede contener espacios.

- Si utiliza un servidor de Amazon EC2 u otro origen personalizado, revise Uso de Amazon EC2 (u otro origen personalizado).
- Para obtener información sobre el número máximo actual de orígenes que puede crear para una distribución o para solicitar una cuota más alta, consulte Cuotas generales de distribuciones.

2. Cargue el contenido en sus servidores de origen. Debe hacer que sus objetos se puedan leer públicamente, o puede usar URL firmadas por CloudFront para restringir el acceso a su contenido.

> **Important**
>
> Usted es responsable de garantizar la seguridad de su servidor de origen. Debe asegurarse de que CloudFront tenga permiso para obtener acceso al servidor y que la configuración de seguridad proteja su contenido.

3. Cree su distribución de CloudFront:
   - Para obtener un procedimiento detallado de creación de una distribución en la consola de CloudFront, consulte Creación de una distribución de CloudFront en la consola.
   - Para obtener información sobre cómo crear una distribución mediante la API de CloudFront, consulte CreateDistribution en la Referencia de la API de Amazon CloudFront.
4. (Opcional) Si utilizó la consola de CloudFront para crear su distribución, cree más comportamientos de la caché u orígenes para la distribución. Para obtener más información sobre comportamientos y orígenes, consulte Actualización de una distribución de varios inquilinos.
5. Pruebe su distribución. Para obtener más información acerca las pruebas, consulte Prueba de una distribución.
6. Desarrolle el sitio web o aplicación para obtener acceso al contenido utilizando el nombre de dominio que CloudFront devolvió después de creada la distribución en el paso 3. Por ejemplo, si CloudFront devuelve d111111abcdef8.cloudfront.net como nombre de dominio para su distribución, la dirección URL del archivo `image.jpg` en un bucket de Amazon S3 o en el directorio raíz de un servidor HTTP es `https://d111111abcdef8.cloudfront.net/image.jpg`.

Si especificó uno o varios nombres de dominio alternativo (CNAME) al crear la distribución, puede utilizar su propio nombre de dominio. En ese caso, la URL para `image.jpg` sería `https://www.example.com/image.jpg`.

Tenga en cuenta lo siguiente:

- Si desea utilizar URL firmadas para restringir el acceso a su contenido, consulte Distribución de contenido privado con URL firmadas y cookies firmadas.
- Si desea ofrecer contenido comprimido, consulte Ofrecimiento de archivos comprimidos.
- Para obtener información sobre el comportamiento de respuesta y solicitud de CloudFront para Amazon S3 y orígenes personalizados, consulte Comportamiento de solicitudes y respuestas.

Temas

- Creación de una distribución de CloudFront en la consola
- Valores que CloudFront muestra en la consola
- Enlaces adicionales
- Adición de un dominio a la distribución estándar de CloudFront

Creación de una distribución de CloudFront en la consola

Al crear una distribución, CloudFront configura las opciones de la distribución por usted, en función del tipo de origen del contenido. Para obtener más información sobre los ajustes preconfigurados, consulte Referencia de la configuración de distribución preconfigurada. También puede crear distribuciones de varios inquilinos con una configuración que se puede reutilizar en varios inquilinos de distribución. Para obtener más información, consulte Introducción al funcionamiento de las distribuciones de varios inquilinos. De forma alternativa, puede configurar manualmente las opciones de distribución propias.

Multi-tenant

Creación de una distribución de varios inquilinos

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, elija Crear distribución.

3. Elija Arquitectura de varios inquilinos, Siguiente.
4. Ingrese un Nombre de distribución para la distribución de varios inquilinos. El nombre aparecerá como el valor de la clave `Name`. Puede cambiar este valor posteriormente. Puede agregar hasta 50 etiquetas a la distribución de varios inquilinos. Para obtener más información, consulte Etiquetado de una distribución .
5. (Opcional) Para Certificado comodín, elija el certificado de AWS Certificate Manager (ACM) que cubrirá todos los subdominios del dominio raíz, como `*.example.com`. El certificado debe estar en la región Este de EE. UU. (Norte de Virginia).
6. Elija Siguiente.
7. En la página Especificar el origen, seleccione el tipo de origen del que CloudFront obtendrá el contenido. CloudFront utilizará la configuración recomendada para ese tipo de origen para la distribución de varios inquilinos. Para obtener más información sobre los ajustes recomendados, consulte Referencia de la configuración de distribución preconfigurada.
8. En Origen, bajo el tipo de origen que haya seleccionado, elija o ingrese el origen que desee utilizar.
9. En Ruta de origen, ingrese el carácter de barra diagonal (`/`) seguido de la ruta de origen.
10. (Opcional) Para agregar un parámetro, elija Insertar parámetro para el nombre de dominio de origen o la ruta de origen. Puede ingresar hasta dos parámetros para cada campo.
    a. Elija Crear nuevo parámetro.
    b. En el cuadro de diálogo Crear nuevo parámetro, en Nombre del parámetro, ingrese un nombre único para el parámetro y, opcionalmente, una descripción.
    c. En Parámetro obligatorio, marque la casilla de verificación para hacer que el valor de este parámetro sea obligatorio en el nivel de inquilino de distribución. Si no es obligatorio, ingrese un Valor predeterminado que heredará el inquilino de distribución.
    d. Elija Create parameter. Este parámetro aparece en el campo correspondiente.
11. En Opciones, elija una de las siguientes opciones:
    - Usar configuración de origen recomendada: utilice la configuración predeterminada recomendada de caché y origen para el tipo de origen que haya seleccionado.
    - Personalizar la configuración de origen: personalice la caché y la configuración de origen. Si elige esta opción, debe especificar sus propios valores que aparecen.
12. Elija Siguiente.

13. En la página Habilitar las protecciones de seguridad, elija si desea habilitar las protecciones de seguridad de AWS WAF. Más adelante, puede personalizar la ACL web para inquilinos de distribución específicos. Para obtener más información, consulte Habilitación de AWS WAF para una nueva distribución.
14. Elija Siguiente, Crear distribución.
15. En la página Distribuciones, la distribución de varios inquilinos aparece en la lista de recursos. Puede elegir el menú desplegable Todas las distribuciones para filtrar por distribución estándar o distribución de varios inquilinos. También puede elegir la columna Tipo para filtrar por distribución estándar o de varios inquilinos.

De forma predeterminada, CloudFront crea un grupo de conexiones para usted. El grupo de conexiones controla la forma en que las solicitudes de contenido de los lectores se conectan a CloudFront. Puede personalizar algunos ajustes de enrutamiento en el grupo de conexiones. Para obtener más información, consulte Introducción al funcionamiento de las distribuciones de varios inquilinos.

Puede crear inquilinos de distribución adicionales mediante la distribución de varios inquilinos como plantilla.

Creación de un inquilino de distribución

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, lleve a cabo alguna de las siguientes acciones:
   - Elija Distribuciones, elija una distribución de varios inquilinos y, a continuación, elija Crear inquilino.
   - Elija Inquilinos de distribución y, a continuación, elija Crear inquilino.
3. En Nombre de inquilino de distribución, ingrese el nombre. El nombre debe ser único en la Cuenta de AWS y no se puede cambiar después de crearlo.
4. En Distribución de plantilla, elija un ID de distribución de varios inquilinos de la lista.
5. En Administrar etiquetas, agregue hasta 50 pares clave-valor para el inquilino de distribución. Para obtener más información, consulte Etiquetado de una distribución.
6. Elija Siguiente.
7. En la página Agregar dominios, en Certificado, elija si desea un Certificado TLS personalizado para el inquilino de distribución. El certificado verifica si está autorizado a

usar el nombre de dominio. El certificado debe existir en la región Este de EE. UU. (Norte de Virginia).

8. En Dominios, escriba el nombre del dominio.

> **Note**
>
> Si ha ingresado un nombre de dominio que no está cubierto por un certificado, tendrá que verificar que es el propietario del dominio. Aún puede crear el inquilino de distribución por ahora y verificar la propiedad del dominio más adelante. Para obtener más información, consulte Solicitud de certificados para el inquilino de distribución de CloudFront.

9. Elija Siguiente.
10. En la página Definir parámetros, aparecen los parámetros que especificó en la distribución de varios inquilinos. Para los parámetros obligatorios, ingrese un valor junto al nombre del parámetro y guarde los cambios.
11. Para agregar otro parámetro, elija Agregar parámetro e ingrese un nombre y un valor.
12. Elija Siguiente.
13. (Opcional) Para Personalización de seguridad, si elige Invalidar la configuración de distribución, seleccione la opción que mejor se adapte al caso de uso.
14. (Opcional) Para Personalización de restricciones geográficas, si elige Invalidar la configuración de distribución, seleccione el Tipo de restricción y los Países correspondientes para el inquilino de distribución. Para obtener más información, consulte Restricción de la distribución geográfica de su contenido.
15. Elija Siguiente.
16. Elija Crear inquilino de distribución.

Puede encontrar todos los inquilinos de distribución en la página Inquilinos de distribución. Puede filtrar según los siguientes elementos:

Asociación

- ID de distribución
- ID de certificado
- ID del grupo de conexiones

- ID de ACL web

Propiedades

- Nombre
- Dominio

Puede editar los inquilinos de distribución para personalizar ajustes específicos. Para obtener más información, consulte Personalizaciones de inquilinos de distribución.

Standard

Creación de una distribución estándar

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, elija Crear distribución.
3. Introduzca un Nombre de distribución para la distribución estándar. El nombre aparecerá como el valor de la clave `Name` como una etiqueta. Puede cambiar este valor posteriormente. Puede agregar hasta 50 etiquetas a la distribución estándar. Para obtener más información, consulte Etiquetado de una distribución.
4. Elija Sitio web o aplicación únicos, Siguiente.
5. (Opcional) Para Configuración del dominio, introduzca un dominio que ya esté registrado con Route 53 en la Cuenta de AWS o registre un nuevo dominio. Complete los pasos de configuración.
   - Si el dominio utiliza un proveedor de DNS distinto de Route 53, puede agregar el dominio, pero deberá hacerlo después de crear la distribución. Omita la configuración del dominio por ahora para continuar con la creación de la distribución. Deberá configurar manualmente el dominio y el certificado TLS más adelante. Para obtener más información, consulte Adición de un dominio a la distribución estándar de CloudFront.
6. Elija Siguiente.
7. En la página Especificar el origen, seleccione el tipo de origen del que CloudFront obtendrá el contenido. CloudFront utilizará la configuración recomendada para ese tipo de origen para la distribución. Para obtener más información sobre los ajustes recomendados, consulte Referencia de la configuración de distribución preconfigurada.

8. En Origen, elija o introduzca el origen.
9. En Configuración, elija una de las siguientes opciones:
   - Usar configuración de origen recomendada: utilice la configuración predeterminada recomendada de caché y origen para el tipo de origen que haya seleccionado.
   - Personalizar la configuración de origen: personalice la caché y la configuración de origen. Si elige esta opción, especifique valores propios.
10. Elija Siguiente.
11. En la página Habilitar las protecciones de seguridad, elija si desea habilitar las protecciones de seguridad de AWS WAF.
12. Elija Siguiente.
13. (Opcional) Si utiliza Route 53 para el dominio, verá la página Certificado TLS. Si CloudFront no puede encontrar un certificado de AWS Certificate Manager (ACM) existente para el dominio en la Cuenta de AWS en la Región de AWS `us-east-1`, puede elegir crear un certificado automáticamente o crearlo de forma manual. Después de crear el certificado, seleccione Siguiente.
14. Revise los detalles de distribución y seleccione Crear distribución.
15. Después de que CloudFront cree la distribución, el valor de la columna Estado de la distribución cambiará de Implementando a la fecha y hora en que se implementa la distribución.

    El nombre de dominio que CloudFront asigna a su distribución aparece en la lista de distribuciones. (También aparece en la pestaña General de la distribución seleccionada).

    > **Tip**
    >
    > Puede utilizar un nombre de dominio alternativo, en lugar del nombre que le ha asignado CloudFront, según los pasos que se indican en Uso de URL personalizadas añadiendo nombres de dominio alternativos (CNAME).

16. Una vez implementada la distribución, confirme que puede acceder al contenido con la nueva URL de CloudFront (d111111abcdef8.cloudfront.net) o el CNAME. Para obtener más información, consulte Prueba de una distribución.
17. Asegúrese de actualizar los registros de DNS para que apunten a CloudFront cuando esté listo para enviar tráfico a la distribución. Para obtener más información, consulte Apunte de los dominios a CloudFront (distribución estándar).

Valores que CloudFront muestra en la consola

Al crear una nueva distribución o actualizarla, CloudFront muestra la siguiente información en su consola.

> **Note**
>
> Los firmantes de confianza activos, esto es, las Cuentas de AWS con un par de claves de CloudFront activas y que se pueden utilizar para crear URL firmadas válidas, actualmente no se pueden ver en la consola de CloudFront.

ID de distribución

Al ejecutar una acción en una distribución mediante la API de CloudFront, use el ID de distribución para especificar qué distribución desea utilizar, por ejemplo, `EDFDVBD6EXAMPLE`. No se puede cambiar el ID de distribución de una distribución.

Implementación y estado

Al implementar una distribución, verá el estado Implementando en la columna Última modificación. Espere a que finalice la implementación de la distribución y asegúrese de que la columna Estado muestra Habilitado. Para obtener más información, consulte Estado de la distribución.

Última modificación

La fecha y hora de la última modificación de la distribución, con formato ISO 8601; por ejemplo, 2012-05-19T19:37:58Z. Para obtener más información, consulte https://www.w3.org/TR/NOTE-datetime.

Nombre del dominio

El nombre de dominio de la distribución se utiliza en los enlaces a los objetos. Por ejemplo, si el nombre de dominio de su distribución es `d111111abcdef8.cloudfront.net`, el enlace a `/images/image.jpg` será `https://d111111abcdef8.cloudfront.net/images/image.jpg`. No se puede cambiar el nombre de dominio de CloudFront para la distribución. Para obtener más información acerca de las URL de CloudFront para los objetos, consulte Personalización del formato de URL para archivos en CloudFront.

Si especificó uno o varios nombres de dominio alternativo (CNAME), puede utilizar sus propios nombres de dominio en lugar del nombre de dominio de CloudFront para los enlaces a sus objetos. Para obtener más información acerca de CNAME, consulte Nombres de dominio alternativos (CNAME).

> **Note**
>
> Los nombres de dominio de CloudFront son únicos. El nombre de dominio de la distribución nunca se utilizó para una distribución anterior y nunca se reutilizará para otra distribución futura.

Enlaces adicionales

Para obtener más información acerca de cómo crear una distribución, consulte los siguientes enlaces.

- Para aprender a crear una distribución que utilice como origen un bucket de Amazon Simple Storage Service (Amazon S3) con control de acceso de origen (OAC), consulte Introducción a una distribución estándar de CloudFront.
- Para obtener información sobre el uso de las API de CloudFront para crear una distribución, consulte CreateDistribution en la Referencia de la API de Amazon CloudFront.
- Para obtener información sobre cómo actualizar una distribución (por ejemplo, para agregar comportamientos de caché a distribuciones estándar o para personalizar inquilinos de distribución), consulte Actualizar una distribución.
- Para ver el número máximo actual de distribuciones que puede crear para cada cuenta de AWS o para solicitar una cuota (antes denominada límite) más alta, consulte Cuotas generales de distribuciones.

Adición de un dominio a la distribución estándar de CloudFront

Después de crear una nueva distribución estándar de CloudFront, puede agregarle un dominio. Si lo desea, puede configurar un dominio de Amazon Route 53 para la distribución estándar cuando la cree. Para obtener más información, consulte Creación de una distribución de CloudFront en la consola.

Adición de un dominio a la distribución estándar existente

Adición de un dominio a la distribución estándar

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, elija el ID de la distribución.
3. En Configuración, Nombres de dominio alternativos, elija Agregar un dominio.
4. Introduzca hasta cinco dominios para servir.
5. Elija Siguiente.
6. Para Certificado TLS, si CloudFront no puede encontrar un certificado de AWS Certificate Manager (ACM) existente para el dominio en la Cuenta de AWS en la Región de AWS `us-east-1`, puede crear uno.
   - Si utiliza Amazon Route 53 (Route 53), CloudFront crea automáticamente un certificado para usted.
7. Cuando se aprovisione el certificado, debe actualizar los registros de DNS con el proveedor de DNS para demostrar la propiedad del dominio. A continuación, elija Validar certificado. Para obtener más información, consulte Apunte de los dominios a CloudFront (distribución estándar).
   - Si utiliza Route 53, CloudFront actualiza los registros de DNS por usted.
8. Elija Siguiente.
9. Revise los cambios y elija Agregar dominios.
10. Antes de enviar tráfico a la distribución, asegúrese de actualizar los registros de DNS para que apunten a CloudFront. Para obtener más información, elija Enrutar dominios a CloudFront en la sección Configuración de la página de detalles de la distribución.
    - Si utiliza Route 53, puede hacer que CloudFront configure el enrutamiento de DNS automáticamente.

Apunte de los dominios a CloudFront (distribución estándar)

Actualice los registros de DNS para enrutar el tráfico de cada dominio al nombre de host de CloudFront. Puede tener varios nombres de dominio, pero todos deben resolverse a este nombre de host.

Dirección de dominios a CloudFront

1. Copie el valor del nombre de host de CloudFront, como d111111abcdef8.cloudfront.net.
2. Actualice los registros de DNS para enrutar el tráfico de cada dominio al nombre de host de CloudFront.
   1. Inicie sesión en el registrador de dominios o en la consola de administración del proveedor de DNS.
   2. Vaya a la sección de administración de DNS del dominio.
      - Para subdominios: cree un registro CNAME. Por ejemplo:
        - Nombre: el subdominio (como `www` o `app`)
        - Valor/Destino: el nombre de host de CloudFront
        - Tipo de registro: CNAME
        - TTL: 3600 (o lo que sea adecuado para el caso de uso)
      - Para dominios de vértice/raíz: esto requiere una configuración de DNS única, ya que los registros CNAME estándar no se pueden utilizar en el dominio raíz o de vértice. Como la mayoría de los proveedores de DNS no admiten los registros ALIAS, recomendamos crear un registro ALIAS en Route 53. Por ejemplo:
        - Nombre: el dominio de apex (por ejemplo, `example.com`)
        - Tipo de registro: A
        - Alias: sí
        - Destino del alias: el nombre de host de CloudFront
        - Política de enrutamiento: simple (o lo que sea apropiado para el caso de uso)
   3. Compruebe que el cambio de DNS se haya propagado. (Esto suele ocurrir cuando caduca TTL. A veces puede tardar entre 24 y 48 horas). Use una herramienta como `dig` o `nslookup`.

      ```
      dig www.example.com
      # Should eventually return a CNAME pointing to your CloudFront hostname
      ```
3. Vuelva a la consola de CloudFront y elija Enviar. Cuando el dominio está activo, CloudFront actualiza el estado del dominio para indicar que el dominio está listo para atender el tráfico.

Para obtener más información, consulte la documentación del proveedor de DNS:

- Cloudflare
- ClouDNS
- DNSimple
- Gandi.net
- GoDaddy
- Google Cloud DNS
- Namecheap

Referencia de la configuración de distribución preconfigurada

Al crear la distribución de CloudFront, CloudFront configura automáticamente gran parte de la configuración de distribución por usted, en función del tipo de origen del contenido. Si lo desea, puede editar manualmente la configuración de la distribución. Para obtener más información, consulte Referencia de toda la configuración de distribución.

Las siguientes secciones describen los ajustes de preconfiguración predeterminados para las distribuciones y los ajustes que puede personalizar.

Origen de Amazon S3

A continuación se muestran los ajustes de origen que CloudFront preconfigura para el origen de Amazon S3 en una distribución de varios inquilinos.

Ajustes de origen (preconfigurados)

- Control de acceso de origen (solo consola): CloudFront lo configura automáticamente. CloudFront intenta agregar la política de bucket de S3 para distribuciones estándar y para distribuciones de varios inquilinos sin parámetros utilizados en el dominio de origen.
- Agregar encabezado personalizado: ninguno
- Habilitar el escudo de origen: no
- Intentos de conexión – 3

A continuación, se muestran los ajustes de caché que CloudFront preconfigura para el origen de Amazon S3 en una distribución de varios inquilinos.

Ajustes de caché (preconfigurados)

- Comprimir objetos automáticamente: sí
- Política de protocolo de lector: redirigir a HTTPS
- Método HTTP permitido – `GET, HEAD`
- Acceso de lector restringido: no
- Política de caché – `CachingOptimized`
- Política de solicitud de origen: ninguna
- Política de encabezado de respuesta: ninguna
- Smooth Streaming: no
- Cifrado en el nivel de campo: no
- Habilitación de registros de acceso en tiempo real: no
- Funciones: no

A continuación, se muestran los ajustes que puede personalizar para el origen de Amazon S3 en una distribución de varios inquilinos.

Ajustes personalizables

- Acceso a S3: CloudFront lo establece automáticamente en función de la configuración del bucket de S3:
  - Si el bucket es público: no se necesita una política de control de acceso de origen (OAC).
  - Si el bucket es privado: puede elegir o crear una política de OAC para utilizarla.
- Habilitar el escudo de origen: no
- Comprimir objetos automáticamente: sí
  - Si elige Sí, se utilizará la política de almacenamiento en caché `CachingOptimized`.
  - Si elige No, se utilizará la política de almacenamiento en caché `CachingOptimizedForUncompressedObjects`.

Origen de API Gateway

A continuación, se muestran los ajustes de origen que CloudFront preconfigura para el origen de API Gateway en una distribución de varios inquilinos.

Ajustes de origen (preconfigurados)

- Protocolo: solo HTTPS
- Puerto HTTPS – 443
- Protocolo SSL mínimo del origen: TLSv1.2
- Ruta de origen: ninguna
- Control de acceso de origen (solo consola): CloudFront lo configura automáticamente
- Agregar encabezado personalizado: ninguno
- Habilitar el escudo de origen: no
- Intentos de conexión – 3
- Tiempo de espera de respuesta – 30
- Tiempo de espera de Keep-alive – 5

A continuación se muestran los ajustes de caché que CloudFront preconfigura para el origen de API Gateway en una distribución de varios inquilinos.

Ajustes de caché (preconfigurados)

- Comprimir objetos automáticamente: sí
- Política de protocolo de lector: redirigir a HTTPS
- Método HTTP permitido – `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Almacenar en caché métodos HTTP: no
- Cómo permitir solicitudes de gRPC a través de HTTP/2: no
- Acceso de lector restringido: no
- Política de caché: `CachingDisabled` (valores posibles: `UseOriginCacheControlHeaders`, `UseOriginCacheControlHeaders-QueryStrings`)
- Política de solicitud de origen: `AllViewerExceptHostHeader` (valores posibles: `AllViewer`, `AllViewerandCloudFrontHeaders-2022-06`)
- Política de encabezado de respuesta: ninguna
- Smooth Streaming: no
- Cifrado en el nivel de campo: no
- Habilitación de registros de acceso en tiempo real: no
- Funciones: no

A continuación, se muestran los ajustes que puede personalizar para el origen de API Gateway en una distribución de varios inquilinos.

Ajustes personalizables

- Habilitar escudo de origen: (predeterminado: no)
- Comprimir objetos automáticamente: (predeterminado: sí)

Origen personalizado e instancia de EC2

A continuación, se muestran los ajustes de origen que CloudFront preconfigura para el origen personalizado en una distribución de varios inquilinos.

Ajustes de origen (preconfigurados)

- Protocolo: coincidir con lector
- Puerto HTTP – 80
- Puerto HTTPS – 443
- Protocolo SSL mínimo del origen: TLSv1.2
- Ruta de origen: ninguna
- Agregar encabezado personalizado: ninguno
- Habilitar el escudo de origen: no
- Intentos de conexión – 3
- Tiempo de espera de respuesta – 30
- Tiempo de espera de Keep-alive – 5

A continuación, se muestran los ajustes de caché que CloudFront preconfigura para el origen personalizado y la instancia de EC2 en una distribución de varios inquilinos.

Ajustes de caché (preconfigurados)

- Comprimir objetos automáticamente: sí
- Política de protocolo de lector: redirigir a HTTPS
- Método HTTP permitido – `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Almacenar en caché métodos HTTP: no
- Cómo permitir solicitudes de gRPC a través de HTTP/2: no

- Acceso de lector restringido: no
- Política de caché: `UseOriginCacheControlHeaders` (valores posibles: `UseOriginCacheControlHeaders-QueryStrings`, `CachingDisabled`, `CacheOptimized`, `CachingOptimizedForUncompressedObjects`)
- Política de solicitud de origen: `AllViewer` (valores posibles: `AllViewerExceptHostHeader`, `AllViewerandCloudFrontHeaders-2022-06`)
- Política de encabezado de respuesta: ninguna
- Smooth Streaming: no
- Cifrado en el nivel de campo: no
- Habilitación de registros de acceso en tiempo real: no
- Funciones: no

A continuación, se muestran los ajustes que puede personalizar para el origen personalizado y la instancia de EC2 en una distribución de varios inquilinos.

Ajustes personalizables

- Habilitar escudo de origen: (predeterminado: no)
- Comprimir objetos automáticamente: (predeterminado: sí)
- Almacenamiento en caché: (predeterminado: `Cache by Default`)
  - Si se selecciona `Cache by Default`, se utiliza la política de caché `UseOriginCacheControlHeaders`.
  - Si se selecciona `Do Not Cache by Default`, se utiliza la política de caché `CachingDisabled`.
- Incluir cadena de consulta en la caché: (predeterminado: sí, si `Cache by Default` ya está seleccionado)
  - Si `Do Not Cache by Default` ya está seleccionado y luego elige incluir la cadena de consulta en la memoria caché, se utiliza la política de memoria caché `UseOriginCacheControlHeaders-QueryStrings`.

Origen de Elastic Load Balancing

A continuación, se muestran los ajustes de origen que CloudFront preconfigura para el origen de Elastic Load Balancing en una distribución de varios inquilinos.

Ajustes de origen (preconfigurados)

- Protocolo: solo HTTPS
- Puerto HTTPS – 443
- Protocolo SSL mínimo del origen: TLSv1.2
- Ruta de origen: ninguna
- Agregar encabezado personalizado: ninguno
- Habilitar el escudo de origen: no
- Intentos de conexión – 3
- Tiempo de espera de respuesta – 30
- Tiempo de espera de Keep-alive – 5

A continuación, se muestran los ajustes de la caché que CloudFront preconfigura para el origen de Elastic Load Balancing en una distribución de varios inquilinos.

Ajustes de caché (preconfigurados)

- Comprimir objetos automáticamente: sí
- Política de protocolo de lector: redirigir a HTTPS
- Método HTTP permitido – `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Almacenar en caché métodos HTTP: no
- Cómo permitir solicitudes de gRPC a través de HTTP/2: no
- Acceso de lector restringido: no
- Almacenamiento en caché: (predeterminado: `Cache by Default`)
  - Si se selecciona `Cache by Default`, se utiliza la política de caché `UseOriginCacheControlHeaders`.
  - Si se selecciona `Do Not Cache by Default`, se utiliza la política de caché `CachingDisabled`.
- Incluir cadena de consulta en la caché: (predeterminado: sí, si `Cache by Default` ya está seleccionado)
  - Si `Do Not Cache by Default` ya está seleccionado y luego elige incluir la cadena de consulta en la memoria caché, se utiliza la política de memoria caché `UseOriginCacheControlHeaders-QueryStrings`.

- Política de solicitud de origen: `All Viewer` (valores posibles: `AllViewerExceptHostHeader`, `AllViewerandCloudFrontHeaders-2022-06`)
- Política de encabezado de respuesta: ninguna
- Smooth Streaming: no
- Cifrado en el nivel de campo: no
- Habilitación de registros de acceso en tiempo real: no
- Funciones: no

A continuación, se muestran los ajustes que puede personalizar para el origen de Elastic Load Balancing en una distribución de varios inquilinos.

Ajustes personalizables

- Habilitar escudo de origen: (predeterminado: no)
- Comprimir objetos automáticamente: (predeterminado: sí)
- Almacenamiento en caché: (predeterminado: `Cache by Default`)
  - Si se selecciona `Cache by Default`, se utiliza la política de caché `UseOriginCacheControlHeaders`.
  - Si se selecciona `Do Not Cache by Default`, se utiliza la política de caché `CachingDisabled`.
- Incluir cadena de consulta en la caché: (predeterminado: sí, si `Cache by Default` ya está seleccionado)
  - Si `Do Not Cache by Default` ya está seleccionado y luego elige incluir la cadena de consulta en la memoria caché, se utiliza la política de memoria caché `UseOriginCacheControlHeaders-QueryStrings`.

Origen de MediaPackage v1

A continuación, se muestran los ajustes de origen que CloudFront preconfigura para el origen de MediaPackage v1 en una distribución de varios inquilinos.

Ajustes de origen (preconfigurados)

- Protocolo: solo HTTPS
- Puerto HTTPS – 443

- Protocolo SSL mínimo del origen: TLSv1.2
- Ruta de origen: la proporciona ingresando la URL del MediaPackage.
- Agregar encabezado personalizado: ninguno
- Habilitar el escudo de origen: no
- Intentos de conexión – 3
- Tiempo de espera de respuesta – 30
- Tiempo de espera de Keep-alive – 5

A continuación, se muestran los ajustes de la caché que CloudFront preconfigura para el origen de MediaPackage v1 en una distribución de varios inquilinos.

Ajustes de caché (preconfigurados)

- Comprimir objetos automáticamente: sí
- Política de protocolo de lector: redirigir a HTTPS
- Método HTTP permitido – `GET, HEAD`
- Almacenar en caché métodos HTTP: no
- Cómo permitir solicitudes de gRPC a través de HTTP/2: no
- Acceso de lector restringido: no
- Política de caché – `Elemental-MediaPackage`
- Política de solicitud de origen: ninguna
- Política de encabezado de respuesta: ninguna
- Smooth Streaming: no
- Cifrado en el nivel de campo: no
- Habilitación de registros de acceso en tiempo real: no
- Funciones: no

Origen de MediaPackage v2

A continuación, se muestran los ajustes de origen que CloudFront preconfigura para el origen de MediaPackage v2 en una distribución de varios inquilinos.

Ajustes de origen (preconfigurados)

- Control de acceso de origen: CloudFront lo configura automáticamente y agrega la política
- Protocolo: solo HTTPS
- Puerto HTTPS – 443
- Protocolo SSL mínimo del origen: TLSv1.2
- Ruta de origen: ninguna
- Agregar encabezado personalizado: ninguno
- Habilitar el escudo de origen: no
- Intentos de conexión – 3
- Tiempo de espera de respuesta – 30
- Tiempo de espera de Keep-alive – 5

A continuación, se muestran los ajustes de la caché que CloudFront preconfigura para el origen de MediaPackage v2 en una distribución de varios inquilinos.

Ajustes de caché (preconfigurados)

- Comprimir objetos automáticamente: sí
- Política de protocolo de lector: redirigir a HTTPS
- Método HTTP permitido – `GET, HEAD`
- Almacenar en caché métodos HTTP: no
- Cómo permitir solicitudes de gRPC a través de HTTP/2: no
- Acceso de lector restringido: no
- Política de caché – `Elemental-MediaPackage`
- Política de solicitud de origen: ninguna
- Política de encabezado de respuesta: ninguna
- Smooth Streaming: no
- Cifrado en el nivel de campo: no
- Habilitación de registros de acceso en tiempo real: no
- Funciones: no

Origen de MediaTailor

A continuación, se muestran los ajustes de origen que CloudFront preconfigura para el origen de MediaTailor en una distribución de varios inquilinos.

Ajustes de origen (preconfigurados)

- Protocolo: solo HTTPS
- Puerto HTTPS – 443
- Protocolo SSL mínimo del origen: TLSv1.2
- Ruta de origen: la proporciona ingresando la URL del MediaPackage.
- Agregar encabezado personalizado: ninguno
- Habilitar el escudo de origen: no
- Intentos de conexión – 3
- Tiempo de espera de respuesta – 30
- Tiempo de espera de Keep-alive – 5

A continuación, se muestran los ajustes de la caché que CloudFront preconfigura para el origen de MediaTailor en una distribución de varios inquilinos.

Ajustes de caché (preconfigurados)

- Comprimir objetos automáticamente: sí
- Política de protocolo de lector: redirigir a HTTPS
- Método HTTP permitido – `GET, HEAD`
- Almacenar en caché métodos HTTP: no
- Cómo permitir solicitudes de gRPC a través de HTTP/2: no
- Acceso de lector restringido: no
- Política de caché: ninguna
- Política de solicitud de origen – `Elemental-MediaTailor-PersonalizedManifests`
- Política de encabezado de respuesta: ninguna
- Smooth Streaming: no
- Cifrado en el nivel de campo: no

- Habilitación de registros de acceso en tiempo real: no
- Funciones: no

Referencia de toda la configuración de distribución

Puede editar manualmente la configuración de la distribución de CloudFront al crear o actualizar la distribución. A continuación, se muestra la configuración que puede editar.

No obstante, CloudFront configura la mayoría de las opciones de configuración de distribución por usted, en función del tipo de origen del contenido. Para obtener más información, consulte Referencia de la configuración de distribución preconfigurada.

Para obtener más información acerca de cómo crear o actualizar una distribución utilizando la consola de CloudFront, consulte the section called “Creación de una distribución” o the section called “Actualizar una distribución”.

Temas

- Configuración de origen
- Configuración del comportamiento de la caché
- Ajustes de la distribución
- Páginas de error personalizadas y almacenamiento de errores en caché
- Restricciones geográficas

Configuración de origen

Al crear o actualizar una distribución mediante la consola de CloudFront, proporciona información acerca de una o varias ubicaciones, conocidas como orígenes, donde se almacenan las versiones originales del contenido web. CloudFront obtiene el contenido web desde sus orígenes y los envía a los lectores a través de una red global de servidores periféricos.

Para obtener información sobre el número máximo actual de orígenes que puede crear para una distribución o para solicitar una cuota más alta, consulte the section called “Cuotas generales de distribuciones”.

Si desea eliminar un origen, primero debe editar o eliminar los comportamientos de la caché que están asociados con dicho origen.

> **Important**
>
> Si elimina un origen, confirme que los archivos que se han servido anteriormente a ese origen estén disponibles en otro origen y que los comportamientos de la caché ya estén direccionando las solicitudes para dichos archivos al nuevo origen.

Al crear o actualizar una distribución deberá especificar los siguientes valores para cada origen.

Temas

- Dominio de origen
- Protocolo (solo orígenes personalizados)
- Ruta de origen
- Nombre
- Acceso de origen (solo orígenes de Amazon S3)
- Agregar encabezado personalizado
- Habilitar Origin Shield
- Intentos de conexión
- Tiempo de espera de conexión
- Tiempo de espera de respuesta
- Tiempo de espera de finalización de la respuesta
- Tiempo de espera de keep-alive (solo orígenes personalizados y de VPC)
- Cuotas de tiempo de espera de respuesta y de keep-alive

Dominio de origen

El dominio del origen es el nombre del dominio de DNS del recurso donde CloudFront obtendrá objetos para el origen, por ejemplo, un bucket de Amazon S3 o un servidor HTTP. Por ejemplo:

- Bucket de Amazon S – `amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com`

> **Note**
>
> Si ha creado recientemente el bucket de S3, la distribución de CloudFront podría devolver respuestas `HTTP 307 Temporary Redirect` durante un periodo máximo de 24 horas.

El nombre del bucket de S3 puede tardar hasta 24 horas en propagarse a todas las regiones de AWS. Cuando se complete la propagación, la distribución deja de enviar automáticamente estas respuestas de redirección; no es necesario que realice ninguna acción. Para obtener más información, consulte ¿Por qué recibo una respuesta de redirección temporal HTTP 307 de Amazon S3? y Redirección temporal de solicitudes.

- Bucket de Amazon S3 configurado como un sitio web – `amzn-s3-demo-bucket.s3-website.us-west-2.amazonaws.com`
- Contenedor MediaStore – `examplemediastore.data.mediastore.us-west-1.amazonaws.com`
- Punto de enlace de MediaPackage – `examplemediapackage.mediapackage.us-west-1.amazonaws.com`
- Instancia Amazon EC – `ec2-203-0-113-25.compute-1.amazonaws.com`
- Balanceador de carga Elastic Load Balancing – `example-load-balancer-1234567890.us-west-2.elb.amazonaws.com`
- Su propio servidor web – `www.example.com`

Elija el nombre de dominio en el campo Origin domain (Dominio de origen) o escriba el nombre. Los recursos de las regiones registradas se deben ingresar de forma manual. El nombre de dominio no distingue entre mayúsculas y minúsculas. El dominio de origen debe tener un nombre de DNS que se resuelve públicamente que enruta las solicitudes de los clientes a destinos a través de Internet.

Si configura CloudFront para conectarse al origen a través de HTTP, uno de los nombres de dominio del certificado debe coincidir con el nombre de dominio que especifique para Nombre de dominio de origen. Si no coincide ningún nombre de dominio, CloudFront devuelve al lector un código de estado HTTP 502 (Puerta de enlace incorrecta). Para obtener más información, consulte Nombres de dominio en la distribución de CloudFront y en el certificado y Error de negociación SSL/TLS entre CloudFront y un servidor de origen personalizado.

> **Note**
>
> Si está usando una política de solicitud de origen que reenvía el encabezado de host de lector al origen, el origen debe responder con un certificado que coincida con el encabezado de host de lector. Para obtener más información, consulte Añadido de encabezados de solicitudes de CloudFront.

Si su origen es un bucket de Amazon S3, tenga en cuenta lo siguiente:

- Si el bucket está configurado como sitio web, ingrese el punto de conexión de alojamiento de sitios web estáticos de Amazon S3 del bucket. No seleccione el nombre del bucket en la lista del campo Origin domain (Dominio de origen). Este punto de conexión de alojamiento del sitio web aparecerá en la consola de Amazon S3 en la página Properties (Propiedades), en Static Website Hosting (Alojamiento de sitio web estático). Para obtener más información, consulte the section called "Uso de un bucket de Amazon S3 configurado como punto de conexión del sitio web".
- Si ha configurado Amazon S3 Transfer Acceleration en su bucket, no especifique el punto de conexión `s3-accelerate` para Origin domain (Dominio de origen).
- Si utiliza un bucket de otra cuenta de AWS y el bucket no está configurado como un sitio web, escriba el nombre en el siguiente formato:

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

  Si su bucket se encuentra en una región de EE. UU. y desea que Amazon S3 direccione las solicitudes a una instalación en el norte de Virginia, utilice el siguiente formato:

  ```
  bucket-name.s3.us-east-1.amazonaws.com
  ```
- Los archivos deben ser legibles públicamente a no ser que proteja su contenido en Amazon S3 mediante un control de acceso de origen de CloudFront. Para obtener más información sobre el control de acceso, consulte the section called "Restricción del acceso a un origen de Amazon S3".

> **Important**
>
> Si el origen es un bucket de Amazon S3, el nombre del bucket debe cumplir los requisitos de nomenclatura de DNS. Para obtener más información, consulte Restricciones y limitaciones de buckets en la Guía del usuario de Amazon Simple Storage Service.

Al cambiar el valor de Origin Domain (Dominio de origen) por un origen, CloudFront inmediatamente comienza a replicar el cambio en las ubicaciones de borde de CloudFront. Hasta que la configuración de la distribución se actualiza en una ubicación de borde determinada, CloudFront continúa reenviando solicitudes al servidor HTTP o al origen anterior. Tan pronto como la configuración de la distribución se actualiza en esa ubicación de borde, CloudFront comienza a reenviar solicitudes al nuevo origen.

Cambiar el origen no requiere que CloudFront vuelva a incluir las cachés periféricas con objetos del nuevo origen. Siempre que las solicitudes de los lectores en su aplicación no cambien, CloudFront sigue ofreciendo objetos que ya estén en una caché de borde hasta que el TTL de cada objeto caduque o hasta que los objetos poco solicitados sean desalojados.

Protocolo (solo orígenes personalizados)

> **Note**
>
> Esto solo se aplica a los orígenes personalizados.

La política de protocolo que desea que CloudFront utilice cuando solicite objetos del origen.

Elija uno de los valores siguientes:

- HTTP Only (Solo HTTP): CloudFront utiliza solo HTTP para acceder al origen.

  > **Important**
  >
  > HTTP Only (Solo HTTP): es la configuración predeterminada cuando el origen es un punto de conexión de alojamiento de sitio web estático de Amazon S3, ya que Amazon S3 no admite conexiones HTTPS para puntos de conexión de alojamiento de sitio web estático. La consola de CloudFront no admite el cambio de esta configuración para los puntos de enlace de alojamiento de sitios web estáticos de Amazon S3.

- HTTPS Only (Solo HTTPS): CloudFront solo utiliza HTTPS para obtener acceso al origen.
- Match Viewer (Coincidir con lector): CloudFront se comunica con el origen mediante HTTP o HTTPS, en función del protocolo de la solicitud del lector. Tenga en cuenta que CloudFront almacena en caché el objeto solo una vez, incluso si los lectores realizan solicitudes a través de los protocolos HTTP y HTTPS.

  > **Important**
  >
  > En el caso de la solicitudes HTTPS de lector que CloudFront reenvía a este origen, uno de los nombres de dominio del certificado SSL/TLS en su servidor de origen debe coincidir con el nombre de dominio que especifique en Origin domain (Dominio de origen). En caso contrario, CloudFront responde a las solicitudes del lector con un código de estado HTTP 502 (Gateway incorrecta) en lugar de devolver el objeto solicitado. Para obtener más

información, consulte the section called “Requisitos para la utilización de certificados SSL/TLS con CloudFront”.

Temas

- Puerto HTTP
- Puerto HTTPS
- Protocolo SSL mínimo del origen

Puerto HTTP

> **Note**
>
> Esto solo se aplica a los orígenes personalizados.

(Opcional) Puede especificar el puerto HTTP en el que escucha el origen personalizado. Los valores válidos son los puertos 80, 443 y 1024 y 65535. El valor predeterminado es el puerto 80.

> **Important**
>
> El puerto 80 es la configuración predeterminada cuando el origen es un punto de enlace de alojamiento de sitio web estático de Amazon S3, ya que Amazon S3 solo admite el puerto 80 para los puntos de enlace de alojamiento de sitio web estático. La consola de CloudFront no admite el cambio de esta configuración para los puntos de enlace de alojamiento de sitios web estáticos de Amazon S3.

Puerto HTTPS

> **Note**
>
> Esto solo se aplica a los orígenes personalizados.

(Opcional) Puede especificar el puerto HTTPS en el que escucha el origen personalizado. Los valores válidos son los puertos 80, 443 y 1024 y 65535. El valor predeterminado es el puerto 443.

Cuando Protocol (Protocolo) se establece en HTTP only (Solo HTTP), no puede especificar un valor para HTTPS port (Puerto HTTPS).

Protocolo SSL mínimo del origen

> **Note**
>
> Esto solo se aplica a los orígenes personalizados.

Elija el protocolo TLS/SSL que CloudFront puede utilizar como mínimo cuando establece una conexión HTTPS con el origen. Los protocolos TLS inferiores son menos seguros, por lo que le recomendamos que elija el protocolo TLS más reciente que admita el origen. Cuando Protocol (Protocolo) se establece en HTTP only (Solo HTTP), no puede especificar un valor para Minimum origin SSL protocol (Protocolo SSL de origen mínimo).

Si utiliza la API de CloudFront para establecer el protocolo TLS/SSL para que CloudFront lo utilice, no podrá establecer un protocolo mínimo. En su lugar, debe especificar todos los protocolos TLS/SSL que CloudFront puede utilizar con su origen. Para obtener más información, consulte OriginSslProtocols en la Referencia de la API de Amazon CloudFront.

Ruta de origen

Si desea que CloudFront solicite el contenido de un directorio en su origen, ingrese la ruta del directorio comenzando por una barra diagonal (/). CloudFront agrega la ruta del directorio al valor de Origin domain (Dominio de origen), por ejemplo, **`cf-origin.example.com/production/images`**. No añada una barra inclinada (/) al final de la ruta.

Por ejemplo, suponga que ha especificado los siguientes valores para su distribución:

- Origin domain (Dominio de origen): un bucket de Amazon S3 llamado **`amzn-s3-demo-bucket`**
- Origin path (Ruta de origen – **`/production`**
- Alternate domain names (CNAME) (Nombres de dominio alternativos (CNAME) – **`example.com`**

Cuando un usuario escribe `example.com/index.html` en un navegador, CloudFront envía una solicitud a Amazon S3 de `amzn-s3-demo-bucket/production/index.html`.

Cuando un usuario escribe `example.com/acme/index.html` en un navegador, CloudFront envía una solicitud a Amazon S3 de `amzn-s3-demo-bucket/production/acme/index.html`.

Nombre

Un nombre es una cadena que identifica de forma exclusiva este origen en esta distribución. Si crea comportamientos de caché además del comportamiento de caché predeterminado, utilice el nombre que especifique aquí para identificar el origen al que desea que CloudFront dirija una solicitud cuando esta coincida con el patrón de ruta de ese comportamiento de caché.

Acceso de origen (solo orígenes de Amazon S3)

> **Note**
>
> Esto solo se aplica a los orígenes del bucket de Amazon S3 (aquellos que no utilizan el punto de enlace del sitio web estático de S3).

Elija Origin access control settings (recommended) (Configuración de control de acceso de origen [recomendada]) si desea que sea posible restringir el acceso a un origen de bucket de Amazon S3 solo a determinadas distribuciones de CloudFront.

Elija Public (Público) si el origen del bucket de Amazon S3 es de acceso público.

Para obtener más información, consulte the section called “Restricción del acceso a un origen de Amazon S3”.

Para obtener información acerca de cómo exigir a los usuarios a obtener acceso a los objetos de un origen personalizado empleando solo URL de CloudFront, consulte the section called “Restricción del acceso a archivos en orígenes personalizados”.

Agregar encabezado personalizado

Si desea que CloudFront agregue encabezados personalizados cada vez que envía una solicitud al origen, especifique el encabezado y su valor. Para obtener más información, consulte the section called “Añadido de encabezados personalizados a solicitudes de origen”.

Para ver la cantidad máxima actual de encabezados personalizados que puede agregar, la longitud máxima de los nombres de encabezado personalizados y sus valores, y la longitud máxima total de todos los nombres y valores de encabezados, consulte Cuotas.

Habilitar Origin Shield

Elija Yes (Sí) para habilitar CloudFront Origin Shield. Para obtener más información sobre Origin Shield, consulte the section called “Uso del escudo de origen”.

Intentos de conexión

Puede configurar el número de veces que CloudFront intenta conectarse al origen. Puede especificar 1, 2 o 3 como el número de intentos. El número predeterminado (si no especifica lo contrario) es 3.

Utilice esta configuración junto con Connection Timeout (Tiempo de espera de conexión) para especificar cuánto tiempo debe esperar CloudFront antes de intentar conectarse al origen secundario o devolver una respuesta de error al lector. De forma predeterminada, CloudFront espera hasta 30 segundos (3 intentos de 10 segundos cada uno) antes de intentar conectarse al origen secundario o devolver una respuesta de error. Puede reducir este tiempo si especifica menos intentos, un tiempo de espera de conexión más corto o ambas opciones.

Si se produce un error en el número especificado de intentos de conexión, CloudFront realiza una de las acciones siguientes:

- Si el origen forma parte de un grupo de orígenes, CloudFront intenta conectarse al origen secundario. Si se produce un error en el número especificado de intentos de conexión al origen secundario, CloudFront devuelve una respuesta de error al lector.
- Si el origen no forma parte de un grupo de orígenes, CloudFront devuelve una respuesta de error al lector.

En el caso de un origen personalizado (incluido un bucket de Amazon S3 configurado con alojamiento de sitio web estático), esta configuración también especifica el número de veces que CloudFront intenta obtener una respuesta del origen. Para obtener más información, consulte the section called “Tiempo de espera de respuesta”.

Tiempo de espera de conexión

El tiempo de espera de conexión de origen es el número de segundos que CloudFront espera al intentar establecer una conexión con el origen. Puede especificar un número de segundos entre 1 y 10 (ambos inclusive). El tiempo de espera predeterminado (si no especifica lo contrario) es de 10 segundos.

Utilice esta configuración junto con Connection attempts (Intentos de conexión) para especificar cuánto tiempo debe esperar CloudFront antes de intentar conectarse al origen secundario o antes

de devolver una respuesta de error al lector. De forma predeterminada, CloudFront espera hasta 30 segundos (3 intentos de 10 segundos cada uno) antes de intentar conectarse al origen secundario o devolver una respuesta de error. Puede reducir este tiempo si especifica menos intentos, un tiempo de espera de conexión más corto o ambas opciones.

Si CloudFront no establece una conexión con el origen en el número de segundos especificado, CloudFront realiza una de las acciones siguientes:

- Si el número especificado de Connection attempts (Intentos de conexión) es superior a 1, CloudFront intenta de nuevo establecer una conexión. CloudFront lo intenta hasta tres veces, según lo determinado por el valor de Connection attempts (Intentos de conexión).
- Si fallan todos los intentos de conexión y el origen forma parte de un grupo de orígenes, CloudFront intenta conectarse al origen secundario. Si se produce un error en el número especificado de intentos de conexión al origen secundario, CloudFront devuelve una respuesta de error al lector.
- Si fallan todos los intentos de conexión y el origen no forma parte de un grupo de orígenes, CloudFront devuelve una respuesta de error al lector.

Tiempo de espera de respuesta

El tiempo de espera de respuesta del origen, también conocido como tiempo de espera de lectura de origen y tiempo de espera de solicitud de origen, se aplica a los dos valores siguientes:

- Tiempo (en segundos) que CloudFront espera una respuesta después de enviar una solicitud al origen.
- Tiempo (en segundos) que CloudFront espera después de recibir el paquete de una respuesta desde el origen y antes de recibir el paquete siguiente.

> **Tip**
>
> Si desea aumentar el valor de tiempo de espera porque los lectores están experimentando errores de código de estado HTTP 504, considere la posibilidad de explorar otras formas de eliminar dichos errores antes de cambiar el valor del tiempo de espera. Consulte las sugerencias de resolución de problemas en the section called “Código de estado HTTP 504 (Tiempo de espera de puerta de enlace agotado)”.

El comportamiento CloudFront depende del método HTTP en la solicitud del lector.

- Solicitudes `GET` y `HEAD`: si el origen no responde o deja de responder durante el tiempo de espera de la respuesta, CloudFront interrumpe la conexión. CloudFront intenta de nuevo conectarse de acuerdo con el valor de the section called “Intentos de conexión”.
- Solicitudes `DELETE`, `OPTIONS`, `PATCH`, `PUT` y `POST`: si el origen no responde mientras dura el tiempo de espera de lectura, CloudFront interrumpe la conexión y no vuelve a intentar ponerse en contacto con el origen. El cliente puede volver a enviar la solicitud en caso de que sea necesario.

Tiempo de espera de finalización de la respuesta

> **Note**
>
> El tiempo de espera de finalización de la respuesta no admite la característica de implementación continua.

El tiempo (en segundos) que una solicitud de CloudFront al origen puede permanecer abierta y esperar una respuesta. Si en ese tiempo no se recibe la respuesta completa del origen, CloudFront finaliza la conexión.

A diferencia de Tiempo de espera de respuesta, que es el tiempo de espera de los paquetes de respuesta individuales, Tiempo de espera de finalización de respuesta es el tiempo máximo permitido que CloudFront espera a que se complete la respuesta. Puede usar esta configuración para asegurarse de que CloudFront no espere indefinidamente un origen lento o que no responda, incluso si otras opciones de configuración de tiempo de espera permiten una espera más larga.

Este tiempo de espera máximo incluye lo que ha especificado para otras opciones de configuración de tiempo de espera y el número de intentos de conexión por cada reintento. Puede usar estas opciones juntas a fin de especificar cuánto tiempo espera CloudFront para recibir la solicitud completa y cuándo finalizarla, independientemente de si se ha completado o no.

Por ejemplo, si establece las siguientes opciones:

- Intentos de conexión es 3
- Tiempo de espera de conexión es 10 segundos
- Tiempo de espera de respuesta es 30 segundos
- Tiempo de espera de finalización de respuesta es 60 segundos

Esto significa que CloudFront intentará conectarse al origen (hasta tres intentos en total) y que cada intento de conexión caducará a los 10 segundos. Una vez conectado, CloudFront esperará un máximo de 30 segundos a que el origen responda a la solicitud hasta que reciba el último paquete de la respuesta.

Independientemente del número de intentos de conexión o del tiempo de espera de la respuesta, CloudFront finalizará la conexión si la respuesta completa del origen tarda más de 60 segundos en completarse. CloudFront devolverá al lector una respuesta de error the section called "Código de estado HTTP 504 (Tiempo de espera de puerta de enlace agotado)" o una respuesta de error personalizada si usted ha especificado una.

> **Notas**
>
> - Si establece un valor para el tiempo de espera de finalización de respuesta, el valor debe ser igual o mayor que el valor del tiempo de espera de respuesta (tiempo de espera de lectura de origen).
> - Si no establece un valor para el tiempo de espera de finalización de respuesta, CloudFront no aplica un valor máximo.

Tiempo de espera de keep-alive (solo orígenes personalizados y de VPC)

El tiempo de espera de keep-alive es el tiempo (en segundos) que CloudFront intenta mantener una conexión con el origen personalizado después de que obtenga el último paquete de una respuesta. Garantizar una conexión persistente ahorra el tiempo necesario para restablecer la conexión TCP y realizar otro protocolo de enlace TLS para solicitudes posteriores. Aumentar el tiempo de keep-alive ayuda a mejorar la métrica de solicitud por conexión en distribuciones.

> **Note**
>
> Para que el valor de Keep-alive timeout (Tiempo de espera de keep-alive) tenga efecto, el origen debe estar configurado para permitir las conexiones persistentes.

Cuotas de tiempo de espera de respuesta y de keep-alive

- El valor predeterminado de Tiempo de espera de respuesta es de 30 segundos.

- El valor predeterminado de Tiempo de espera de keep-alive es de 5 segundos.

Si solicita un aumento del tiempo de espera para la Cuenta de AWS, actualice los orígenes de la distribución para que tengan los valores de tiempo de espera de respuesta y keep-alive que desee. Al aumentar la cuota para su cuenta, no se actualizan automáticamente sus orígenes. Por ejemplo, si utiliza una función de Lambda@Edge para establecer un tiempo de espera de keep-alive de 90 segundos, su origen ya debe tener un tiempo de espera de keep-alive de 90 segundos o más. De lo contrario, es posible que la función de Lambda@Edge no se ejecute.

Para obtener más información sobre las cuotas de distribución, incluido cómo solicitar un aumento, consulte Cuotas generales de distribuciones.

Configuración del comportamiento de la caché

Al configurar el comportamiento de la caché, puede configurar una amplia variedad de funcionalidades de CloudFront para un determinado patrón de ruta de URL de archivos en su sitio web. Por ejemplo, un comportamiento de la caché puede ser aplicable a todos los archivos `.jpg` del directorio `images` del servidor web que se esté utilizando como servidor de origen para CloudFront. La funcionalidad que puede definir para cada comportamiento de la caché incluye:

- El patrón de ruta.
- Si ha configurado varios orígenes para su distribución de CloudFront, el origen al que desea que CloudFront reenvíe sus solicitudes.
- Si enviar cadenas de consulta a su origen.
- Si acceder a los archivos especificados requiere URL firmadas.
- Si exigir a los usuarios que utilicen HTTPS para obtener acceso a los archivos.
- El tiempo mínimo que dichos archivos se mantienen en la caché de CloudFront independientemente del valor de los encabezados `Cache-Control` que el origen agregue a los archivos.

Al crear una nueva distribución, debe especificar la configuración del comportamiento de la caché predeterminado, que reenvía automáticamente todas las solicitudes al origen que especifique al crear la distribución. Después de crear una distribución, puede crear más comportamientos de la caché que definen cómo CloudFront responde cuando recibe una solicitud de objetos que coincide con un patrón de ruta, por ejemplo, `*.jpg`. Si crea más comportamientos de la caché, el predeterminado será siempre el último en procesarse. Los demás comportamientos de la caché se procesan en el

orden en que aparecen en la consola de CloudFront o, si está utilizando la API de CloudFront, en el orden en que se enumeran en el elemento `DistributionConfig` de la distribución. Para obtener más información, consulte Patrón de ruta.

Al crear un comportamiento de la caché, debe especificar el origen desde el que desea que CloudFront obtenga objetos. Por lo tanto, si desea que CloudFront distribuya objetos de todos los orígenes, debe crear al menos tantos comportamientos de la caché (incluido el predeterminado) como orígenes tenga. Por ejemplo, si tiene dos orígenes y solo el comportamiento de la caché predeterminado, este hace que CloudFront obtenga objetos desde uno de los orígenes, pero el otro origen no se usa jamás.

Para obtener información sobre el número máximo actual de comportamientos de la caché que puede agregar a una distribución o para solicitar una cuota (antes denominada límite) más alta, consulte Cuotas generales de distribuciones.

Temas

- Patrón de ruta
- Origen o grupo de origen
- Política de protocolo para lectores
- Métodos HTTP permitidos
- Configuración de cifrado de nivel de campo
- Métodos HTTP almacenados en caché
- Cómo permitir solicitudes de gRPC a través de HTTP/2
- Caché en función de encabezados de solicitud seleccionados
- Encabezados de lista de permitidos
- Almacenamiento de objetos en caché
- Tiempo de vida mínimo
- Tiempo de vida máximo
- Tiempo de vida (TTL) predeterminado
- Reenvío de cookies
- Cookies de lista de permitidos
- Reenvío de cadenas de consulta y almacenamiento en caché
- Lista de permitidos de cadenas de consulta

- Smooth Streaming
- Restringir el acceso del lector (usar URL firmadas o cookies firmadas)
- Firmantes de confianza
- Cuenta de AWSNúmeros de
- Comprimir objetos automáticamente
- Evento CloudFront
- ARN de la función Lambda
- Incluir cuerpo

Patrón de ruta

El patrón de ruta (por ejemplo, `images/*.jpg`) que especifica a qué solicitudes desea que sea aplicable este comportamiento de la caché. Cuando CloudFront recibe una solicitud de un usuario final, la ruta solicitada se compara con patrones de ruta en el orden en el que se enumeran los comportamientos de la caché en la distribución. La primera coincidencia determina el comportamiento de la caché que se aplicará a dicha solicitud. Por ejemplo, suponga que tiene tres comportamientos de la caché con los siguientes tres patrones de ruta, en este orden:

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

> **Note**
>
> De forma opcional, puede incluir una barra inclinada (/) al principio de la ruta de acceso, por ejemplo, `/images/*.jpg`. El comportamiento de CloudFront es el mismo con o sin la / al principio. Si no especifica “/” al principio de la ruta, este carácter se deduce de forma automática; CloudFront trata la ruta igual con el carácter “/” inicial o sin él. Por ejemplo, CloudFront trata `/*product.jpg` igual que `*product.jpg`.

Una solicitud del archivo `images/sample.gif` no satisface el primer patrón de ruta, por lo que los comportamientos de la caché asociados no se aplicarán a la solicitud. El archivo satisface el segundo patrón de ruta, por lo que los comportamientos de la caché asociados al segundo patrón de ruta se aplican a pesar de que la solicitud también coincide con el tercer patrón de ruta.

> **Note**
>
> Al crear una nueva distribución, el valor de Path Pattern (Patrón de ruta) del comportamiento de la caché predeterminado se establece como * (todos los archivos) y no puede modificarse. Este valor hace que CloudFront reenvíe todas las solicitudes de los objetos al origen que ha especificado en el campo Dominio de origen. Si la solicitud de un objeto no coincide con el patrón de ruta de ningún otro comportamiento de la caché, CloudFront aplica el comportamiento que especifique al comportamiento de la caché predeterminado.

> **Important**
>
> Defina los patrones de ruta y su orden detenidamente para evitar que los usuarios puedan acceder a contenido al que no desea otorgar acceso. Supongamos que una solicitud coincide con el patrón de ruta de dos comportamientos de la caché. El primer comportamiento de la caché no requiere URL firmadas ni cookies firmadas y el segundo requiere URL firmadas. Los usuarios pueden tener acceso a los objetos sin usar una URL firmada porque CloudFront procesa el comportamiento de la caché asociado a la primera coincidencia.

Si trabaja con un canal de MediaPackage, debe incluir patrones de ruta específicos para el comportamiento de la caché que se haya definido para el tipo de punto de enlace del origen. Por ejemplo, en el caso de un punto de enlace DASH, debería escribir `*.mpd` para Path Pattern (Patrón de ruta). Para obtener más información e instrucciones específicas, consulte Distribución de vídeo en directo formateado con AWS Elemental MediaPackage.

La ruta especificada es aplicable a las solicitudes de todos los archivos del directorio especificado y sus subdirectorios. CloudFront no tiene en cuenta las cadenas de consulta ni cookies a la hora de evaluar el patrón de ruta. Por ejemplo, si un directorio `images` contiene subdirectorios `product1` y `product2`, el patrón de ruta `images/*.jpg` resulta aplicable a las solicitudes de cualquier archivo .jpg en los directorios `images`, `images/product1`y `images/product2`. Si desea aplicar un comportamiento de la caché a los archivos del directorio `images/product1` que sea distinto al comportamiento a aplicar a los archivos de los directorios `images` y `images/product2`, cree un comportamiento de la caché independiente para `images/product1` y muévalo a la posición superior (previa) a la del comportamiento de la caché para el directorio `images`.

Puede utilizar los siguientes caracteres comodín en el patrón de ruta:

- `*` coincide con 0 o más caracteres.
- `?` coincide exactamente con 1 carácter.

Los siguientes ejemplos muestran cómo funcionan los caracteres comodín:

Patrón de ruta	Archivos que coinciden con el patrón de ruta
`*.jpg`	Todos los archivos .jpg.
`images/*.jpg`	Todos los archivos .jpg del directorio `images` y de los subdirectorios de `images`.
`a*.jpg`	• Todos los archivos .jpg cuyos nombre de archivo comienzan por `a`, por ejemplo, `apple.jpg` y `appalachian_trail_2012_05_21.jpg`. • Todos los archivos .jpg cuyas rutas de archivo comienzan por `a`, por ejemplo, `abra/cadabra/magic.jpg`.
`a??.jpg`	Todos los archivos .jpg cuyos nombres de archivo comienzan por `a` y que les siguen exactamente dos caracteres, por ejemplo, `ant.jpg` y `abe.jpg`.
`*.doc*`	Todos los archivos cuyas extensiones de nombre de archivo comienzan por `.doc`, por ejemplo, archivos `.doc`, `.docx` y `.docm`. En este caso no se puede utilizar el patrón de ruta `*.doc?`, ya que no sería aplicable a las solicitudes de archivos `.doc`; el comodín `?` sustituye exactamente un carácter.

La longitud máxima de un patrón de ruta es 255 caracteres. El valor puede contener cualquiera de los siguientes caracteres:

- A-Z, a-z

Los patrones de ruta distinguen entre mayúsculas y minúsculas, por lo que el patrón de ruta `*.jpg` no sería aplicable al archivo `LOGO.JPG`.

- 0-9
- _ - . * $ / ~ " ' @ : +
- &, pasado y devuelto como `&`

Normalización de rutas

CloudFront normaliza las rutas de URI de acuerdo con la RFC 3986 y, a continuación, hace coincidir la ruta con el comportamiento de caché correcto. Una vez que coincide el comportamiento de caché, CloudFront envía la ruta de URI sin procesar al origen. Si no coinciden, las solicitudes se ajustan al comportamiento de caché predeterminado.

Algunos caracteres se normalizan y se eliminan de la ruta, como las barras diagonales múltiples (`//`) o los puntos (`..`). Esto puede alterar la URL que CloudFront utiliza para que coincida con el comportamiento de caché previsto.

Example Ejemplo

Especifique las rutas `/a/b*` y `/a*` del comportamiento de caché.

- Un lector que envíe la ruta `/a/b?c=1` coincidirá con el comportamiento de caché `/a/b*`.
- Un lector que envíe la ruta `/a/b/..?c=1` coincidirá con el comportamiento de caché `/a*`.

Para evitar que las rutas se normalicen, puede actualizar las rutas de solicitud o el patrón de ruta del comportamiento de caché.

Origen o grupo de origen

Esta configuración solo se aplica cuando se crea o actualiza un comportamiento de caché para una distribución existente.

Especifique el valor de un origen o grupo de origen existente. Este identifica el origen o el grupo de orígenes al que desea que CloudFront dirija solicitudes cuando una solicitud (como https://example.com/logo.jpg) coincide con el patrón de ruta para un comportamiento de caché (como *.jpg) o para el comportamiento de caché predeterminado (*).

Política de protocolo para lectores

Elija la política de protocolo que desea que los lectores utilicen para acceder a su contenido en las ubicaciones de borde de CloudFront:

- HTTP and HTTPS (HTTP y HTTPS): los espectadores pueden utilizar ambos protocolos.
- Redirect HTTP to HTTPS (Redireccionamiento de HTTP a HTTPS): los espectadores pueden utilizar ambos protocolos, pero las solicitudes HTTP se redirigirán automáticamente a solicitudes HTTPS.
- HTTPS Only (Solo HTTPS): los espectadores solo pueden obtener acceso a su contenido si utilizan HTTPS.

Para obtener más información, consulte Exigencia de HTTPS para la comunicación entre lectores y CloudFront.

Métodos HTTP permitidos

Especifique los métodos HTTP que desea que CloudFront procese y reenvíe al origen:

- GET, HEAD: puede usar CloudFront solo para obtener los objetos desde su origen o para obtener encabezados de objeto.
- GET, HEAD, OPTIONS: puede utilizar CloudFront solo para obtener objetos del origen, obtener encabezados de objeto o recuperar una lista de las opciones admitidas por su servidor de origen.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE: puede utilizar CloudFront para obtener, agregar, actualizar y eliminar objetos, así como para obtener encabezados de objeto. Además, puede realizar otras operaciones de POST como enviar datos desde un formulario web.

> **Note**
>
> Si utiliza gRPC en la carga de trabajo, debe seleccionar GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. Las cargas de trabajo de gRPC requieren el método `POST`. Para obtener más información, consulte Uso de gRPC con distribuciones de CloudFront. CloudFront almacena en caché las respuestas a las solicitudes `GET` y `HEAD` y, de forma opcional, de las solicitudes `OPTIONS`. Las respuestas a las solicitudes `OPTIONS` se almacenan en caché de forma independiente de las respuestas a las solicitudes `GET` y `HEAD` (el método `OPTIONS` se incluye en la clave de caché para solicitudes `OPTIONS`).

CloudFront no almacena en caché las respuestas a las solicitudes que utilizan otros métodos.

Important

Si elige GET, HEAD, OPTIONS o GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE, seguramente necesite restringir el acceso al bucket de Amazon S3 o a su origen personalizado para que los usuarios no puedan realizar operaciones indeseadas. Los siguientes ejemplos explican cómo restringir el acceso:

- Si utiliza Amazon S3 como origen de la distribución: cree un control de acceso de origen de CloudFront para restringir el acceso a su contenido de Amazon S3 y conceda permisos al control de acceso de origen. Por ejemplo, si configura CloudFront para que acepte y reenvíe estos métodos solo porque desea utilizar `PUT`, deberá volver a configurar las políticas del bucket de Amazon S3 para gestionar las solicitudes `DELETE` de forma adecuada. Para obtener más información, consulte Restricción del acceso a un origen de Amazon S3.
- Si utiliza un origen personalizado: configure el servidor de origen para gestionar todos los métodos. Por ejemplo, si configura CloudFront para que acepte y reenvíe estos métodos solo porque desea utilizar `POST`, deberá volver a configurar el servidor de origen para gestionar las solicitudes `DELETE` de forma adecuada.

Configuración de cifrado de nivel de campo

Si desea aplicar el cifrado en el nivel de campo en campos de datos específicos, elija una configuración de cifrado en el nivel de campo en la lista desplegable.

Para obtener más información, consulte Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial.

Métodos HTTP almacenados en caché

Especifique si desea que CloudFront almacene en caché la respuesta de su origen cuando un lector envíe una solicitud `OPTIONS`. CloudFront siempre almacena en caché las respuesta a las solicitudes `GET` y `HEAD`.

Cómo permitir solicitudes de gRPC a través de HTTP/2

Especifique si desea que su distribución permita solicitudes de gRPC. Para activar el gRPC, seleccione la siguiente configuración:

- En Métodos HTTP permitidos, seleccione los métodos GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. gRPC requiere el método `POST`.
- Seleccione la casilla de verificación de gRPC que aparece después de seleccionar el método `POST`.
- En Versiones de HTTP compatibles, seleccione HTTP/2.

Para obtener más información, consulte Uso de gRPC con distribuciones de CloudFront.

Caché en función de encabezados de solicitud seleccionados

Especifique si desea que CloudFront almacene en caché objetos en función de los valores de los encabezados especificados:

- Ninguno (mejora el almacenamiento en caché): CloudFront no almacena en caché los objetos en función de los valores de encabezado.
- Lista de permitidos: CloudFront almacena en caché los objetos solo según los valores de los encabezados especificados. Utilice Encabezados de la lista de permitidos para elegir los encabezados en los que desea que CloudFront base el almacenamiento en caché.
- Todos: CloudFront no almacena en caché los objetos que están asociados con este comportamiento de la caché. En su lugar, CloudFront envía todas las solicitudes al origen. (No se recomienda para los orígenes de Amazon S3).

Independientemente de la opción que elija, CloudFront reenvía determinados encabezados a su origen y realiza acciones específicas en función de los encabezados que reenvíe. Para obtener más información acerca de cómo administra CloudFront el reenvío de encabezado, consulte Encabezados de solicitudes HTTP y comportamiento de CloudFront (personalizado y orígenes de Amazon S3).

Para obtener más información acerca de cómo configurar el almacenamiento en caché en CloudFront utilizando encabezados de solicitud, consulte Almacenamiento en caché de contenido en función de encabezados de solicitud.

Encabezados de lista de permitidos

Esta configuración solo se aplica cuando elige Lista de permisos en Caché basada en encabezados de solicitud seleccionados.

Especifique los encabezados que desea que CloudFront tenga en cuenta a la hora de almacenar los objetos en caché. Seleccione los encabezados en la lista de encabezados disponibles y elija Add (Añadir). Para reenviar un encabezado personalizado, escriba el nombre en el campo y elija Añadir personalizado.

Para obtener información sobre el número máximo actual de encabezados que puede incluir en la lista de permitidos para cada comportamiento de la caché o para solicitar una cuota (antes denominada límite) más alta, consulte Cuotas en encabezados.

Almacenamiento de objetos en caché

Si su servidor de origen está agregando un encabezado `Cache-Control` a sus objetos para controlar el tiempo durante el cual deben mantenerse en la caché de CloudFront y no desea cambiar el valor de `Cache-Control`, elija Use Origin Cache Headers (Usar encabezados de caché de origen).

Para especificar el tiempo mínimo y máximo durante el cual los objetos deben mantenerse en la caché de CloudFront independientemente de los encabezados `Cache-Control` y un tiempo predeterminado durante el cual un objeto deberá mantenerse en la caché de CloudFront cuando le falte el encabezado `Cache-Control`, elija Customize (Personalizar). A continuación, especifique los valores en los campos Minimum TTL (Tiempo de vida mínimo), Default TTL (Tiempo de vida predeterminado) y Maximum TTL (Tiempo de vida máximo).

Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Tiempo de vida mínimo

Especifique el tiempo mínimo, en segundos, que desea que los objetos permanezcan en la caché de CloudFront antes de que CloudFront envíe otra solicitud al origen para ver si el objeto se ha actualizado.

> **Warning**
>
> Si el TTL mínimo es superior a 0, CloudFront almacenará en caché el contenido al menos durante el tiempo especificado en el TTL mínimo de la política de caché, aunque estén

presentes las directivas `Cache-Control: no-cache`, `no-store` o `private` en los encabezados de origen.

Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Tiempo de vida máximo

Especifique el tiempo máximo en segundos durante el cual desea que los objetos permanezcan en las cachés de CloudFront antes de que CloudFront consulte a su origen para determinar si el objeto se ha actualizado. El valor que especifique en Maximum TTL (Tiempo de vida máximo) será aplicable solo cuando el origen personalizado añada encabezados HTTP como `Cache-Control max-age`, `Cache-Control s-maxage` o `Expires` a los objetos. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Para especificar un valor en Maximum TTL (Tiempo de vida máximo), elija la opción Customize (Personalizar) en el ajuste Object Caching (Almacenamiento de objetos en caché).

El valor predeterminado de Maximum TTL (Tiempo de vida máximo) es 31 536 000 segundos (un año). Si cambia el valor de Minimum TTL (Tiempo de vida mínimo) o de Default TTL (Tiempo de vida predeterminado) a más de 31 536 000 segundos, el valor predeterminado de Maximum TTL (Tiempo de vida máximo) cambia al valor Default TTL (Tiempo de vida predeterminado).

Tiempo de vida (TTL) predeterminado

Especifique el tiempo predeterminado, en segundos, durante el cual desea que los objetos permanezcan en las cachés de CloudFront antes de que CloudFront reenvíe otra solicitud a su origen para determinar si el objeto se ha actualizado. El valor que especifique en Periodo de vida predeterminado es aplicable solo cuando el origen no agrega encabezados HTTP como `Cache-Control max-age`, `Cache-Control s-maxage` o `Expires` a los objetos. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Para especificar un valor en Default TTL (Tiempo de vida predeterminado), elija la opción Customize (Personalizar) en el ajuste Object Caching (Almacenamiento de objetos en caché).

El valor predeterminado de Default TTL (Tiempo de vida predeterminado) es 86 400 segundos (un día). Si cambia el valor de Minimum TTL (Tiempo de vida mínimo) a más de 86 400 segundos, el

valor predeterminado de Default TTL (Tiempo de vida predeterminado) cambia al valor Minimum TTL (Tiempo de vida mínimo).

Reenvío de cookies

> **Note**
>
> Para los orígenes de Amazon S3, esta opción solo se aplica a los buckets configurados como punto de conexión del sitio web.

Especifique si desea que CloudFront reenvíe las cookies al servidor de origen y, en tal caso, cuáles de ellas. Si decide reenviar únicamente unas cookies determinadas (las contenidas en una lista de permitidos de cookies), escriba sus nombres en el campo Lista de permitidos de cookies. Si elige Todas, CloudFront reenvía todas las cookies independientemente de la cantidad que utilice la aplicación.

Amazon S3 no procesa las cookies y reenviar cookies al origen reduce la capacidad de la caché. Para comportamientos de la caché que reenvíen solicitudes a un origen de Amazon S3, elija Ninguna en Reenviar cookies.

Para obtener más información acerca del reenvío de cookies al origen, visite Almacenamiento en caché de contenido en función de cookies.

Cookies de lista de permitidos

> **Note**
>
> Para los orígenes de Amazon S3, esta opción solo se aplica a los buckets configurados como punto de conexión del sitio web.

Si eligió Lista de permitidos en la lista Reenviar cookies, escriba en el campo Lista de permitidos de cookies los nombres de las cookies que desea que CloudFront reenvíe a su servidor de origen para este comportamiento de la caché. Escriba una cookie por línea.

Puede especificar los siguientes comodines para especificar nombres de cookies:

- * coincide con 0 más caracteres en el nombre de la cookie.

- ? coincide exactamente con un carácter en el nombre de la cookie

Por ejemplo, supongamos que las solicitudes de un objeto enviadas por un espectador incluyen una cookie con el nombre:

`userid_member-number`

Donde el valor de *`member-number`* es único para cada usuario. Desea que CloudFront almacene en caché una versión independiente del objeto por cada miembro. Podría conseguirlo reenviando todas las cookies al origen, pero las solicitudes de lectores incluyen algunas que no desea que CloudFront las almacene en caché. Otra opción sería especificar el siguiente valor como nombre de cookie, lo que haría que CloudFront reenviara al origen todas las cookies que comienzan por `userid_`:

`userid_*`

Para obtener información sobre el número máximo actual de nombres de cookies que puede incluir en la lista de permitidos para cada comportamiento de la caché o para solicitar una cuota (antes denominada límite) más alta, consulte Cuotas en cookies (configuración de caché heredada).

Reenvío de cadenas de consulta y almacenamiento en caché

CloudFront puede almacenar en caché diferentes versiones del contenido en función de los valores de los parámetros de las cadenas de consulta. Elija una de las siguientes opciones:

Ninguno (mejora el almacenamiento en caché)

Seleccione esta opción si el origen devuelve la misma versión de un objeto independientemente de los valores de los parámetros de las cadenas de consulta. Esto aumenta la probabilidad de que CloudFront pueda atender una solicitud de la caché, lo que mejora el rendimiento y reduce la carga en el origen.

Reenviar todo y caché basada en lista de permitidos

Seleccione esta opción si su servidor de origen devuelve distintas versiones de sus objetos en función de uno o más parámetros de cadenas de consulta. A continuación, especifique los parámetros que desee que CloudFront utilice como base para el almacenamiento en caché en el campo Lista de permitidos de cadenas de consulta.

Reenviar todo y almacenar todo en caché

Seleccione esta opción si su servidor de origen devuelve distintas versiones de sus objetos para todos los parámetros de cadenas de consulta.

Para obtener más información acerca del almacenamiento en caché en función de los parámetros de las cadenas de consulta y acerca de formas de mejorar el desempeño, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta.

Lista de permitidos de cadenas de consulta

Esta configuración se aplica solo cuando elige Reenviar todo y caché basada en lista de permitidos para Reenvío de cadenas de consulta y almacenamiento en caché. Puede especificar los parámetros de cadena de consulta que quiera que CloudFront utilice como base para el almacenamiento en caché.

Smooth Streaming

Elija Yes (Sí) si desea distribuir archivos multimedia en el formato Microsoft Smooth Streaming y no dispone de un servidor de IIS.

Elija No si tiene un servidor Microsoft IIS que desea utilizar como origen para distribuir archivos multimedia en el formato Microsoft Smooth Streaming, o si no distribuye archivos multimedia Smooth Streaming.

> **Note**
>
> Si especifica Yes (Sí), puede seguir distribuyendo otro tipo de contenido con este comportamiento de la caché si dicho contenido coincide con el valor de Path Pattern (Patrón de ruta).

Para obtener más información, consulte Configuración de vídeo bajo demanda para Microsoft Smooth Streaming.

Restringir el acceso del lector (usar URL firmadas o cookies firmadas)

Si desea que las solicitudes de objetos que coinciden con el valor de `PathPattern` en este comportamiento de la caché utilicen direcciones URL públicas, elija No.

Si desea que las solicitudes de objetos que coinciden con el valor de `PathPattern` en este comportamiento de la caché utilicen direcciones URL firmadas, elija Yes (Sí). A continuación, especifique las cuentas de AWS que desea utilizar para crear URL firmadas; a estas cuentas se les conoce como signatarios de confianza.

Para obtener más información acerca de los signatarios de confianza, consulte Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas.

Firmantes de confianza

Esta configuración solo se aplica cuando elige Sí en Restringir acceso al lector (Usar URL firmadas o cookies firmadas).

Seleccione las cuentas de AWS que desea utilizar como signatarios de confianza para este comportamiento de la caché:

- Self (Automático): utilice la cuenta con la que tiene iniciada sesión en la Consola de administración de AWS como signatario de confianza. Si actualmente su sesión se inició como usuario de IAM, la cuenta de AWS asociada se agrega como signatario de confianza.
- Specify Accounts (Especificar cuentas): escriba los números de cuenta de los signatarios de confianza en el campo de AWSAccount Numbers (Números de cuenta).

Para crear URL firmadas, la cuenta de AWS debe tener al menos un par de claves activas de CloudFront.

> **Important**
>
> Si está actualizando una distribución que ya utiliza para distribuir contenido, añada signatarios de confianza solo cuando esté listo para comenzar a generar URL firmadas para los objetos. Después de añadir signatarios de confianza a una distribución, los usuarios deben utilizar las URL firmadas para obtener acceso a los objetos que coincidan con `PathPattern` para este comportamiento de la caché.

Cuenta de AWSNúmeros de

Esta configuración solo se aplica cuando elige Especificar cuentas en Firmantes de confianza.

Si desea crear URL firmadas a través de cuentas de Cuentas de AWS además de, o en lugar de, hacerlo con la cuenta actual, ingrese un número de cuenta de Cuenta de AWS por línea en este campo. Tenga en cuenta lo siguiente:

- Las cuentas que especifique deben tener al menos un par de claves de CloudFront activo. Para obtener más información, consulte Creación de pares de claves para los firmantes.

- No puede crear pares de claves de CloudFront para usuarios de IAM, lo que significa que no puede utilizar usuarios de IAM como signatarios de confianza.
- Para obtener información acerca de cómo obtener el número de Cuenta de AWS para una cuenta, consulte Ver identificadores de Cuenta de AWS en la Guía de referencia de administración de Cuenta de AWS.
- Si escribe el número de la cuenta actual, CloudFront marca automáticamente la casilla Automático y elimina el número de cuenta de la lista AWS de Números de cuenta.

Comprimir objetos automáticamente

Si desea que CloudFront comprima automáticamente archivos de tipos determinados cuando los lectores admiten contenido comprimido, elija Sí. Cuando CloudFront comprime el contenido, las descargas son más veloces, ya que los archivos son más pequeños y las páginas web se muestran más rápido a los usuarios. Para obtener más información, consulte Ofrecimiento de archivos comprimidos.

Evento CloudFront

Esta configuración se aplica a las Asociaciones de funciones de Lambda.

Puede elegir ejecutar una función de Lambda cuando se produzcan uno o varios de los siguientes eventos de CloudFront:

- Cuando CloudFront reciba una solicitud de un espectador (solicitud del espectador)
- Antes de que CloudFront reenvíe una solicitud al origen (solicitud al origen)
- Cuando CloudFront reciba una respuesta del origen (respuesta del origen)
- Antes de que CloudFront devuelva la respuesta al espectador (respuesta al espectador)

Para obtener más información, consulte Elección del evento para desencadenar la función.

ARN de la función Lambda

Esta configuración se aplica a las Asociaciones de funciones de Lambda.

Especifique el nombre de recurso de Amazon (ARN) de la función de Lambda para la que desea agregar un desencadenador. Para obtener información sobre cómo obtener el ARN de una función, consulte el paso 1 del procedimiento Agregar desencadenadores mediante la consola de CloudFront.

Incluir cuerpo

Esta configuración se aplica a las Asociaciones de funciones de Lambda.

Para obtener más información, consulte Incluir cuerpo.

Ajustes de la distribución

Los siguientes valores se aplican a toda la distribución.

Temas

- Clase de precio
- ACL web de AWS WAF
- Nombres de dominio alternativos (CNAME)
- Certificado SSL
- Compatibilidad con clientes SSL personalizados
- Política de seguridad (versión mínima de SSL/TLS)
- Versiones de HTTP compatibles
- Objeto raíz predeterminado
- Registro estándar
- Registros de conexiones
- Prefijo de registros
- Registro de cookies
- Habilitación de IPv6 (solicitudes de espectadores)
- Autenticación mutua
- Habilitación de IPv6 para los orígenes personalizados (solicitudes de origen)
- Comment
- Estado de la distribución

Clase de precio

Elija la clase de precio que corresponde al precio máximo que desea pagar por el servicio de CloudFront. De forma predeterminada, CloudFront distribuye sus objetos desde ubicaciones de borde en todas las regiones de CloudFront.

Para obtener más información acerca de las clases de precios y cómo la clase que elija afecta al rendimiento de CloudFront para la distribución, consulte Precios de CloudFront.

ACL web de AWS WAF

Puede proteger la distribución de CloudFront con AWS WAF, un firewall de aplicaciones web que le permite proteger las aplicaciones web y las API para bloquear las solicitudes antes de que lleguen a los servidores. Puede Habilitación de AWS WAF para distribuciones al crear o editar una distribución de CloudFront.

Si lo desea, puede configurar más adelante protecciones de seguridad adicionales para otras amenazas específicas de la aplicación en la consola de AWS WAF en https://console.aws.amazon.com/wafv2/.

Para obtener más información sobre AWS WAF, consulte la Guía para desarrolladores de AWS WAF.

Nombres de dominio alternativos (CNAME)

Opcional. Especifique uno o varios nombres de dominio que desee utilizar para direcciones URL de sus objetos en lugar del nombre de dominio que CloudFront asigna al crear la distribución. Debe ser el propietario del nombre de dominio, o tener autorización para utilizarlo, lo que puede demostrar añadiendo un certificado SSL/TLS.

Por ejemplo, si desea que la URL del objeto:

```
/images/image.jpg
```

Sea así:

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

En lugar de así:

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

Añada un CNAME para `www.example.com`.

> **Important**
>
> Si añade un CNAME para `www.example.com` a la distribución, también debe hacer lo siguiente:

- Crear o actualizar un registro de CNAME en el servicio de DNS para dirigir las consultas de `www.example.com` a `d111111abcdef8.cloudfront.net`.
- Agregar un certificado a CloudFront de una entidad de certificación (CA) de confianza emitido para el nombre de dominio (CNAME) que va a agregar a la distribución, con el fin de demostrar que dispone de autorización para utilizar el nombre de dominio.

Debe tener permiso para crear un registro CNAME con el proveedor de servicios de DNS para el dominio. Por lo general, esto indica que es el propietario del dominio o que está desarrollando una aplicación para el propietario del dominio.

Para obtener el número máximo actual de nombres de dominio alternativos que puede agregar a una distribución o solicitar una cuota (antes denominada límite) más alta, consulte Cuotas generales de distribuciones.

Para obtener más información acerca de los nombres de dominio alternativos, consulte Uso de URL personalizadas añadiendo nombres de dominio alternativos (CNAME). Para obtener más información acerca de las direcciones URL de CloudFront, consulte Personalización del formato de URL para archivos en CloudFront.

Certificado SSL

Si ha especificado un nombre de dominio alternativo para usarlo con la distribución, seleccione Custom SSL Certificate (Certificado SSL personalizado) y, a continuación, para validar su autorización para utilizar el nombre de dominio alternativo, elija un certificado emitido para él. Si desea que los espectadores utilicen HTTPS para obtener acceso a sus objetos, elija el ajuste correspondiente.

- Default CloudFront Certificate (*.cloudfront.net) (Certificado de CloudFront predeterminado (*.cloudfront.net)): elija esta opción si desea utilizar el nombre de dominio de CloudFront en las URL de los objetos, por ejemplo, `https://d111111abcdef8.cloudfront.net/image1.jpg`.
- Custom SSL Certificate (Certificado SSL personalizado): elija esta opción si desea utilizar su propio nombre de dominio en las URL de sus objetos como nombre de dominio alternativo; por ejemplo `https://example.com/image1.jpg`. A continuación, elija un certificado que haya sido emitido para el nombre de dominio alternativo. En la lista de certificados puede haber los elementos siguientes:

- Certificados proporcionados por AWS Certificate Manager
- Certificados adquiridos a una entidad de certificación de terceros y cargados en ACM
- Certificados adquiridos a una entidad de certificación de terceros y cargados en el almacén de certificados de IAM

Si elige esta opción, le recomendamos que utilice solo un nombre de dominio alternativo en las URL de sus objetos (https://example.com/logo.jpg). Si utiliza el nombre de dominio de la distribución de CloudFront (https://d111111abcdef8.cloudfront.net/logo.jpg) y un cliente utiliza un lector antiguo que no admite SNI, la respuesta del lector depende del valor que elija para Clients Supported (Clientes admitidos):

- All Clients (Todos los clientes): el lector muestra una advertencia, ya que el nombre de dominio de CloudFront no coincide con el nombre de dominio del certificado SSL/TLS.
- Only Clients that Support Server Name Indication (SNI) (Solo los clientes que admiten indicación de nombre de servidor (SNI)): CloudFront interrumpe la conexión con el lector sin devolver el objeto.

Compatibilidad con clientes SSL personalizados

Se aplica solo cuando elige Certificado SSL personalizado (example.com) en Certificado SSL. Si especificó uno o más nombres de dominio alternativos y un certificado SSL personalizado para la distribución, elija cómo desea que CloudFront sirva las solicitudes HTTPS:

- Clientes compatibles con la indicación de nombre de servidor (SNI) - (recomendado): con esta configuración, prácticamente todos los navegadores web y clientes modernos pueden conectarse a la distribución, ya que admiten SNI. Sin embargo, algunos usuarios pueden utilizar navegadores web antiguos o clientes que no admiten SNI, lo que significa que no pueden conectarse a la distribución.

  Para aplicar esta configuración mediante la API de CloudFront, especifique `sni-only` en el campo `SSLSupportMethod`. En CloudFormation, el campo se denomina `SslSupportMethod`, (tenga en cuenta el uso de mayúsculas y minúsculas).
- Compatibilidad con clientes heredados: con esta configuración, los navegadores web antiguos y los clientes que no admiten SNI pueden conectarse a la distribución. Sin embargo, a esta configuración se le aplican cargos mensuales adicionales. Para obtener el precio exacto, vaya a la página Precios de Amazon CloudFront y busque la página de SSL personalizado de IP dedicada.

Para aplicar esta configuración mediante la API de CloudFront, especifique `vip` en el campo `SSLSupportMethod`. En CloudFormation, el campo se denomina `SslSupportMethod` (tenga en cuenta el uso de mayúsculas y minúsculas).

Para obtener más información, consulte Elección de la forma en que CloudFront atiende las solicitudes HTTPS.

Política de seguridad (versión mínima de SSL/TLS)

Especifique la política de seguridad que desea que utilice CloudFront para las conexiones HTTPS con lectores (clientes). Una política de seguridad determina dos ajustes:

- El protocolo SSL/TLS mínimo que utiliza CloudFront para comunicarse con los lectores.
- El cifrado que puede utilizar CloudFront para cifrar el contenido que devuelve a los espectadores.

Para obtener más información acerca de las políticas de seguridad, incluidos los protocolos y los cifrados que incluye cada una, consulte Protocolos y cifrados admitidos entre lectores y CloudFront.

Las políticas de seguridad disponibles dependen de los valores que especifique para el Certificado SSL y el Soporte de cliente SSL personalizado (conocidos como `CloudFrontDefaultCertificate` y `SSLSupportMethod` en la API de CloudFront):

- Cuando el SSL Certificate (Certificado SSL) es el Default CloudFront Certificate (*.cloudfront.net) (Certificado predeterminado de CloudFront (*.cloudfront.net)) (cuando `CloudFrontDefaultCertificate` es `true` en la API), CloudFront configura automáticamente la política de seguridad a TLSv1.
- Cuando el Certificado SSL es el Certificado SSL personalizado (ejemplo.com) y el Soporte de cliente SSL personalizado es Clientes que admiten la indicación de nombre de servidor (SNI) - (Recomendado) (cuando `CloudFrontDefaultCertificate` es `false` y `SSLSupportMethod` es `sni-only` en la API), puede elegir entre las siguientes políticas de seguridad:
  - TLSv1.3_2025
  - TLSv1.2_2025
  - TLSv1.2_2021
  - TLSv1.2_2019
  - TLSv1.2_2018

  - TLSv1.1_2016
  - TLSv1_2016
  - TLSv1
- Cuando el Certificado SSL es el Certificado SSL personalizado (ejemplo.com) y el Soporte de cliente SSL personalizado es Soporte de clientes heredados (cuando `CloudFrontDefaultCertificate` es `false` y `SSLSupportMethod` es `vip` en la API), puede elegir entre las siguientes políticas de seguridad:
  - TLSv1
  - SSLv3

  En esta configuración, las políticas de seguridad TLSv1.3_2025, TLSv1.2_2025, TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016, y TLSv1_2016 no están disponibles en la API ni en la consola de CloudFront. Si desea utilizar una de estas políticas de seguridad, tiene las siguientes opciones:

  - Evalúe si su distribución necesita soporte de clientes heredados con direcciones IP dedicadas. Si los espectadores admiten la indicación de nombre de servidor (SNI), recomendamos que actualice la configuración de Soporte de cliente SSL personalizado de la distribución a Clientes que admiten la indicación de nombre de servidor (SNI) (configure `SSLSupportMethod` como `sni-only` en la API). Esto le permite utilizar cualquiera de las políticas de seguridad TLS disponibles y también puede reducir sus cargos de CloudFront.
  - Si tiene que mantener el soporte de clientes heredados con direcciones IP dedicadas, puede solicitar alguna de las otras políticas de seguridad de TLS (TLSv1.3_2025, TLSv1.2_2025, TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016 o TLSv1_2016) mediante la creación de un caso en el Centro de soporte de AWS.

  > **Note**
  >
  > Antes de contactar con AWS Support para solicitar este cambio, tenga en cuenta lo siguiente:
  >
  > - Cuando agrega una de estas políticas de seguridad (TLSv1.3_2025, TLSv1.2_2025, TLSv1.2_2021, TLSv1.2_2019, TLSv1.2_2018, TLSv1.1_2016 o TLSv1_2016) a una distribución de soporte de clientes heredados, la política de seguridad se aplica a todas las solicitudes de espectador que no sean SNI para todas las distribuciones de soporte de clientes heredados en la cuenta de AWS. En cambio, cuando los espectadores envían solicitudes SNI a una distribución con soporte de clientes

heredados, se aplica la política de seguridad de dicha distribución. Para asegurarse de que se aplica su política de seguridad deseada a todas las solicitudes de lector enviadas a todas las distribuciones de soporte de clientes heredados en su cuenta de AWS, agregue la política de seguridad deseada a cada distribución individualmente.

- Por definición, la nueva política de seguridad no admite los mismos cifrados y protocolos que la anterior. Por ejemplo, si decide actualizar la política de seguridad de una distribución de TLSv1 a TLSv1.1_2016, esa distribución ya no admitirá el cifrado DES-CBC3-SHA. Para obtener más información sobre los cifrados y protocolos compatibles con cada política de seguridad, consulte Protocolos y cifrados admitidos entre lectores y CloudFront.

Versiones de HTTP compatibles

Elija las versiones de HTTP que desea que admita la distribución cuando los lectores se comuniquen con CloudFront.

Para que los lectores y CloudFront utilicen HTTP/2, los lectores deben ser compatibles con TLSv1.2 o posterior y con la indicación de nombre de servidor (SNI).

Para que los lectores y CloudFront utilicen HTTP/3, los lectores deben ser compatibles con TLSv1.3 y con la indicación del nombre del servidor (SNI). CloudFront es compatible con la migración de la conexión HTTP/3 para que el lector pueda cambiar de red sin perder la conexión. Para obtener más información sobre la migración de conexiones, consulte Connection Migration (Migración de conexiones) en RFC 9000.

> **Note**
>
> Para obtener más información acerca de los cifrados TLSv1.3, consulte Protocolos y cifrados admitidos entre lectores y CloudFront.

> **Note**
>
> Si utiliza Amazon Route 53, puede utilizar registros HTTPS para permitir la negociación de protocolos como parte de la búsqueda de DNS si el cliente lo admite. Para obtener más información, consulte Create alias resource record set.

Objeto raíz predeterminado

Opcional. El objeto que quiera que CloudFront solicite desde su origen (por ejemplo, `index.html`) cuando un lector solicite la URL raíz de la distribución (`https://www.example.com/`) en lugar de un objeto de la distribución (`https://www.example.com/product-description.html`). Especificar un objeto raíz predeterminado evita exponer el contenido de su distribución.

La longitud máxima de un nombre es 255 caracteres. El nombre puede contener cualquiera de los siguientes caracteres:

- A-Z, a-z
- 0-9
- _ - . * $ / ~ " '
- &, pasado y devuelto como `&`

Al especificar el objeto raíz predeterminado, escriba únicamente el nombre de objeto, por ejemplo, `index.html`. No añada `/` antes del nombre del objeto.

Para obtener más información, consulte Especificación de un objeto raíz predeterminado.

Registro estándar

Especifique si desea que CloudFront registre información acerca de cada solicitud de un objeto y almacene los archivos de registro. Puede habilitar o deshabilitar el registro de acceso en cualquier momento. No se aplica ningún cargo adicional si activa el registro, pero se podrían acumular cargos por almacenar y acceder a los archivos. Puede eliminar los registros en cualquier momento.

CloudFront admite las siguientes opciones de registro estándar:

- Registro estándar (v2): puede enviar registros a los destinos de entrega, incluidos los registros de Amazon CloudWatch, Amazon Data Firehose y Amazon Simple Storage Service (Amazon S3).
- Registro estándar (heredado): solo puede enviar registros a un bucket de Amazon S3.

Registros de conexiones

Al activar la autenticación mutua para la distribución, CloudFront proporciona registros de conexión que capturan atributos sobre las solicitudes enviadas a las distribuciones. Los registros de conexión contienen información como la dirección IP y el puerto del cliente, la información del certificado del

cliente, los resultados de la conexión y los cifrados TLS que se utilizan. Estos registros de conexión se pueden usar luego para revisar los patrones de solicitudes y otras tendencias.

Para obtener más información sobre los registros de conexión, consulte . Observabilidad mediante registros de conexión.

Prefijo de registros

(Opcional) Si activa el registro estándar (heredado), especifique la cadena, de haberla, a la que CloudFront debe agregar un prefijo para los nombres de archivo de los registros de acceso de esta distribución; por ejemplo, `examplepref ix/`. La barra inclinada (/) al final es opcional pero recomendable para simplificar la navegación de los archivos de registro. Para obtener más información, consulte Configuración del registro estándar (heredado).

Registro de cookies

Si desea que CloudFront incluya cookies en los registros de acceso, elija On. Si decide incluir las cookies en los registros, CloudFront registra todas las cookies independientemente de cómo configura los comportamientos de la caché para esta distribución: para reenviar al origen todas las cookies, ninguna o las que se determinen en una lista concreta.

Amazon S3 no procesa las cookies, por lo que, a menos que la distribución también incluya un origen de Amazon EC2 u otro personalizado, le recomendamos que elija el valor Off en Registros de cookies.

Para obtener más información acerca de cookies, consulte Almacenamiento en caché de contenido en función de cookies.

Habilitación de IPv6 (solicitudes de espectadores)

Si desea que CloudFront responda a las solicitudes de los espectadores desde direcciones IP IPv4 e IPv6, seleccione Habilitar IPv6. Para obtener más información, consulte Habilitación de IPv6 para las distribuciones de CloudFront.

Autenticación mutua

Opcional. Tiene la opción de elegir activar la autenticación mutua para la distribución de CloudFront. Para obtener más información, consulte Autenticación TLS mutua con CloudFront (mTLS de espectador).

Habilitación de IPv6 para los orígenes personalizados (solicitudes de origen)

Cuando utiliza un origen personalizado (excepto los orígenes de Amazon S3 y VPC), puede personalizar la configuración de origen de la distribución para elegir la forma en que CloudFront se conecta al origen mediante direcciones IPv4 o IPv6. Para obtener más información, consulte Habilitación de IPv6 para las distribuciones de CloudFront.

Comment

Opcional. Al crear una distribución, puede incluir un comentario de hasta 128 caracteres. Puede actualizarlo en cualquier momento.

Estado de la distribución

Indica si desea habilitar o deshabilitar la distribución una vez implementada:

- Enabled (Habilitada) significa que tan pronto como la distribución se implemente totalmente, podrá implementar enlaces que utilizan el nombre de dominio de la distribución y los usuarios podrán recuperar contenido. Cuando una distribución está habilitada, CloudFront acepta y gestiona cualquier solicitud de contenido realizada por cualquier usuario final y que utilice el nombre de dominio asociado a esa distribución.

  Al crear, modificar o eliminar una distribución de CloudFront, lleva tiempo propagar los cambios a la base de datos de CloudFront. Una solicitud inmediata para obtener información acerca de una distribución puede no mostrar el cambio. La propagación suele completarse en cuestión de minutos, pero una carga de sistema o una partición de red elevadas podrían aumentar este tiempo.
- Disabled (Deshabilitada) significa que, aunque la distribución puede haberse implementado y estar lista para su uso, los usuarios no pueden utilizarla. Cuando una distribución está desactivada, CloudFront no acepta ninguna solicitud realizada por ningún usuario final y que utilice el nombre de dominio asociado a esa distribución. Hasta que no cambie la distribución de deshabilitada a habilitada (actualizando de la distribución de la configuración), nadie podrá utilizarla.

Puede cambiar una distribución entre habilitada y deshabilitada tantas veces como quiera. Siga el proceso para actualizar la configuración de una distribución. Para obtener más información, consulte Actualizar una distribución.

Páginas de error personalizadas y almacenamiento de errores en caché

Puede hacer que CloudFront devuelva un objeto al lector (por ejemplo, un archivo HTML) cuando su origen de Amazon S3 u origen personalizado devuelve un código de estado HTTP 4xx y 5xx de CloudFront. También puede especificar por cuánto tiempo almacenar en las cachés de borde de CloudFront una respuesta de error desde su origen o una página de error personalizada. Para obtener más información, consulte Creación de una página de error personalizada para códigos de estado HTTP específicos.

> **Note**
>
> Los siguientes valores no se incluyen en el asistente Create Distribution, lo que significa que solo puede configurar páginas de error personalizadas al actualizar una distribución.

Temas

- Código de error HTTP
- Ruta de la página de respuesta
- Código de respuesta HTTP
- TTL mínimo de almacenamiento de errores en caché (segundos)

Código de error HTTP

El código de estado HTTP para el que desea que CloudFront devuelva una página de error personalizada. Puede configurar CloudFront para devolver páginas de error personalizadas para ninguno, algunos o todos los códigos de estado HTTP que CloudFront almacena en caché.

Ruta de la página de respuesta

La ruta a la página de error personalizada (por ejemplo, `/4xx-errors/403-forbidden.html`) que desea que CloudFront lector a un lector cuando el origen devuelve el código de estado HTTP especificado en Error Code (Código de error) (por ejemplo, 403). Si desea almacenar los objetos y las páginas de error personalizadas en diferentes ubicaciones, la distribución debe incluir un comportamiento de la caché que cumpla con las siguientes condiciones:

- El valor de Path Pattern (Patrón de ruta) debe coincidir con la ruta de los mensajes de error personalizados. Por ejemplo, supongamos que ha guardado páginas para errores 4xx

personalizadas en un bucket de Amazon S3 en un directorio llamado `/4xx-errors`. La distribución debe incluir un comportamiento de caché cuyo patrón de ruta dirija las solicitudes de las páginas de error personalizadas a esa ubicación, por ejemplo, /4xx-errors/*.

- El valor de Origin (Origen) especifica el valor de Origin ID (ID de origen) del origen que contiene las páginas de error personalizadas.

Código de respuesta HTTP

El código de estado HTTP que desea que CloudFront devuelva al lector junto con la página de error personalizada.

TTL mínimo de almacenamiento de errores en caché (segundos)

El tiempo mínimo que desee que CloudFront almacene en caché las respuestas de error de su servidor de origen.

Restricciones geográficas

Si necesita impedir que los usuarios de países concretos accedan al contenido, puede configurar la distribución de CloudFront con una Lista de permitidos o una Lista de bloqueados. No se aplica ningún cargo adicional por la configuración de restricción geográfica. Para obtener más información, consulte Restricción de la distribución geográfica de su contenido.

Prueba de una distribución

Una vez creada la distribución, CloudFront; conocerá el lugar en el que se encuentra su servidor de origen, y usted sabrá el nombre de dominio asociado a la distribución. Para probar la distribución, haga lo siguiente:

1. Espere a que se implemente la distribución.
   - Vea los detalles de su distribución en la consola. Cuando la distribución termine de implementarse, el campo Última modificación cambiará de Implementando a una fecha y hora.
2. Cree enlaces a sus objetos con el nombre de dominio de CloudFront mediante el siguiente procedimiento.
3. Pruebe los enlaces. CloudFront envía los objetos a su página web o aplicación.

Creación de enlaces a sus objetos

Utilice el siguiente procedimiento para crear enlaces de prueba para los objetos de la distribución web de CloudFront.

Crear enlaces a objetos en una distribución web

1. Copie el siguiente código HTML a un nuevo archivo, sustituya *domain-name* con el nombre de dominio de su distribución y sustituya *object-name* con el nombre de su objeto.

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

   Por ejemplo, si su nombre de dominio es `d111111abcdef8.cloudfront.net` y su objeto es `image.jpg`, la URL del vínculo será:

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

   Si su objeto se encuentra en una carpeta del servidor de origen, la carpeta también deberá incluirse en la URL. Por ejemplo, si image.jpg estaba situada en la carpeta de imágenes de su servidor de origen, la URL debería ser:

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

2. Guarde el código HTML en un archivo que tenga una extensión .html.
3. Abra su página web en un navegador para asegurarse de que pueda ver su objeto.

El navegador devolverá su página con el archivo de imagen integrado, ofrecido desde la ubicación de borde que CloudFront determinó que era adecuada para servir el objeto.

Actualizar una distribución

En la consola de CloudFront, puede ver las distribuciones de CloudFront asociadas a la Cuenta de AWS, así como la configuración de una distribución y puede actualizar la mayoría de los ajustes. Tenga en cuenta que los cambios de configuración que realice no surtirán efecto sino hasta que la distribución no haya propagado a las ubicaciones periféricas de AWS.

Actualización de una distribución en la consola

Los siguientes procedimientos muestran cómo actualizar una distribución de CloudFront en la consola.

Multi-tenant

Actualización de una distribución de varios inquilinos

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Busque y elija el ID de la distribución de varios inquilinos.
3. Elija la pestaña para la configuración que desea actualizar.
4. Realice las actualizaciones y, a continuación, para guardar los cambios, elija Guardar cambios. Para obtener más información acerca de la configuración que puede actualizar, consulte Referencia de la configuración de distribución preconfigurada.

También puede actualizar una distribución con la API de CloudFront:

- Para actualizar una distribución, consulte UpdateDistribution en la Referencia de API de Amazon CloudFront.

> **Important**
>
> Al actualizar la distribución, tenga en cuenta que hay una serie de campos adicionales necesarios que no se necesitan al crear por primera vez una distribución. Para asegurarse de que todos los campos obligatorios se incluyen cuando utilice la API de CloudFront para actualizar una distribución, siga los pasos que se describen en UpdateDistribution en la Referencia de la API de Amazon CloudFront.

Para cambiar la distribución de varios inquilinos de un inquilino de distribución, actualice el inquilino de distribución. También debe actualizar el inquilino de distribución para actualizar su dominio, certificado, personalizaciones o valores de parámetros. Para obtener más información sobre la actualización del certificado del inquilino de distribución, consulte Agregación de un dominio y un certificado (inquilino de distribución).

Actualización de un inquilino de distribución

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En SaaS, elija Inquilinos de distribución.
3. Busque el inquilino de distribución. Utilice el menú desplegable de la barra de búsqueda para filtrar por dominio, nombre, ID de distribución, ID de certificado, ID de grupo de conexión o ID de ACL web.
4. Elija el nombre del inquilino de la distribución.
5. Para actualizar los Detalles generales, elija Editar, realice las actualizaciones y elija Actualizar inquilino de distribución.
6. Elija la pestaña adecuada para actualizar cualquier otra configuración, realice las actualizaciones y guárdelas. Para obtener más información acerca de la configuración de distribución del inquilino que puede personalizar, consulte Personalizaciones de inquilinos de distribución.

Standard

Actualización de una distribución estándar

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleccione el ID de una distribución. La lista incluye todas las distribuciones asociadas a la cuenta de AWS que utilizó para iniciar sesión en la consola de CloudFront.
3. Para actualizar la configuración general, elija Edit (Editar). De lo contrario, elija la pestaña de la configuración que desea actualizar.
4. Realice las actualizaciones y, a continuación, elija Guardar cambios. Para obtener información acerca de los campos, consulte los siguientes temas:
   - Configuración general: Ajustes de la distribución

- Configuración del origen: Configuración de origen
- Configuración del comportamiento de la caché: Configuración del comportamiento de la caché

5. Si desea eliminar un origen de la distribución, haga lo siguiente:

   a. Elija Behaviors (Comportamientos) y asegúrese de que ha movido a otro origen los comportamientos predeterminados de la caché asociados con el origen.

   b. Elija Origins (Orígenes) y, a continuación, seleccione un origen.

   c. Elija Eliminar.

También puede actualizar una distribución con la API de CloudFront:

- Para actualizar una distribución, consulte UpdateDistribution en la Referencia de API de Amazon CloudFront.

> **Important**
>
> Al actualizar su distribución, tenga en cuenta que hay una serie de campos adicionales necesarios que no se necesitan para crear una distribución. Para asegurarse de que todos los campos obligatorios se incluyen cuando utilice la API de CloudFront para actualizar una distribución, siga los pasos que se describen en UpdateDistribution en la Referencia de la API de Amazon CloudFront.

Al guardar los cambios en la configuración de su distribución, CloudFront comienza a propagar los cambios en todas las ubicaciones periféricas. Los cambios de configuración sucesivos se propagan en su orden respectivo. Hasta que la configuración se actualiza en una ubicación periférica, CloudFront continúa ofreciendo el contenido desde dicha ubicación en función de la configuración anterior. Después de que la configuración se actualiza en una ubicación de borde, CloudFront comienza a ofrecer el contenido inmediatamente desde dicha ubicación en función de la configuración nueva.

Los cambios no se propagan a todas las ubicaciones periféricas al mismo tiempo. Aunque CloudFront propaga los cambios, no podemos determinar si una ubicación periférica concreta está ofreciendo su contenido en función de la configuración anterior o de la nueva.

> **Note**
>
> En raras ocasiones, cuando se interrumpe un enlace de red o host, es posible que parte del tráfico de inquilinos de distribución se atienda con configuraciones antiguas durante un breve periodo hasta que se ingresen los cambios en la red.

Para ver cuándo se propagan los cambios, consulte los Detalles de su distribución en la consola. El campo Última modificación cambia de Implementando a una fecha y hora cuando se ha completado la implementación.

Etiquetado de una distribución

Las etiquetas son palabras o frases que puede utilizar para identificar y organizar sus recursos de AWS. Puede añadir varias etiquetas a cada recurso, y cada etiqueta incluye una clave y un valor que usted define. Por ejemplo, la clave puede ser "dominio" y el valor puede ser "example.com". Puede buscar y filtrar sus recursos en función de las etiquetas que añada.

Puede usar etiquetas con CloudFront, como en los ejemplos siguientes:

- Aplicación de permisos basados en etiquetas a las distribuciones de CloudFront. Para obtener más información, consulte ABAC con CloudFront.
- Seguimiento de la información de facturación en diferentes categorías. Al aplicar etiquetas a distribuciones de CloudFront y a otros recursos de AWS (por ejemplo, instancias de Amazon EC2 o buckets de Amazon S3) y activarlas, AWS genera un informe de asignación de costos en formato de valores separados por comas (archivo CSV) con el uso y los costos agrupados por etiquetas activas.

  Puede aplicar etiquetas que representen categorías de negocio (por ejemplo, centros de costos, nombres de aplicación o propietarios) para estructurar los costos entre diferentes servicios. Para obtener más información sobre el uso de etiquetas para la asignación de costes, consulte Uso de etiquetas de asignación de costes en la Guía del usuario de AWS Billing.

> **Notas**
>
> - Puede etiquetar distribuciones, pero no puede etiquetar identidades de acceso de origen ni invalidaciones.

- El editor de etiquetas y los grupos de recursos no son compatibles con CloudFront.
- Para consultar el máximo actual de la cantidad de etiquetas que puede agregar a una distribución web, consulte Cuotas generales.

Contenido

- Restricciones de las etiquetas
- Adición, edición y eliminación de etiquetas para distribuciones
- Etiquetado programático

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- Para comprobar el número máximo de etiquetas por distribución, consulte Cuotas generales.
- Longitud máxima de la clave: 128 caracteres Unicode.
- Longitud máxima del valor: 256 caracteres Unicode.
- Valores válidos para claves y valores: a-z, A-Z, 0-9, espacio y los siguientes caracteres: _ . : / = + - y @
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas
- No utilice `aws:` como prefijo para claves. Este prefijo se reserva para uso de AWS.

Adición, edición y eliminación de etiquetas para distribuciones

Puede usar la consola de CloudFront para administrar etiquetas para sus distribuciones.

Para añadir, editar o eliminar etiquetas en una distribución

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la ID de la distribución que desea actualizar.
3. Elija la pestaña Tags.
4. Elija Administrar etiquetas.
5. En la página Administrar etiquetas, puede hacer lo siguiente:

- Para agregar una etiqueta, especifique una clave y, de forma opcional, un valor para la etiqueta. Para agregar más etiquetas, elija Agregar nueva etiqueta.
- Para editar una etiqueta, cambie la clave de la etiqueta, su valor, o ambos. También puede eliminar el valor de una etiqueta, pero la clave es necesaria.
- Para eliminar una etiqueta, elija Eliminar.

6. Seleccione Save changes (Guardar cambios).

Etiquetado programático

También puede usar la API de CloudFront, AWS Command Line Interface (AWS CLI), los SDK de AWS y AWS Tools for Windows PowerShell para aplicar etiquetas. Para obtener más información, consulte los temas siguientes:

- Operaciones de la API de CloudFront:
  - ListTagsForResource
  - TagResource
  - UntagResource
- AWS CLI: consulte cloudfront en la Referencia de comandos de AWS CLI
- SDK de AWS: consulte la documentación del SDK correspondiente en la página Documentación de AWS.
- Tools for Windows PowerShell: consulte Amazon CloudFront en la Referencia de Cmdlet de Herramientas de AWS para PowerShell

Eliminar una distribución

El siguiente procedimiento elimina una distribución mediante la consola de CloudFront. Para obtener información sobre la eliminación con la API de CloudFront, consulte DeleteDistribution en la Referencia de la API de Amazon CloudFront.

Si necesita eliminar una distribución con un OAC adjunto a un bucket de S3, consulte en Eliminación de una distribución con un OAC adjunto a un bucket de S3 los detalles importantes.

Warning

- Antes de poder eliminar una distribución, debe desactivarla, lo que requiere permiso para actualizar la distribución. Una vez eliminada, la distribución no se puede recuperar.
- Si desactiva una distribución que tiene asociado un nombre de dominio alternativo, CloudFront deja de aceptar tráfico para ese nombre de dominio (por ejemplo, www.ejemplo.com), aunque haya otra distribución que tenga un nombre de dominio alternativo con un carácter comodín (*) que coincida con el mismo dominio (por ejemplo, *.example.com).
- No puede eliminar una distribución que esté suscrita a un Plan de precios de tarifa fija de CloudFront. Recibirá un mensaje de error que dice: “No puede eliminar esta distribución mientras esté suscrita a un plan de precios”. Primero debe cancelar el plan de precios y, después del ciclo de facturación actual, eliminar la distribución.

Multi-tenant

Antes de eliminar una distribución de varios inquilinos, primero debe eliminar todos los inquilinos de distribución asociados.

Eliminación de una distribución de varios inquilinos

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel derecho de la consola de CloudFront, elija el nombre de la distribución de varios inquilinos que desea eliminar.
3. En Inquilinos, seleccione y elimine todos los inquilinos de distribución asociados.
4. Elija Desactivar para desactivar la distribución y elija Desactivar distribución para confirmar la operación.
5. Espere a que aparezca la nueva marca temporal en la columna Última modificación.
   - Puede que CloudFront tarde unos minutos en propagar el cambio a todas las ubicaciones periféricas.
6. Elija Eliminar, Eliminar distribución.

Eliminación de un inquilino de distribución

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En SaaS, elija Inquilinos de distribución.
3. Busque el inquilino de distribución. Utilice el menú desplegable de la barra de búsqueda para filtrar por dominio, nombre, ID de distribución, ID de certificado, ID de grupo de conexión o ID de ACL web.
4. Seleccione el inquilino de distribución que desee eliminar.
5. Elija Eliminar inquilino, Eliminar inquilino de distribución.

Standard

Eliminación de una distribución estándar

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel derecho de la consola de CloudFront, busque la distribución que desea eliminar.
   - Si la columna Estado muestra que la distribución ya está Desactivada, vaya al paso 6.
   - Si el Estado muestra Habilitado, pero la distribución sigue mostrando Implementando en la columna Última modificación, espere a que finalice la implementación antes de continuar con el paso 3.
3. En el panel derecho de la consola de CloudFront, seleccione la casilla de la distribución que desea eliminar.
4. Elija Disable (Deshabilitar) para deshabilitar la distribución y elija Yes, Disable (Sí, deshabilitar) para confirmar la operación. A continuación, seleccione Close (Cerrar).
   - El valor de la columna Estado cambia de forma inmediata a Deshabilitado.
5. Espere a que aparezca la nueva marca temporal en la columna Última modificación.
   - Puede que CloudFront tarde unos minutos en propagar el cambio a todas las ubicaciones periféricas.
6. Seleccione la casilla de verificación de la distribución que desea eliminar.
7. Elija Delete (Eliminar), Delete (Eliminar).

- Si la opción Eliminar no está disponible, eso significa que CloudFront sigue propagando el cambio a las ubicaciones periféricas. Espere a que aparezca la nueva marca temporal en la columna Última modificación y después repita los pasos 6 y 7.

Uso de varios orígenes con distribuciones de CloudFront

Cuando cree una distribución, especifique el origen al que CloudFront envía las solicitudes de los archivos. Puede utilizar varios tipos de orígenes con CloudFront. Por ejemplo, puede utilizar un bucket de Amazon S3, un contenedor MediaStore, un canal MediaPackage, un Application Load Balancer o una URL de función AWS Lambda. Al crear la distribución de CloudFront, CloudFront configura automáticamente gran parte de la configuración de distribución por usted, en función del tipo de origen del contenido. Para obtener más información, consulte Referencia de la configuración de distribución preconfigurada.

Si tiene un equilibrador de carga de aplicación, un equilibrador de carga de red o una instancia de EC2 de una subred privada, puede usarlos como origen de la VPC. Con los orígenes de la VPC, solo se puede acceder a las aplicaciones en una subred privada con una distribución de CloudFront, lo que impide que la aplicación sea accesible en Internet pública. Para obtener más información, consulte the section called “Restricción del acceso con orígenes de la VPC”.

> **Note**
>
> Puede utilizar las funciones periféricas para seleccionar dinámicamente el origen apropiado para cada solicitud. Al usar CloudFront Functions o Lambda@Edge, puede dirigir las solicitudes a diferentes orígenes en función de factores como la ubicación geográfica del espectador, los encabezados de la solicitud o los parámetros de la cadena de consulta. Para obtener más información, consulte Personalización en la periferia con funciones.

Temas

- Uso de un bucket de Amazon S3
- Uso de un contenedor de MediaStore o un canal de MediaPackage
- Uso de un equilibrador de carga de aplicación
- Uso de un equilibrador de carga de red
- Uso de una URL de función de Lambda

- Uso de Amazon EC2 (u otro origen personalizado)
- Uso de los grupos de origen de CloudFront
- Uso de Amazon API Gateway

Uso de un bucket de Amazon S3

En los siguientes temas se describen las diferentes formas en que puede utilizar un bucket de Amazon S3 como origen para una distribución de CloudFront.

Temas

- Uso de un bucket de Amazon S3 estándar
- Uso de Amazon S3 Object Lambda
- Uso de puntos de acceso de Amazon S3
- Uso de un bucket de Amazon S3 configurado como punto de conexión del sitio web
- Adición de CloudFront a un bucket de Amazon S3 existente
- Traslado de un bucket de Amazon S3 a otra Región de AWS

Uso de un bucket de Amazon S3 estándar

Cuando utiliza Amazon S3 como origen para su distribución, coloque los objetos que desee que CloudFront entregue en un bucket de Amazon S3. Puede utilizar cualquier método admitido por Amazon S3 para incorporar sus objetos a Amazon S3. Por ejemplo, puede utilizar la consola o la API de Amazon S3, o una herramienta de terceros. Puede crear una jerarquía en su bucket para almacenar los objetos, del mismo modo que lo haría con cualquier otro bucket de Amazon S3 estándar.

El uso de un bucket de Amazon S3 ya existente como su servidor de origen de CloudFront no cambia el bucket en absoluto. Puede utilizarlo como lo haría normalmente para almacenar y obtener acceso a los objetos de Amazon S3 a precios estándar de Amazon S3. Se le cobrarán los cargos habituales de Amazon S3 por almacenar los objetos en el bucket. Para obtener más información acerca de los cargos por usar CloudFront, consulte Precios de Amazon CloudFront. Para obtener más información sobre el uso de CloudFront con un bucket de S3 existente, consulte the section called “Adición de CloudFront a un bucket de Amazon S3 existente”.

> **Important**
>
> Para que su bucket pueda funcionar con CloudFront, el nombre debe cumplir los requisitos de nomenclatura de DNS. Para obtener más información, consulte Reglas para nombrar buckets en la Guía del usuario de Amazon Simple Storage Service.

Cuando especifique un bucket de Amazon S3 como origen para CloudFront, le recomendamos que utilice el siguiente formato:

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

Cuando especifique el nombre del bucket en este formato, puede utilizar las siguientes características de CloudFront:

- Configure CloudFront para que se comunique con su bucket de Amazon S3 mediante SSL/TLS. Para obtener más información, consulte the section called “Uso de HTTPS con CloudFront”.
- Utilice un control de acceso de origen para solicitar que los lectores obtengan acceso al contenido utilizando la URL de CloudFront, y no mediante las URL de Amazon S3. Para obtener más información, consulte the section called “Restricción del acceso a un origen de Amazon S3”.
- Actualice el contenido de su bucket mediante el envío de las solicitudes `POST` y `PUT` a CloudFront. Para obtener más información, consulte the section called “Métodos HTTP” en el tema the section called “Cómo CloudFront procesa y reenvía solicitudes a su origen de Amazon S3”.

No especifique el bucket con los siguientes formatos:

- El estilo de ruta de Amazon S3: `s3.amazonaws.com/bucket-name`
- El CNAME de Amazon S3

> **Note**
>
> CloudFront admite orígenes de S3 que utilizan cualquier clase de almacenamiento, incluido S3 Intelligent-Tiering. Cuando CloudFront solicita objetos de un origen de S3, estos se recuperan independientemente del nivel de almacenamiento en el que se encuentren actualmente. El uso de CloudFront con S3 Intelligent-Tiering no afecta al rendimiento ni a la funcionalidad de la distribución. Para obtener más información, consulte Administración de

los costos de almacenamiento con Amazon S3 Intelligent-Tiering en la Guía del usuario de Amazon Simple Storage Service.

Uso de Amazon S3 Object Lambda

Al crear un punto de acceso de Object Lambda, Amazon S3 genera automáticamente un alias único para el punto de acceso de Object Lambda. Puede utilizar este alias en lugar de un nombre de bucket de Amazon S3 como origen para la distribución de CloudFront.

Cuando utilice un alias de punto de acceso de Object Lambda como origen para CloudFront, le recomendamos que utilice el siguiente formato:

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

Para obtener más información acerca de cómo encontrar el *alias*, consulte Cómo usar un alias de estilo bucket para el punto de acceso de Object Lambda de bucket de S3 en la Guía del usuario de Amazon S3.

> **Important**
>
> Cuando utilice un punto de acceso de Object Lambda como origen para CloudFront, debe utilizar el control de acceso de origen.

Para ver un ejemplo de caso de uso, consulte Uso de Amazon S3 Object Lambda con Amazon CloudFront para personalizar el contenido para los usuarios finales.

CloudFront trata un origen de punto de acceso de Object Lambda de la misma manera que un origen de bucket de Amazon S3 estándar.

Si utiliza Amazon S3 Object Lambda como origen para la distribución, debe configurar los cuatro permisos siguientes.

Object Lambda Access Point

Cómo agregar permisos para el punto de acceso de Object Lambda

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación, elija Puntos de acceso de Object Lambda.

3. Elija el punto de acceso de Object Lambda que desea usar.
4. Elija la pestaña Permisos.
5. Elija Editar en la sección Política de punto de acceso de Object Lambda.
6. Pegue la siguiente política en el campo Política.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3-object-lambda:Get*",
            "Resource": "arn:aws:s3-object-lambda:us-
east-1:123456789012:accesspoint/Object-Lambda-Access-Point-name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/CloudFront-distribution-
ID"
                }
            }
        }
    ]
}
```

7. Seleccione Save changes (Guardar cambios).

Amazon S3 Access Point

Cómo agregar permisos para el punto de acceso de Amazon S3

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación, elija Puntos de acceso.
3. Elija el punto de acceso de Amazon S3 que desea usar.

4. Elija la pestaña Permisos.
5. Elija Editar en la sección Política de punto de acceso.
6. Pegue la siguiente política en el campo Política.

   JSON

```
{
    "Version":"2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name/object/*"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "s3-object-lambda.amazonaws.com"
                }
            }
        }
    ]
}
```

7. Seleccione Save.

Amazon S3 bucket

Cómo agregar permisos al bucket de Amazon S3

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.

2. En el panel de navegación, elija Buckets.
3. Elija el bucket de Amazon S3 que desea usar.
4. Elija la pestaña Permisos.
5. Elija Editar en la sección Política de bucket.
6. Pegue la siguiente política en el campo Política.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:DataAccessPointAccount": "AWS-account-ID"
                }
            }
        }
    ]
}
```

7. Seleccione Save changes (Guardar cambios).

AWS Lambda function

Cómo agregar permisos a la función de Lambda

1. Inicie sesión en la Consola de administración de AWS y abra la consola AWS Lambda en https://console.aws.amazon.com/lambda/.
2. Seleccione Funciones en el panel de navegación.

3. Elija la función AWS Lambda que desea usar.
4. Elija la pestaña Configuración y, a continuación, elija Permisos.
5. Elija Agregar permisos en la sección Instrucciones de políticas basadas en recursos.
6. Elija Cuenta de AWS.
7. Ingrese un nombre para el ID de instrucción.
8. Ingrese `cloudfront.amazonaws.com` para Entidad principal.
9. Elija `lambda:InvokeFunction` del menú desplegable Acción.
10. Seleccione Save.

Uso de puntos de acceso de Amazon S3

Al usar un punto de acceso de S3, Amazon S3 genera automáticamente un alias único para usted. Puede utilizar este alias en lugar de un nombre de bucket de Amazon S3 como origen para la distribución de CloudFront.

Cuando utilice un alias de punto de acceso de Amazon S3 como origen para CloudFront, le recomendamos que utilice el siguiente formato:

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

Para obtener más información acerca de cómo encontrar el *alias*, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en la Guía del usuario de Amazon S3.

> **Important**
>
> Cuando utilice un punto de acceso de Amazon S3 como origen para CloudFront, debe utilizar el control de acceso de origen.

CloudFront trata un origen de Punto de acceso de Amazon S3 de la misma manera que un origen de bucket de Amazon S3 estándar.

Al utilizar Amazon S3 Object Lambda como origen para la distribución, se deben configurar los dos permisos siguientes.

Amazon S3 Access Point

Cómo agregar permisos para el punto de acceso de Amazon S3

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación, elija Puntos de acceso.
3. Elija el punto de acceso de Amazon S3 que desea usar.
4. Elija la pestaña Permisos.
5. Elija Editar en la sección Política de punto de acceso.
6. Pegue la siguiente política en el campo Política.

   JSON

```
{
    "Version":"2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {"Service": "cloudfront.amazonaws.com"},
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name/object/*"
            ],
            "Condition": {
                "StringEquals": {"aws:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/CloudFront-distribution-
ID"}
            }
        }
    ]
}
```

7. Seleccione Save.

Amazon S3 bucket

Cómo agregar permisos al bucket de Amazon S3

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación, elija Buckets.
3. Elija el bucket de Amazon S3 que desea usar.
4. Elija la pestaña Permisos.
5. Elija Editar en la sección Política de bucket.
6. Pegue la siguiente política en el campo Política.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:DataAccessPointAccount": "AWS-account-ID"
                }
            }
        }
    ]
}
```

7. Seleccione Save changes (Guardar cambios).

Uso de un bucket de Amazon S3 configurado como punto de conexión del sitio web

Puede usar un bucket de Amazon S3 que está configurado como punto de conexión del sitio web como un origen personalizado con CloudFront. Al configurar su distribución de CloudFront, para el origen, escriba el punto de enlace de alojamiento de sitio web estático de Amazon S3 para el bucket. Este valor aparecerá en la consola de Amazon S3 en la pestaña Properties (Propiedades), en el panel Static website hosting (Alojamiento de sitio web estático). Por ejemplo:

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

Para obtener más información sobre cómo especificar los puntos de enlace de sitios web estáticos de Amazon S3, consulte Website endpoints (Puntos de enlace de sitio web) en la Guía del usuario de Amazon Simple Storage Service.

Al especificar el nombre del bucket en este formato como origen, puede utilizar redireccionamientos y documentos de error personalizados de Amazon S3. Para obtener más información, consulte Configuración de un documento de error personalizado y Configuración de una redirección en la Guía del usuario de Amazon Simple Storage Service. (CloudFront también ofrece páginas de error personalizadas; para obtener más información, consulte). the section called “Creación de una página de error personalizada para códigos de estado HTTP específicos”.)

El uso de un bucket de Amazon S3 como servidor de origen de CloudFront no cambia el bucket de ninguna manera. Puede seguir utilizándolo como lo haría normalmente y se le cobrarán los cargos normales de Amazon S3. Para obtener más información acerca de los cargos por usar CloudFront, consulte Precios de Amazon CloudFront.

> **Note**
>
> Si utiliza la API de CloudFront para crear su distribución con un bucket de Amazon S3 configurado como punto de enlace de un sitio web, debe configurarlo mediante `CustomOriginConfig`, aunque el sitio web esté alojado en un bucket de Amazon S3. Para obtener más información acerca de la creación de distribuciones mediante la API de CloudFront, consulte CreateDistribution en la Referencia de la API de Amazon CloudFront.

Adición de CloudFront a un bucket de Amazon S3 existente

Si almacena sus objetos en un bucket de Amazon S3, puede permitir que los usuarios obtengan acceso a sus objetos directamente desde S3 o puede configurar CloudFront para obtener sus objetos desde S3 y distribuirlos después a los usuarios. Usar CloudFront puede ser más rentable si sus

usuarios obtienen acceso a sus objetos frecuentemente porque si el uso es elevado, el precio de transferencia de datos de CloudFront es menor que el de Amazon S3. Además, las descargas son más rápidas con CloudFront que con solo Amazon S3 porque sus objetos se almacenan más cerca de sus usuarios.

> **Note**
>
> Si desea que CloudFront respete la configuración de uso compartido de recursos de origen cruzado de Amazon S3, configure CloudFront para que reenvíe el encabezado `Origin` a Amazon S3. Para obtener más información, consulte the section called "Almacenamiento en caché de contenido en función de encabezados de solicitud".

Si actualmente distribuye contenido directamente desde el bucket de Amazon S3 con su nombre de dominio propio (como example.com) en lugar del nombre de dominio del bucket de Amazon S3 (como amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com), puede agregar CloudFront sin interrupciones con el siguiente procedimiento.

Para agregar CloudFront cuando ya esté distribuyendo su contenido desde Amazon S3

1. Crear una distribución de CloudFront. Para obtener más información, consulte the section called "Creación de una distribución".

   Al crear la distribución, especifique el nombre de su bucket de Amazon S3 como servidor de origen.

   > **Important**
   >
   > Para que su bucket pueda funcionar con CloudFront, el nombre debe cumplir los requisitos de nomenclatura de DNS. Para obtener más información, consulte Reglas para nombrar buckets en la Guía del usuario de Amazon Simple Storage Service.

   Si está utilizando un CNAME con Amazon S3, especifique también el CNAME de su distribución.

2. Cree una página web de prueba que contenga enlaces a objetos legibles públicamente en su bucket de Amazon S3 y pruebe dichos enlaces. Para esta prueba inicial, utilice el nombre de dominio de CloudFront de su distribución en las URL de sus objetos, por ejemplo, `https://d111111abcdef8.cloudfront.net/images/image.jpg`.

Para obtener más información acerca del formato de las URL de CloudFront, consulte the section called “Personalización de URL de archivo”.

3. Si utiliza CNAME de Amazon S3, la aplicación usa su nombre de dominio (por ejemplo, example.com) para hacer referencia a los objetos del bucket de Amazon S3 en lugar de utilizar el nombre del bucket (por ejemplo, amzn-s3-demo-bucket.s3.amazonaws.com). Para seguir utilizando su nombre de dominio para hacer referencia a objetos en lugar de usar el nombre de dominio de CloudFront de su distribución (por ejemplo, d111111abcdef8.cloudfront.net), debe actualizar la configuración con su proveedor de servicios de DNS.

   Para que los CNAME de Amazon S3 funcionen, su proveedor de servicios de DNS debe tener un conjunto de registros de recursos de CNAME para su dominio que actualmente dirija las consultas del dominio a su bucket de Amazon S3. Por ejemplo, si un usuario solicita este objeto:

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

   la solicitud se redirige automáticamente y el usuario ve este objeto:

   ```
   https://amzn-s3-demo-bucket.s3.amazonaws.com/images/image.jpg
   ```

   Para dirigir consultas a su distribución de CloudFront en lugar a de su bucket de Amazon S3, deberá utilizar el método proporcionado por su proveedor de servicios DNS para actualizar el conjunto de registros de recursos de CNAME de su dominio. Este registro de CNAME actualizado redirige consultas de DNS de su dominio al nombre de dominio de CloudFront de su distribución. Para obtener más información, consulte la documentación de su proveedor de servicios de DNS.

   > **Note**
   >
   > Si utiliza Route 53 como servicio de DNS, puede utilizar un conjunto de registros de recursos de CNAME o un conjunto de registros de recursos de alias. Para obtener información acerca de la edición de conjuntos de registros de recursos, consulte Edición de registros. Para obtener información sobre los conjuntos de registros de recursos de alias, consulte Elección entre registros de alias y sin alias. Ambos temas se encuentran en la Guía para desarrolladores de Amazon Route 53.

   Para obtener más información acerca del uso de CNAME con CloudFront, consulte the section called “Uso de URL personalizadas”.

Después de actualizar el conjunto de registros de recursos de CNAME, la propagación a lo largo del sistema DNS puede tardar hasta 72 horas, aunque suele ser más rápida. Durante este tiempo, algunas de las solicitudes de contenido seguirán dirigiéndose a su bucket de Amazon S3 y otras se dirigirán a CloudFront.

Traslado de un bucket de Amazon S3 a otra Región de AWS

Si utiliza Amazon S3 como origen de una distribución de CloudFront y cambia el bucket de Región de AWS, CloudFront puede tardar hasta una hora en actualizar sus registros para usar la nueva región si las dos condiciones siguientes se cumplen:

- Utiliza una identidad de acceso de origen (OAI) de CloudFront para restringir el acceso al bucket
- Cambia el bucket de Amazon S3 a una región que requiera autenticación mediante Signature Version 4

Cuando utiliza OAI, CloudFront utiliza la región (entre otros valores) para calcular la firma que se utiliza para solicitar los objetos de su bucket. Para obtener más información acerca de OAI, consulte the section called “Uso de una identidad de acceso de origen (heredado, no recomendado)”. Para obtener una lista de Regiones de AWS que admiten Signature Version 2, consulte Proceso de firma de Signatura Version 2 en la Referencia general de Amazon Web Services.

Para forzar una actualización más rápida de los registros de CloudFront, puede actualizar su distribución de CloudFront, por ejemplo, con la actualización del campo Descripción en la pestaña General de la consola de CloudFront. Cuando usted actualiza una distribución, CloudFront comprueba inmediatamente la región en la que se encuentra su bucket. La propagación del cambio a todas las ubicaciones de borde debería durar solo unos minutos.

Uso de un contenedor de MediaStore o un canal de MediaPackage

Para transmitir vídeo mediante CloudFront, puede configurar un bucket de Amazon S3 configurado como contenedor MediaStore o crear un canal y puntos de conexión con MediaPackage. A continuación, deberá crear y configurar una distribución en CloudFront para transmitir el vídeo.

Para obtener más información e instrucciones paso a paso, consulte los temas siguientes:

- the section called “Distribución de vídeo utilizando AWS Elemental MediaStore como origen”

- the section called “Distribución de vídeo en directo formateado con AWS Elemental MediaPackage”

Uso de un equilibrador de carga de aplicación

Puede usar CloudFront para enrutar el tráfico a equilibradores de carga de aplicaciones internos y a orientados a Internet.

Si el origen es uno o varios servidores HTTP(S) (servidores web) alojados en una o varias instancias de Amazon EC2, tiene la opción de elegir utilizar un equilibrador de carga de aplicación orientado a Internet para distribuir el tráfico a las instancias. Un equilibrador de carga expuesto a Internet tiene un nombre de DNS que se puede resolver públicamente y direcciona las solicitudes de los clientes a través de Internet hasta los destinos.

Para obtener más información sobre el uso de un equilibrador de carga de aplicación orientado a Internet como el origen para CloudFront, incluido cómo asegurarse de que los espectadores solo puedan acceder a los servidores web a través de CloudFront y no accediendo directamente al equilibrador de carga, consulte the section called “Restricción del acceso a Application Load Balancer”.

Otra opción, puede usar orígenes de VPC para entregar contenido desde aplicaciones alojadas con un equilibrador de carga de aplicación interno en las subredes privadas de la nube privada virtual (VPC). Orígenes de la VPC impide que se pueda acceder a la aplicación en la Internet pública. Para obtener más información, consulte Restricción del acceso con orígenes de la VPC.

Uso de un equilibrador de carga de red

Puede utilizar equilibradores de carga de red internos y orientados a Internet con Amazon CloudFront. Puede usar equilibradores de carga de red internos dentro de subredes privadas con CloudFront mediante orígenes de la VPC. Los orígenes de la VPC de CloudFront le permiten ofrecer contenido de aplicaciones alojadas en subredes de la VPC privadas sin exponerlas a Internet pública. Para obtener más información, consulte Restricción del acceso con orígenes de la VPC.

Otra opción, también puede usar CloudFront para entregar tráfico desde equilibradores de carga de red orientados a Internet. Un equilibrador de carga orientado a Internet tiene un nombre de DNS que se puede resolver públicamente y puede recibir solicitudes de clientes en Internet y de distribuciones de CloudFront.

Uso de una URL de función de Lambda

Una URL de una función de Lambda es un punto de conexión HTTPS dedicado a una función de Lambda. Puede utilizar una URL de función de Lambda para crear una aplicación web sin servidor completamente dentro de Lambda. Puede invocar la aplicación web Lambda directamente a través de la URL de la función, sin necesidad de integrarse con API Gateway ni un Application Load Balancer.

Si crea una aplicación web sin servidor mediante funciones de Lambda con URL de función, puede agregar CloudFront para obtener los siguientes beneficios:

- Acelerar su aplicación con el almacenamiento en caché de los contenidos más cerca de los lectores
- Utilizar un nombre de dominio personalizado para su aplicación web
- Dirigir diferentes rutas de URL a distintas funciones Lambda mediante comportamientos de caché de CloudFront
- Bloquear solicitudes específicas mediante las restricciones geográficas de CloudFront o AWS WAF (o ambas)
- Utilizar AWS WAF con CloudFront para proteger su aplicación de los bots maliciosos, prevenir las vulnerabilidades comunes de las aplicaciones y mejorar la protección contra los ataques DDoS.

Para utilizar una URL de función Lambda como origen de una distribución de CloudFront, especifique el nombre de dominio completo de la URL de función Lambda como dominio de origen. Un nombre de dominio de la URL de la función Lambda utiliza el siguiente formato:

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

Cuando utilice una URL de función de Lambda como origen para una distribución de CloudFront, la URL de la función debe ser de acceso público. Para ello, utilice una de las siguientes opciones:

- Si usa el control de acceso de origen (OAC), el parámetro `AuthType` de la URL de la función de Lambda debe usar el valor `AWS_IAM` y conceder los permisos `lambda:InvokeFunctionUrl` y `lambda:InvokeFunction` en una política basada en recursos. Para obtener más información sobre el uso de URL de funciones de Lambda para OAC, consulte Restricción del acceso a un origen de URL de función de AWS Lambda.
- Si no utiliza OAC, puede establecer el parámetro `AuthType` de la URL de función como `NONE` y autorizar el permiso `lambda:InvokeFunctionUrl` en una política basada en recursos.

También puede agregar un encabezado de origen personalizado a las solicitudes que CloudFront envía al origen y escribir un código de función para devolver una respuesta de error si el encabezado no está presente en la solicitud. Esto contribuye a garantizar que los usuarios solo puedan acceder a su aplicación web a través de CloudFront y no utilizando directamente la URL de función de Lambda.

Para obtener más información sobre las URL de función Lambda, consulte los siguientes temas en la Guía para desarrolladores de AWS Lambda:

- URL de función Lambda: información general sobre la característica de las URL de función Lambda
- Invocación de URL de función Lambda: incluye detalles sobre las cargas útiles de solicitud y respuesta que debe utilizar para codificar su aplicación web sin servidor
- Modelo de seguridad y autenticación para las URL de funciones de Lambda: incluye detalles sobre los tipos de autenticación de Lambda

Uso de Amazon EC2 (u otro origen personalizado)

Puede utilizar instancias de EC2 internas y orientadas a Internet con Amazon CloudFront. Puede usar instancias de EC2 internas dentro de subredes privadas con CloudFront mediante orígenes de la VPC. Los orígenes de la VPC de CloudFront le permiten servir contenido desde aplicaciones alojadas en subredes de VPC privadas sin exponerlas a Internet pública. Para obtener más información, consulte Restricción del acceso con orígenes de la VPC.

Un origen personalizado es un servidor web HTTP(S) con un nombre de DNS que se puede resolver públicamente y que enruta las solicitudes de los clientes a destinos a través de Internet. El servidor HTTP(S) se puede alojar en AWS (por ejemplo, una instancia de Amazon EC2) o en otro lugar. Un origen de Amazon S3 configurado como punto de conexión de sitio web también se considera un origen personalizado. Para obtener más información, consulte the section called “Uso de un bucket de Amazon S3 configurado como punto de conexión del sitio web”.

Cuando use su propio servidor HTTP como origen personalizado, especifique el nombre DNS del servidor, junto con los puertos HTTP y HTTPS, y el protocolo que desea que CloudFront utilice al obtener objetos de su origen.

La mayoría de las características de CloudFront se admiten al utilizar un origen personalizado, excepto el contenido privado. Aunque puede utilizar una URL firmada para distribuir contenido desde un origen personalizado, para que CloudFront obtenga acceso al origen personalizado, el origen

debe mantenerse accesible públicamente. Para obtener más información, consulte the section called "Restricción de contenido con URL firmadas y cookies firmadas".

Siga estas directrices para utilizar instancias de Amazon EC2 y otros orígenes personalizados con CloudFront.

- Aloje y distribuya el mismo contenido en todos los servidores que están distribuyendo contenido para el mismo origen de CloudFront. Para obtener más información, consulte the section called "Configuración de origen" en el tema the section called "Toda la configuración de distribución".
- Registre las entradas del encabezado `X-Amz-Cf-Id` en todos los servidores en caso de que necesite Soporte o CloudFront utilice este valor para la depuración.
- Restrinja las solicitudes a los puertos HTTP y HTTPS que escucha su origen personalizado.
- Sincronice los relojes de todos los servidores de su implementación. Tenga en cuenta que CloudFront utiliza la hora universal coordinada (UTC, por sus siglas en inglés) para las URL y cookies firmadas, para los registros y los informes. Además, si monitorea la actividad de CloudFront mediante las métricas de CloudWatch, tenga en cuenta que CloudWatch también utiliza UTC.
- Utilice servidores redundantes para gestionar errores.
- Para obtener más información acerca del uso de un origen personalizado para ofrecer contenido privado, consulte the section called "Restricción del acceso a archivos en orígenes personalizados".
- Para obtener más información acerca del comportamiento de solicitudes y respuestas y códigos de estado HTTP admitidos, consulte Comportamiento de solicitudes y respuestas.

Si utiliza Amazon EC2 para un origen personalizado, le recomendamos que haga lo siguiente:

- Utilice una Imagen de máquina de Amazon que instale el software de un servidor web automáticamente. Para obtener más información, consulte la documentación de Amazon EC2.
- Utilice un balanceador de carga de Elastic Load Balancing para gestionar el tráfico en varias instancias de Amazon EC2 y aislar la aplicación de los cambios realizados en las instancias de Amazon EC2. Por ejemplo, si utiliza un balanceador de carga, puede agregar y eliminar instancias Amazon EC2 sin cambiar su aplicación. Para obtener más información, consulte la Documentación de Elastic Load Balancing.
- Al crear su distribución de CloudFront, especifique la URL del balanceador de carga para el nombre de dominio del servidor de origen. Para obtener más información, consulte the section called "Creación de una distribución".

Uso de los grupos de origen de CloudFront

Puede especificar un grupo de origen para su origen de CloudFront si, por ejemplo, desea configurar escenarios de conmutación por error de origen cuando necesite alta disponibilidad. Utilice una conmutación por error de origen para designar un origen principal para CloudFront además de un segundo origen al que CloudFront cambia automáticamente cuando el origen principal devuelve respuestas de error de código de estado HTTP específicas.

Para obtener más información, incluidos los pasos para configurar un grupo de origen, consulte the section called “Aumento de alta disponibilidad con conmutación por error”.

Uso de Amazon API Gateway

Puede usar API Gateway como origen personalizado para la distribución de CloudFront. Para obtener más información, consulte los temas siguientes:

- Entrada de blog de AWS Securing Amazon API Gateway with secure ciphers using Amazon CloudFront
- Cómo configuro API Gateway con mi propia distribución de CloudFront? AWS re:Post

Habilitación de IPv6 para las distribuciones de CloudFront

Amazon CloudFront admite IPv4 e IPv6 desde los clientes hasta las ubicaciones periféricas de AWS. CloudFront también admite IPv6 y la conectividad de doble pila (IPv4 e IPv6) con origen. Esto le ayuda a lograr una entrega de IPv6 de extremo a extremo.

IPv6 es el protocolo de Internet de próxima generación diseñado para reemplazar a IPv4. Mientras IPv4 usa direcciones de 32 bits (como 192.0.2.44), IPv6 usa direcciones de 128 bits (como 2001:0db8:85a3::8a2e:0370:7334). IPv6 proporciona un espacio de direcciones ampliado para dar cabida a más dispositivos conectados a Internet.

Temas

- Solicitudes de espectadores de IPv6
- Solicitudes de origen de IPv6

Solicitudes de espectadores de IPv6

En general, debe habilitar IPv6 si tiene usuarios en redes IPv6 que desean obtener acceso a su contenido. Sin embargo, si utiliza URL firmadas o cookies firmadas para restringir el acceso a su contenido además de una política personalizada con el parámetro `IpAddress` para restringir las direcciones IP que pueden obtener acceso a su contenido, no habilite IPv6. Si desea restringir el acceso a algún contenido por dirección IP pero no restringir otro contenido (o restringir el acceso, pero no por dirección IP), puede crear dos distribuciones. Para obtener información acerca de cómo crear URL firmadas mediante una política personalizada, consulte Creación de una URL firmada mediante una política personalizada. Para obtener información acerca de cómo crear cookies firmadas mediante una política personalizada, consulte Establecimiento de cookies firmadas mediante una política personalizada.

Si utiliza un conjunto de registros de recursos de alias de Amazon Route 53 para dirigir el tráfico a su distribución de CloudFront, debe crear un segundo conjunto de registros de recursos de alias cuando las dos condiciones siguientes se cumplan:

- Ha habilitado IPv6 para la distribución.
- Está utilizando nombres de dominio alternativo en las URL de sus objetos.

Para obtener más información, consulte Direccionamiento del tráfico a una distribución de Amazon CloudFront mediante el nombre de dominio en la Guía para desarrolladores de Amazon Route 53.

Si ha creado un conjunto de registros de recursos de CNAME, ya sea con Route 53 o con otro servicio de DNS, no es necesario realizar ningún cambio. Un registro CNAME dirige el tráfico hacia la distribución, sin tener en cuenta el formato de la dirección IP de la solicitud del espectador.

Si habilita IPv6 y registros de acceso de CloudFront, la columna `c-ip` incluye valores en formato IPv4 e IPv6. Para obtener más información, consulte Campos de un archivo de registro.

> **Note**
>
> Para mantener una alta disponibilidad para los clientes, CloudFront responde a solicitudes de los lectores a través de IPv4 si nuestros datos sugieren que ese protocolo proporcionará una mejor experiencia de usuario. Para saber qué porcentaje de solicitudes CloudFront atiende por IPv6, habilite el registro de CloudFront para su distribución y analice la columna `c-ip`, que contiene la dirección IP del lector que hizo la solicitud. Este porcentaje debería crecer con el paso del tiempo, pero seguirá siendo una minoría de tráfico ya que IPv6 aún

no es compatible con todas las redes de espectadores en todo el mundo. Algunas redes de espectadores tienen excelente compatibilidad con IPv6, pero otras no admiten IPv6 en absoluto. (En este sentido, una red de espectadores es sinónimo de su red doméstica u operador de Internet).
Para obtener más información acerca de la compatibilidad con IPv6, consulte las preguntas frecuentes de CloudFront. Para obtener más información sobre la activación de registros de acceso, consulte los campos Registro estándar y Prefijo de registros.

Solicitudes de origen de IPv6

Cuando utiliza un origen personalizado (excepto los orígenes de Amazon S3 y VPC), puede personalizar la configuración de origen de la distribución para elegir la forma en que CloudFront se conecta al origen mediante direcciones IPv4 o IPv6. Para los orígenes personalizados (excepto los orígenes de Amazon S3 y VPC), dispone de las siguientes opciones de conectividad:

- Solo IPv4 (predeterminado): esta es la configuración predeterminada que CloudFront usa para conectarse a los orígenes a través de IPv4.
- Solo IPv6: requiere que el dominio de origen se resuelva en una dirección IPv6. CloudFront utilizará exclusivamente direcciones IPv6 para las conexiones de origen.
- Pila doble: permite conexiones mediante IPv4 e IPv6. CloudFront elige automáticamente la conectividad de origen IPv4 o IPv6 para priorizar el rendimiento y la disponibilidad, de modo que pueda usar CloudFront como puerta de enlace de Internet de doble pila IPv6 e IPv4 para las aplicaciones web.

Elija la opción que se ajuste a los requisitos de conectividad y configuración de red del origen. Para obtener más información, consulte Diseño de DNS para IPv6 y consideraciones de seguridad y supervisión de IPv6.

Uso de la implementación continua de CloudFront para probar de forma segura los cambios en la configuración de la CDN

Con la implementación continua de Amazon CloudFront, puede implementar de forma segura los cambios en la configuración de su CDN realizando primero pruebas con un subconjunto del tráfico de producción. Puede utilizar una distribución provisional y una política de implementación

continua para enviar parte del tráfico de los lectores reales (de producción) a la nueva configuración de CDN y validar que funciona según lo esperado. Puede supervisar el rendimiento de la nueva configuración en tiempo real y promover la nueva configuración para que sirva todo el tráfico a través de la distribución principal cuando esté preparado.

En el siguiente diagrama, se muestran las ventajas de utilizar la implementación continua de CloudFront. Sin ella, tendría que probar los cambios en la configuración de la CDN con tráfico simulado. Con la implementación continua, puede probar los cambios con un subconjunto del tráfico de producción y, a continuación, promover los cambios en la distribución principal cuando esté listo.

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

Obtenga más información sobre cómo trabajar con la implementación continua en los siguientes temas.

Temas

- Flujo de trabajo de implementación continua de CloudFront
- Trabajo con una distribución provisional y una política de implementación continua
- Supervisión de una distribución provisional
- Información sobre cómo funciona la implementación continua
- Cuotas y otras consideraciones de la implementación continua

Flujo de trabajo de implementación continua de CloudFront

El siguiente flujo de trabajo de alto nivel explica cómo probar e implementar de forma segura los cambios de configuración con la implementación continua de CloudFront.

1. Elija la distribución que desea utilizar como distribución principal. La distribución principal es la que actualmente proporciona el tráfico de producción.
2. Desde la distribución principal, cree una distribución provisional. Una distribución provisional comienza como una copia de la distribución principal.
3. Cree una configuración de tráfico dentro de una política de implementación continua y asóciela a la distribución principal. Esto determina cómo CloudFront dirige el tráfico a la distribución provisional. Para obtener más información acerca de cómo dirigir las solicitudes a una distribución provisional, consulte the section called “Enrutamiento de solicitudes a la distribución provisional”.
4. Actualice la configuración de la distribución provisional. Para obtener más información acerca de la configuración que puede actualizar, consulte the section called “Actualización de las distribuciones principales y provisionales”.
5. Supervise la distribución provisional para determinar si los cambios de configuración funcionan según lo esperado. Para obtener más información acerca de la supervisión de una distribución provisional, consulte the section called “Supervisión de una distribución provisional”.

   Al supervisar la distribución provisional, podrá:

   - Volver a actualizar la configuración de la distribución provisional para seguir probando los cambios de configuración.
   - Actualizar la política de implementación continua (configuración del tráfico) para enviar más o menos tráfico a la distribución provisional.

6. Cuando esté satisfecho con el rendimiento de la distribución provisional, promueva la configuración de la distribución provisional a la distribución principal, que copia la configuración de la distribución provisional en la distribución principal. Esto también deshabilita la política de implementación continua, lo que significa que CloudFront enruta todo el tráfico a la distribución principal.

Puede crear una automatización que supervise el rendimiento de la distribución provisional (paso 5) y promueva la configuración automáticamente (paso 6) cuando se cumplan ciertos criterios.

Después de promover una configuración, puede volver a utilizar la misma distribución provisional la próxima vez que quiera probar un cambio de configuración.

Para obtener más información sobre cómo trabajar con las distribuciones provisionales y las políticas de implementación continua en la consola de CloudFront, la AWS CLI o la API de CloudFront, consulte la siguiente sección.

Trabajo con una distribución provisional y una política de implementación continua

Puede crear, actualizar y modificar las distribuciones provisionales y las políticas de implementación continua en la consola de CloudFront, con la AWS Command Line Interface (AWS CLI) o con la API de CloudFront.

Creación de una distribución provisional con una política de implementación continua

Los siguientes procedimientos muestran cómo crear una distribución provisional con una política de implementación continua.

Console

Puede crear una distribución provisional con una política de implementación continua mediante la Consola de administración de AWS.

Para crear una distribución provisional y una política de implementación continua (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.

3. Elija la distribución que desea utilizar como distribución principal. La distribución principal es la que actualmente proporciona el tráfico de producción, desde la que se creará la distribución provisional.
4. En la sección Continuous deployment (Implementación continua), elija Create staging distribution (Crear distribución provisional). Esto abre el asistente Create staging distribution (Crear distribución provisional).
5. En el asistente Create staging distribution (Crear distribución provisional), haga lo siguiente:

   a. (Opcional) Escriba una descripción de la distribución provisional.

   b. Elija Siguiente.

   c. Modifique la configuración de la distribución provisional. Para obtener más información acerca de la configuración que puede actualizar, consulte the section called “Actualización de las distribuciones principales y provisionales”.

      Cuando haya terminado de modificar la configuración de la distribución provisional, elija Next (Siguiente).

   d. Utilice la consola para especificar la Traffic configuration (Configuración del tráfico). Esto determina cómo CloudFront dirige el tráfico a la distribución provisional. (CloudFront almacena la configuración del tráfico en una política de implementación continua).

      Para obtener más información acerca de las opciones de una configuración de tráfico, consulte the section called “Enrutamiento de solicitudes a la distribución provisional”.

      Cuando haya terminado con la Traffic configuration (Configuración del tráfico), elija Next (Siguiente).

   e. Revise la configuración de la distribución provisional, incluida la configuración del tráfico, y seleccione Create staging distribution (Crear distribución provisional).

Cuando termine el asistente Create staging distribution (Crear distribución provisional) en la consola de CloudFront, CloudFront hace lo siguiente:

- Crea una distribución provisional con la configuración que especificó (en el paso 5c)
- Crea una política de implementación continua con la configuración de tráfico que especificó (en el paso 5d)
- Asocia la política de implementación continua a la distribución principal desde la que creó la distribución provisional.

Cuando la configuración de la distribución principal, con la política de implementación continua asociada, se implementa en ubicaciones periféricas, CloudFront comienza a enviar la parte especificada del tráfico a la distribución provisional en función de la configuración del tráfico.

CLI

Para crear una distribución provisional y una política de implementación continua con la AWS CLI, utilice los siguientes procedimientos.

Para crear una distribución provisional (CLI)

1. Utilice los comandos aws cloudfront get-distribution y grep juntos para obtener el valor `ETag` de la distribución que desea usar como distribución principal. La distribución principal es la que actualmente proporciona el tráfico de producción, desde la que se creará la distribución provisional.

   A continuación, se muestra un ejemplo del comando: En el siguiente ejemplo, sustituya *`primary_distribution_ID`* por el ID de la distribución principal.

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

   Copie el valor de `ETag` porque lo necesita para el siguiente paso.

2. Utilice el comando aws cloudfront copy-distribution para crear una distribución provisional. En el siguiente comando de ejemplo, se usan caracteres de escape (\) y saltos de línea para facilitar la lectura, pero debe omitirlos en el comando. En el siguiente comando de ejemplo:

   - Sustituya *`primary_distribution_ID`* por el ID de la distribución principal.
   - Sustituya *`primary_distribution_ETag`* por el valor de `ETag` de la distribución principal (que obtuvo en el paso anterior).
   - (Opcional) Sustituya *`CLI_example`* por el identificador de referencia de intermediario deseado.

   ```
   aws cloudfront copy-distribution --primary-distribution-
   id primary_distribution_ID \
                                    --if-match primary_distribution_ETag \
                                    --staging \
   ```

```
                                        --caller-reference 'CLI_example'
```

El resultado del comando muestra información sobre la distribución provisional y su configuración. Copie el nombre de dominio de CloudFront de la distribución provisional porque lo necesita para el siguiente paso.

Para crear una política de implementación continua (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo denominado `continuous-deployment-policy.yaml` que contenga todos los parámetros de entrada del comando create-continuous-deployment-policy. En el siguiente comando, se usan caracteres de escape (\) y saltos de línea para facilitar la lectura, pero debe omitirlos en el comando.

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

2. Abra el archivo llamado `continuous-deployment-policy.yaml` que acaba de crear. Edite el archivo para especificar la configuración de política de implementación continua que desee y, a continuación, guarde el archivo. Al editar el archivo:

   - En la sección `StagingDistributionDnsNames`:
     - Cambie el valor de `Quantity` a `1`.
     - Para `Items`, pegue el nombre de dominio de CloudFront de la distribución provisional (que guardó en el paso anterior).
   - En la sección `TrafficConfig`:
     - Elija un `Type` o un `SingleWeight` o `SingleHeader`.
     - Elimine la configuración para el otro tipo. Por ejemplo, si desea una configuración de tráfico basada en ponderación, defina la configuración de `Type` en `SingleWeight` y, a continuación, elimine la configuración de `SingleHeaderConfig`.
     - Para utilizar una configuración de tráfico basada en ponderación, defina el valor de `Weight` en un número decimal comprendido entre `.01` (uno por ciento) y `.15` (quince por ciento).

Para obtener más información sobre estas opciones en `TrafficConfig`, consulte the section called “Enrutamiento de solicitudes a la distribución provisional” y the section called “Persistencia de sesión para configuraciones basadas en ponderaciones”.

3. Utilice el siguiente comando para crear la política de implementación continua utilizando parámetros de entrada del archivo de `continuous-deployment-policy.yaml`.

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

Copia el valor de `Id` de la salida del comando. Este es el identificador de la política de implementación continua y lo necesitará en el paso siguiente.

Para asociar una política de implementación continua a una distribución principal (CLI con archivo de entrada)

1. Utilice el siguiente comando para guardar la configuración de la distribución principal en un archivo con el nombre `primary-distribution.yaml`. Sustituya *`primary_distribution_ID`* por el ID de la distribución principal.

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

2. Abra el archivo llamado `primary-distribution.yaml` que acaba de crear. Edite el archivo y realice los siguientes cambios:

   - Pegue el ID de la política de implementación continua (que copió del paso anterior) en el campo `ContinuousDeploymentPolicyId`.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución principal y utilizar la política de implementación continua. Sustituya *`primary_distribution_ID`* por el ID de la distribución principal.

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

Cuando la configuración de la distribución principal, con la política de implementación continua asociada, se implementa en ubicaciones periféricas, CloudFront comienza a enviar la parte especificada del tráfico a la distribución provisional en función de la configuración del tráfico.

API

Para crear una distribución provisional y una política de implementación continua con la API de CloudFront, utilice las siguientes operaciones de la API:

- CopyDistribution
- CreateContinuousDeploymentPolicy

Para obtener más información acerca de los campos que especifique en estas llamadas a la API, consulte lo siguiente:

- the section called “Enrutamiento de solicitudes a la distribución provisional”
- the section called “Persistencia de sesión para configuraciones basadas en ponderaciones”
- La documentación de referencia de la API para el SDK de AWS u otro cliente de la API

Tras crear una distribución provisional y una política de implementación continua, utilice UpdateDistribution (en la distribución principal) para asociar la política de implementación continua a la distribución principal.

Actualización de una distribución provisional

Los siguientes procedimientos muestran cómo actualizar una distribución provisional con una política de implementación continua.

Console

Puede actualizar determinadas configuraciones tanto para la distribución principal como para la provisional. Para obtener más información, consulte Actualización de las distribuciones principales y provisionales.

Para actualizar una distribución provisional (consola)

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Elija la distribución principal. Esta es la distribución principal que actualmente proporciona el tráfico de producción, desde la que ha creado la distribución provisional.
4. Elija View staging distribution (Ver distribución provisional).
5. Utilice la consola para modificar la configuración de la distribución provisional. Para obtener más información acerca de la configuración que puede actualizar, consulte the section called "Actualización de las distribuciones principales y provisionales".

En cuanto la configuración de la distribución provisional se implemente en las ubicaciones periféricas, se aplica al tráfico entrante que se dirige a la distribución provisional.

CLI

Para actualizar una distribución provisional (CLI con archivo de entrada)

1. Utilice el siguiente comando para guardar la configuración de la distribución provisional en un archivo con el nombre `staging-distribution.yaml`. Reemplace *`staging_distribution_ID`* por el ID de la distribución provisional.

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

2. Abra el archivo llamado `staging-distribution.yaml` que acaba de crear. Edite el archivo y realice los siguientes cambios:
   - Modifique la configuración de la distribución provisional. Para obtener más información acerca de la configuración que puede actualizar, consulte the section called "Actualización de las distribuciones principales y provisionales".
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.
3. Utilice el siguiente comando para actualizar la configuración de la distribución provisional. Reemplace *`staging_distribution_ID`* por el ID de la distribución provisional.

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

En cuanto la configuración de la distribución provisional se implemente en las ubicaciones periféricas, se aplica al tráfico entrante que se dirige a la distribución provisional.

API

Para actualizar la configuración de una distribución provisional, utilice UpdateDistribution (en la distribución provisional) para modificar la configuración de la distribución provisional. Para obtener más información acerca de la configuración que puede actualizar, consulte the section called "Actualización de las distribuciones principales y provisionales".

Actualización de una política de implementación continua

Los siguientes procedimientos muestran cómo actualizar una política de implementación continua.

Console

Puede actualizar la configuración de tráfico de su distribución actualizando la política de implementación continua.

Para actualizar una política de implementación continua (consola)

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Elija la distribución principal. Esta es la distribución principal que actualmente proporciona el tráfico de producción, desde la que ha creado la distribución provisional.
4. En la sección Continuous deployment (Implementación continua), elija Edit policy (Editar política).
5. Modifique la configuración del tráfico en la política de implementación continua. Cuando haya finalizado, elija Guardar cambios.

Cuando la configuración de la distribución principal, con la política de implementación continua actualizada, se implementa en ubicaciones periféricas, CloudFront comienza a enviar el tráfico a la distribución provisional en función de la configuración del tráfico.

CLI

Para actualizar una política de implementación continua (CLI con archivo de entrada)

1. Utilice el siguiente comando para guardar la configuración de la política de implementación continua en un archivo con el nombre `continuous-deployment-policy.yaml`. Sustituya *`continuous_deployment_policy_ID`* por el ID de la política de implementación continua. En el siguiente comando, se usan caracteres de escape (\) y saltos de línea para facilitar la lectura, pero debe omitirlos en el comando.

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

2. Abra el archivo llamado `continuous-deployment-policy.yaml` que acaba de crear. Edite el archivo y realice los siguientes cambios:

   - Modifique la configuración de la política de implementación continua como desee. Por ejemplo, puede pasar de utilizar una configuración de tráfico basada en encabezados a una configuración basada en ponderaciones, o puede cambiar el porcentaje de tráfico (ponderación) para una configuración basada en ponderaciones. Para obtener más información, consulte the section called “Enrutamiento de solicitudes a la distribución provisional” y the section called “Persistencia de sesión para configuraciones basadas en ponderaciones”.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la política de implementación continua. Sustituya *`continuous_deployment_policy_ID`* por el ID de la política de implementación continua. En el siguiente comando, se usan caracteres de escape (\) y saltos de línea para facilitar la lectura, pero debe omitirlos en el comando.

```
aws cloudfront update-continuous-deployment-policy --
id continuous_deployment_policy_ID \
```

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

Cuando la configuración de la distribución principal, con la política de implementación continua actualizada, se implementa en ubicaciones periféricas, CloudFront comienza a enviar el tráfico a la distribución provisional en función de la configuración del tráfico.

API

Para actualizar una política de implementación continua, utilice UpdateContinuousDeploymentPolicy.

Promoción de una configuración de distribución provisional

Los siguientes procedimientos muestran cómo promocionar una configuración de distribución provisional.

Console

Al promover una distribución provisional, CloudFront copia la configuración de la distribución provisional a la distribución principal. Esto también deshabilita la política de implementación continua y enruta todo el tráfico a la distribución principal.

Después de promover una configuración, puede volver a utilizar la misma distribución provisional la próxima vez que quiera probar un cambio de configuración.

Para promover la configuración de una distribución provisional (consola)

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Elija la distribución principal. Esta es la distribución principal que actualmente proporciona el tráfico de producción, desde la que ha creado la distribución provisional.
4. En la sección Continuous deployment (Implementación continua), elija Promote (Promover).
5. Escriba **`confirm`** y, a continuación, seleccione Promote (Promover).

CLI

Al promover una distribución provisional, CloudFront copia la configuración de la distribución provisional a la distribución principal. Esto también deshabilita la política de implementación continua y enruta todo el tráfico a la distribución principal.

Después de promover una configuración, puede volver a utilizar la misma distribución provisional la próxima vez que quiera probar un cambio de configuración.

Para promover la configuración de una distribución provisional (CLI)

- Utilice el comando aws cloudfront update-distribution-with-staging-config para promover la configuración de la distribución provisional a la distribución principal. En el siguiente comando de ejemplo, se usan caracteres de escape (\) y saltos de línea para facilitar la lectura, pero debe omitirlos en el comando. En el siguiente comando de ejemplo:
  - Sustituya *primary_distribution_ID* por el ID de la distribución principal.
  - Sustituya *staging_distribution_ID* por el ID de la distribución provisional.
  - Sustituya *primary_distribution_ETag* y *staging_distribution_ETag* por los valores de `ETag` de las distribuciones principal y provisional. Asegúrese de que el valor de la distribución principal sea el primero, como se muestra en el ejemplo.

```
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

Para promover la configuración de una distribución provisional a la distribución principal, utilice UpdateDistributionWithStagingConfig.

Supervisión de una distribución provisional

Para supervisar el rendimiento de una distribución provisional, puede utilizar las mismas métricas, registros e informes que CloudFront proporciona para todas las distribuciones. Por ejemplo:

- Puede ver las métricas de distribución predeterminadas de CloudFront (como el total de solicitudes y la tasa de errores) en la consola de CloudFront y activar métricas adicionales (como la tasa de aciertos de caché y la tasa de errores por código de estado) por un coste adicional. También puede crear alarmas en función de estas métricas.
- Puede ver los registros estándar y los registros de acceso en tiempo real para obtener información detallada sobre las solicitudes que recibe la distribución provisional. Los registros estándar contienen los dos campos siguientes que le ayudan a identificar la distribución principal a la que se envió originalmente la solicitud antes de que CloudFront la enrutara a la distribución provisional: `primary-distribution-id` y `primary-distribution-dns-name`.
- Puede ver y descargar informes en la consola de CloudFront, por ejemplo, el informe de estadísticas de caché.

Información sobre cómo funciona la implementación continua

En los siguientes temas, se explica cómo funciona la implementación continua de CloudFront.

Temas

- Enrutamiento de solicitudes a la distribución provisional
- Persistencia de sesión para configuraciones basadas en ponderaciones
- Actualización de las distribuciones principales y provisionales
- Las distribuciones principales y provisionales no comparten la caché

Enrutamiento de solicitudes a la distribución provisional

Si usa la implementación continua de CloudFront, no tiene que cambiar nada en las solicitudes de los lectores. Los lectores no pueden enviar solicitudes directamente a una distribución provisional mediante un nombre DNS, una dirección IP o un CNAME. En cambio, los lectores envían solicitudes a la distribución principal (de producción) y CloudFront redirige algunas de esas solicitudes a la distribución provisional en función de los ajustes de configuración del tráfico de la política de implementación continua. Existen dos tipos de configuraciones del tráfico:

Basada en ponderaciones

Una configuración basada en ponderaciones dirige el porcentaje especificado de solicitudes de los lectores a la distribución provisional. Al utilizar una configuración basada en ponderaciones, también puede habilitar la persistencia de sesión, que ayuda a garantizar que CloudFront trate las solicitudes del mismo lector como parte de una sola sesión. Para obtener más información, consulte the section called “Persistencia de sesión para configuraciones basadas en ponderaciones”.

Basada en encabezados

Una configuración basada en encabezados dirige las solicitudes a la distribución provisional cuando la solicitud del lector contiene un encabezado HTTP específico (usted especifica el encabezado y el valor). Las solicitudes que no contienen el encabezado y el valor especificados se envían a la distribución principal. Esta configuración es útil para realizar pruebas locales o cuando tiene control sobre las solicitudes del lector.

> **Note**
>
> Los encabezados que se envíen a la distribución provisional deben contener el prefijo `aws-cf-cd-`.

Persistencia de sesión para configuraciones basadas en ponderaciones

Al utilizar una configuración basada en ponderaciones para dirigir el tráfico a una distribución provisional, también puede habilitar la persistencia de sesión, lo que ayuda a garantizar que CloudFront trate las solicitudes del mismo lector como una sola sesión. Al habilitar la persistencia de sesión, CloudFront establece una cookie para que todas las solicitudes del mismo lector de una sola sesión las proporciona una sola distribución, ya sea la principal o la provisional.

Al habilitar la persistencia de sesión, también puede especificar la duración de inactividad. Si el lector está inactivo (no envía solicitudes) durante este período de tiempo, la sesión caduca y CloudFront trata las solicitudes futuras de este lector como una sesión nueva. La duración de inactividad se especifica como un número de segundos, de 300 (cinco minutos) a 3600 (una hora).

En los siguientes casos, CloudFront restablece todas las sesiones (incluso las activas) y considera que todas las solicitudes son una sesión nueva:

- Cuando deshabilita o habilita la política de implementación continua

- Cuando deshabilita o habilita la configuración de persistencia de sesión

Actualización de las distribuciones principales y provisionales

Cuando una distribución principal tiene una política de implementación continua asociada, están disponibles los siguientes cambios de configuración tanto para la distribución principal como para la provisional:

- Toda la configuración del comportamiento de caché, incluido el comportamiento predeterminado de caché
- Toda la configuración de origen (orígenes y grupos de origen)
- Respuestas de error personalizadas (páginas de error)
- Restricciones geográficas
- Objeto raíz predeterminado
- Configuración de registros
- Descripción (comentario)

También puede actualizar los recursos externos a los que se hace referencia en la configuración de una distribución, como una política de caché, una política de encabezados de respuesta, una CloudFront Function o una función Lambda@Edge.

Las distribuciones principales y provisionales no comparten la caché

Las distribuciones principales y provisionales no comparten la caché. Cuando CloudFront envía la primera solicitud a una distribución provisional, su caché está vacía. A medida que las solicitudes llegan a la distribución provisional, comienza a almacenar en caché las respuestas (si está configurada para hacerlo).

Cuotas y otras consideraciones de la implementación continua

La implementación continua de CloudFront está supeditada a las siguientes cuotas y otras consideraciones.

Cuotas

- Cantidad máxima de distribuciones provisionales por Cuenta de AWS: 20

- Cantidad máxima de políticas de implementación continua por Cuenta de AWS: 20
- Porcentaje máximo de tráfico que puede enviar a una distribución provisional en una configuración basada ponderaciones: 15 %
- Valores mínimo y máximo de persistencia de sesión y duración de inactividad: 300-3600 segundos

Para obtener más información, consulte Cuotas.

> **Note**
>
> Si utiliza la implementación continua y la distribución principal está configurada con OAC para el acceso al bucket de S3, actualice la política de bucket de S3 para permitir el acceso a la distribución provisional. Por ejemplo, políticas de bucket de S3, consulte the section called "Concesión de permiso de CloudFront para acceder al bucket de S3".

AWS WAFACL web de

Si habilita la implementación continua para su distribución, se deben tener en cuenta las siguientes consideraciones para AWS WAF:

- No puede asociar una lista de control de acceso (ACL) web de AWS WAF a la distribución si es la primera vez que se asocia a la distribución.
- No puede desasociar una ACL web de AWS WAF de la distribución.

Antes de poder realizar las tareas anteriores, debe eliminar la política de implementación continua de su distribución de producción. Esto también elimina la distribución provisional. Para obtener más información, consulte Uso de protecciones de AWS WAF.

Casos en los que CloudFront envía todas las solicitudes a la distribución principal

En ciertos casos, como los períodos de alta utilización de recursos, CloudFront puede enviar todas las solicitudes a la distribución principal independientemente de lo que se especifique en la política de implementación continua.

CloudFront envía todas las solicitudes a la distribución principal durante las horas de mayor tráfico, independientemente de lo que se especifique en la política de implementación continua. El pico de tráfico hace referencia al tráfico del servicio CloudFront y no al tráfico de la distribución.

HTTP/3

No puede utilizar la implementación continua con una distribución que admita HTTP/3.

Uso de URL personalizadas añadiendo nombres de dominio alternativos (CNAME)

Al crear una distribución, CloudFront le proporciona un nombre de dominio, como d111111abcdef8.cloudfront.net. En lugar de utilizar este nombre de dominio proporcionado, puede utilizar un nombre de dominio alternativo (también conocido como CNAME).

Para usar su propio nombre de dominio, como www.example.com, consulte los siguientes temas:

Temas

- Requisitos para el uso de nombres de dominio alternativos
- Restricciones de uso de nombres de dominio alternativos
- Adición de un nombre de dominio alternativo
- Desplazamiento de un nombre de dominio alternativo
- Eliminación de un nombre de dominio alternativo
- Uso de comodines en nombres de dominio alternativos

Requisitos para el uso de nombres de dominio alternativos

Cuando agrega un nombre de dominio alternativo, como www.example.com, a una distribución de CloudFront, los requisitos son los siguientes:

Los nombres de dominio alternativos deben estar en minúsculas

Todos los nombres de dominio alternativos (CNAME) deben estar en minúsculas.

Se debe haber emitido un certificado TLS válido para los nombres de dominio alternativo

Para agregar un nombre de dominio alternativo (CNAME) a una distribución de CloudFront, debe asociar a la distribución un certificado TLS válido de confianza que haya sido emitido para el nombre de dominio alternativo. De este modo, se garantiza que solo las personas con acceso al certificado del dominio pueden asociar a CloudFront un CNAME relacionado con el dominio.

Un certificado de confianza es el que emite AWS Certificate Manager (ACM) u otra entidad de certificación (CA) válida. Puede utilizar un certificado autofirmado para validar un CNAME existente, pero no para un CNAME nuevo. CloudFront admite las mismas entidades de certificación que Mozilla. Para consultar la lista actualizada, visite Mozilla Included CA Certificate List. Para obtener más información sobre los certificados intermedios cuando utiliza una CA de terceros, consulte Certificados intermedios.

Para verificar un nombre de dominio alternativo mediante el certificado que se asocia, incluidos los nombres de dominio alternativos que incluyen comodines, CloudFront comprueba el nombre alternativo de asunto (SAN) en el certificado. El nombre de dominio alternativo que va a añadir debe estar incluido en el SAN.

> **Note**
>
> Solo puede haber un certificado asociado a una distribución de CloudFront en cada momento.

Para demostrar que tiene autorización para añadir un nombre de dominio alternativo a la distribución, realice una de las operaciones siguientes:

- Adjuntar un certificado que incluya el nombre de dominio alternativo, tal como nombre-producto.ejemplo.com.
- Asociar un certificado con un carácter comodín * al principio de un nombre de dominio, para que incluya varios subdominios en un certificado. Si especifica un carácter comodín, puede agregar varios subdominios como nombres de dominio alternativos a CloudFront.

Los siguientes ejemplos ilustran cómo el uso de caracteres comodín en los nombres de dominio de un certificado sirven para permitirle que agregue otros nombres de dominio alternativos específicos a CloudFront.

- Desea añadir marketing.ejemplo.com como nombre de dominio alternativo. El certificado incluye el siguiente nombre de dominio: *ejemplo.com. Cuando adjunta este certificado a CloudFront, puede añadir cualquier nombre de dominio alternativo a la distribución que sustituya el carácter comodín en ese nivel, incluyendo marketing.ejemplo.com. También puede, por ejemplo, añadir los siguientes nombres de dominio alternativos:
  - producto.ejemplo.com
  - api.example.com

Sin embargo, no se puede añadir otros nombres de dominio que estén en niveles superiores o inferiores al carácter comodín. Por ejemplo, no puede añadir los nombres de dominio alternativos ejemplo.com ni marketing.producto.ejemplo.com.

- Desea añadir ejemplo.com como nombre de dominio alternativo. Para ello, debe incluir el nombre de dominio ejemplo.com en el certificado adjuntado a su distribución.
- Desea añadir marketing.producto.ejemplo.com como nombre de dominio alternativo. Para ello, puede incluir *.producto.ejemplo.com en el certificado, o puede incluir marketing.producto.ejemplo.com en el certificado.

Permiso para cambiar la configuración de DNS

Cuando añade nombres de dominio alternativos, debe crear registros CNAME para enrutar las consultas de DNS de los nombres de dominio alternativos a su distribución de CloudFront. Para ello, debe tener permiso para crear registros CNAME en el proveedor de servicios de DNS para los nombres de dominio alternativos que está utilizando. Por lo general, esto indicará que es el propietario de los dominios, aunque también puede estar desarrollando una aplicación para el propietario del dominio.

Nombres de dominio alternativos y HTTPS

Si desea que los espectadores utilicen HTTPS con un nombre de dominio alternativo, debe configurar ajustes adicionales. Para obtener más información, consulte Uso de nombres de dominio alternativos y HTTPS.

Restricciones de uso de nombres de dominio alternativos

Tome en cuenta las siguientes restricciones de uso de nombres de dominio alternativos:

Cantidad máxima de nombres de dominio alternativos

Para obtener el número máximo actual de nombres de dominio alternativos que puede agregar a una distribución o solicitar una cuota (antes denominada límite) más alta, consulte Cuotas generales de distribuciones.

Nombres de dominio alternativos superpuestos y duplicados

No puede agregar un nombre de dominio alternativo a una distribución de CloudFront si ese mismo nombre de dominio alternativo ya existe en otra distribución de CloudFront, incluso si la Cuenta de AWS es la propietaria de la otra distribución.

Sin embargo, puede añadir un nombre de dominio alternativo comodín como, por ejemplo *.ejemplo.com, que incluya (que se superponga) un nombre de dominio alternativo no comodín, como por ejemplo www.ejemplo.com. Si tiene nombres de dominio alternativos superpuestos en dos distribuciones, CloudFront envía la solicitud a la distribución que tiene la coincidencia de nombre más específica, independientemente de la distribución a la que apunta el registro DNS. Por ejemplo, marketing.dominio.com es más específico que *.dominio.com.

Si ya tiene una entrada DNS comodín que apunta a una distribución de CloudFront y recibe un error de DNS configurado incorrectamente al intentar agregar un nuevo CNAME con un nombre más específico, consulte CloudFront devuelve un error de registro DNS mal configurado al intentar agregar un nuevo CNAME.

Domain Fronting

CloudFront tiene protección contra el domain fronting que se produce en diferentes Cuenta de AWS. Esto se produce cuando un cliente no estándar crea una conexión TLS/SSL con un nombre de dominio de una Cuenta de AWS y, a continuación, realiza una solicitud HTTPS para un nombre de dominio no relacionado de otra Cuenta de AWS.

Por ejemplo, la conexión TLS puede conectarse a www.example.com y, a continuación, emitir una solicitud a www.example.org.

Para determinar si una solicitud es domain fronting, CloudFront realiza las siguientes comprobaciones:

- La extensión SNI es igual al encabezado del `Host` de la solicitud HTTP
- El certificado pertenece a la misma Cuenta de AWS que la distribución de la solicitud
- El `Host` de la solicitud HTTP está cubierto por el certificado que se entrega durante el establecimiento de comunicación TLS

Si no se cumple ninguna de estas condiciones, CloudFront determina que la solicitud es domain fronting. CloudFront rechazará la solicitud con una respuesta de error HTTP 421.

> **Note**
>
> Si el cliente no proporciona la extensión SNI y, en su lugar, obtiene un certificado *.cloudfront.net predeterminado, CloudFront aceptará las solicitudes entrantes.

Cómo identifica CloudFront la distribución de una solicitud

CloudFront identifica la distribución de una solicitud HTTP en función del encabezado del `Host`. CloudFront no depende de la dirección IP de CloudFront a la que se conecte ni del establecimiento de comunicación de SNI que se haya proporcionado durante el establecimiento de comunicación de TLS.

Cuando CloudFront recibe una solicitud, utilizará el valor del encabezado del `Host` para hacer coincidir la solicitud con la distribución específica.

Por ejemplo, supongamos que tiene dos distribuciones y que ha actualizado la configuración de DNS para que los nombres de dominio alternativos se dirijan a los siguientes puntos de conexión:

- primary.example.com apunta a d111111primary.cloudfront.net
- secondary.example.com apunta a d222222secondary.cloudfront.net

Si realiza una solicitud a https://primary.example.com pero especifica el encabezado del `Host` como secondary.example.com, por ejemplo `curl https://primary.example.com -H "Host: secondary.example.com"`, la solicitud se dirigirá a la distribución secundaria en su lugar.

Agregar un nombre de dominio alternativo en el nodo principal (ápex de zona) para un dominio

Al agregar un nombre de dominio alternativo a una distribución, normalmente debe crear un registro CNAME en su configuración de DNS para dirigir las consultas de DNS del nombre de dominio a su distribución de CloudFront. Sin embargo, no puede crear un registro CNAME para el nodo superior de un espacio de nombres de DNS, también conocido como ápex de zona; el protocolo de DNS no lo permite. Por ejemplo, si registra el nombre DNS ejemplo.zom, el ápex de zona será ejemplo.com. No puede crear un registro CNAME para ejemplo.com, pero puede crear registros CNAME para www.ejemplo.com, productonuevo.ejemplo.com, etc.

Si utiliza Route 53 como servicio de DNS, puede crear un conjunto de registros de recursos de alias, que tiene dos ventajas con respecto a los registros CNAME:

- Puede crear un conjunto de registros de recursos de alias para un nombre de dominio en el nodo principal (example.com).
- Puede crear un registro HTTPS para un nombre de dominio alternativo a fin de permitir la negociación del protocolo como parte de la búsqueda DNS si el cliente lo admite. Para obtener más información, consulte Create alias resource record set.

- No paga por las consultas de Route 53 cuando utiliza un conjunto de registros de recursos de alias.

> **Note**
>
> Si habilita IPv6, debe crear dos conjuntos de registros de recursos de alias: uno para dirigir el tráfico IPv4 (un registro A) y otro para dirigir el tráfico IPv6 (un registro AAAA). Para obtener más información, consulte Habilitación de IPv6 (solicitudes de espectadores) en el tema Referencia de toda la configuración de distribución.

Para obtener más información, consulte Direccionamiento del tráfico a una distribución web de Amazon CloudFront mediante el nombre de dominio en la Guía para desarrolladores de Amazon Route 53.

Si no utiliza Route 53 para el DNS, puede solicitar direcciones IP estáticas de anycast para enrutar dominios apex como example.com a CloudFront. Para obtener más información, consulte Solicitud de direcciones IP estáticas de anycast para utilizarlas en las listas de permitidos.

Adición de un nombre de dominio alternativo

En la siguiente lista de tareas, se describe cómo utilizar la consola de CloudFront para agregar un nombre de dominio alternativo a la distribución, de modo que pueda utilizar su propio nombre de dominio en lugar del nombre de dominio de CloudFront. Para obtener información acerca de cómo actualizar su distribución con la API de CloudFront, consulte Configuración de distribuciones.

> **Note**
>
> Si desea que los espectadores usen HTTPS con su nombre de dominio alternativo, consulte Uso de nombres de dominio alternativos y HTTPS.

Antes de comenzar: asegúrese de hacer lo siguiente antes de actualizar la distribución para añadir un nombre de dominio alternativo:

- Registre el nombre de dominio en Route 53 o en otro registrador de dominios.
- Obtenga un certificado TLS de una entidad de certificación (CA) autorizada que cubra el nombre de dominio. Añada el certificado a su distribución para validar que usted está autorizado a usar el

dominio. Para obtener más información, consulte Requisitos para el uso de nombres de dominio alternativos.

Adición de un nombre de dominio alternativo

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la ID de la distribución que desea actualizar.
3. En la pestaña General, elija Agregar un dominio.
4. Introduzca hasta cinco dominios para servir.
5. Elija Siguiente.
6. En Certificado TLS, si CloudFront no puede encontrar un certificado de AWS Certificate Manager (ACM) existente para el dominio en la Cuenta de AWS en la Región de AWS `us-east-1`, puede elegir crear un certificado automáticamente o crearlo de forma manual en ACM.
7. Cuando se aprovisione el certificado, debe actualizar los registros de DNS con el proveedor de DNS para demostrar la propiedad del dominio. Las entradas que debe realizar en los registros DNS se proporcionan para usted en la consola de CloudFront.
8. Después de actualizar los registros DNS, elija Validar certificado.
9. Cuando el certificado esté validado, elija Siguiente.
10. Revise los cambios y elija Agregar dominios.
11. En la pestaña General de la distribución, confirme que Distribution Status (Estado de la distribución) ha cambiado a Deployed (Implementada). Si intenta utilizar un nombre de dominio alternativo antes de que las actualizaciones de la distribución se hayan implementado, los enlaces que cree en los pasos siguientes probablemente no funcionen.
12. Configure el servicio de DNS para que el nombre del dominio alternativo (tal como www.ejemplo.com) dirija el tráfico al nombre de dominio de CloudFront de su distribución (tal como d111111abcdef8.cloudfront.net). El método que utilice dependerá de si está utilizando Route 53 como proveedor de servicios de DNS para el dominio u otro proveedor. Para obtener más información, consulte Adición de un dominio a la distribución estándar de CloudFront.

    Route 53

    Cree un conjunto de registros de recursos de alias. Si cuenta con uno, no tendrá que pagar por las consultas de Route 53. También puede crear un conjunto de registros de recursos de alias del nombre de dominio raíz (example.com) cuyo DNS no permita CNAME. Para obtener

instrucciones sobre cómo crear un conjunto de registros de recursos de alias, consulte Enrutamiento del tráfico a una distribución web de Amazon CloudFront mediante el nombre de dominio en la Guía para desarrolladores de Amazon Route 53.

Si lo desea, puede crear un registro HTTPS para un nombre de dominio alternativo a fin de permitir la negociación del protocolo como parte de la búsqueda de DNS si el cliente lo admite.

Creación de un conjunto de registros de recursos de alias con un registro HTTPS (opcional)

1. Habilite HTTP/2 o HTTP/3 en la configuración de distribución de CloudFront. Para obtener más información, consulte Versiones de HTTP compatibles y Actualizar una distribución.
2. En la consola de Route 53, cree un conjunto de registros de recursos de alias. Siga el procedimiento Enrutamiento del tráfico a una distribución web de Amazon CloudFront mediante su nombre de dominio.
3. Mientras crea el conjunto de registros de recursos de alias, cree un registro de alias con el tipo de registro HTTPS.

Otro proveedor de servicios de DNS

Utilice el método proporcionado por el proveedor de servicios DNS para añadir un registro CNAME a su dominio. Este nuevo registro de CNAME redirigirá las consultas de DNS de su dominio alternativo (por ejemplo, www.ejemplo.com) al nombre de dominio de CloudFront de su distribución (por ejemplo, d111111abcdef8.cloudfront.net). Para obtener más información, consulte la documentación de su proveedor de servicios de DNS.

> **Important**
>
> Si ya tiene un registro de CNAME para su nombre de dominio alternativo, actualice dicho registro o sustitúyalo por uno nuevo que apunte al nombre de dominio de CloudFront para su distribución.

13. Con `dig` o una herramienta similar, confirme que la configuración DNS que ha creado en el paso anterior apunta al nombre de dominio de su distribución.

    El siguiente ejemplo muestra una solicitud de `dig` en un dominio llamado www.example.com y la parte pertinente de la respuesta.

```
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 sección de respuestas muestra un registro CNAME que enruta las consultas para www.example.com al nombre de dominio de distribución de CloudFront d111111abcdef8.cloudfront.net. Si el nombre a la derecha de `CNAME` es el nombre de dominio de su distribución de CloudFront, el registro de CNAME está configurado correctamente. Si es cualquier otro valor, por ejemplo, el nombre de dominio de su bucket de Amazon S3, el registro de CNAME se configura de forma incorrecta. En ese caso, vuelva al paso 7 y corrija el registro de CNAME para que apunte al nombre de dominio de su distribución.

14. Pruebe el nombre de dominio alternativo visitando las URL con su nombre de dominio en lugar del nombre del dominio de CloudFront para su distribución.
15. En su aplicación, cambie las URL de sus objetos para utilizar su nombre de dominio alternativo en lugar del nombre de dominio de su distribución de CloudFront.

Desplazamiento de un nombre de dominio alternativo

Si intenta agregar un nombre de dominio alternativo a una distribución estándar o a un inquilino de distribución, y el nombre de dominio alternativo ya está asociado a un recurso diferente, aparecerá un mensaje de error.

Por ejemplo, aparecerá el mensaje de error `CNAMEAlreadyExists` (One or more of the CNAMEs you provided are already associated with a different resource) cuando intente agregar www.example.com a una distribución estándar o a un inquilino de distribución, pero ese nombre de dominio alternativo ya está asociado a un recurso diferente.

En ese caso, es posible que desee mover el nombre de dominio alternativo existente de un recurso a otro. Esta es la distribución de origen y la distribución de destino. Puede mover nombres de dominio alternativos entre distribuciones estándar o inquilinos de distribución.

Para mover el nombre de dominio alternativo, consulte los siguientes temas:

Temas

- Configuración de la distribución estándar o el inquilino de distribución de destino
- Búsqueda de la distribución estándar o el inquilino de distribución de origen
- Mueva el nombre de dominio alternativo

Configuración de la distribución estándar o el inquilino de distribución de destino

Para poder mover un nombre de dominio alternativo, debe configurar el recurso de destino. Se trata de la distribución estándar o el inquilino de distribución de destino al que va a mover el nombre de dominio alternativo.

Standard distribution

Configuración de una distribución estándar de destino

1. Solicite un certificado TLS. Este certificado incluye el nombre de dominio alternativo como sujeto o dominio alternativo del sujeto (SAN) o un carácter comodín (*) que cubre el nombre de dominio alternativo que va a mover. Si no dispone de uno, puede solicitar uno a AWS Certificate Manager (ACM) u obtenerlo de otra entidad de certificación (CA, por sus siglas en inglés) e importarlo a ACM.

   > **Note**
   >
   > Debe solicitar o importar el certificado en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`).

   Para obtener más información, consulte Solicitud de un certificado público mediante la consola e Importación de un certificado en AWS Certificate Manager en la Guía del usuario de AWS Certificate Manager.

2. Si aún no ha creado la distribución estándar de destino, créela ahora. Como parte de la creación de la distribución estándar, asocie el certificado con esta distribución estándar. Para obtener más información, consulte Creación de una distribución.

   Si ya tiene una distribución estándar de destino, asocie el certificado con la distribución estándar. Para obtener más información, consulte Actualizar una distribución.

3. Si va a mover nombres de dominio alternativos en la misma Cuenta de AWS, omita este paso.

   Para mover un nombre de dominio alternativo de una Cuenta de AWS a otra, debe crear un registro TXT en la configuración de DNS. Este paso de verificación ayuda a evitar transferencias de dominio no autorizadas. CloudFront utiliza este registro TXT para validar que usted es el propietario del nombre de dominio alternativo.

   En la configuración de DNS, cree un registro TXT de DNS que asocie el nombre de dominio alternativo con la distribución estándar de destino. El formato del registro TXT puede variar en función del tipo de dominio.

   - En el caso de los subdominios, especifique un guion bajo (_) delante del nombre de dominio alternativo. A continuación, se muestra un ejemplo de registro TXT.

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

   - En el caso de un vértice (o dominio raíz), especifique un guion bajo y un punto (`_.`) delante del nombre de dominio. A continuación, se muestra un ejemplo de registro TXT.

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

Distribution tenant

Configuración del inquilino de distribución de destino

1. Solicite un certificado TLS. Este certificado incluye el nombre de dominio alternativo como sujeto o dominio alternativo del sujeto (SAN) o un carácter comodín (*) que cubre el nombre de dominio alternativo que va a mover. Si no dispone de uno, puede solicitar uno a AWS Certificate Manager (ACM) u obtenerlo de otra entidad de certificación (CA, por sus siglas en inglés) e importarlo a ACM.

> **Note**
>
> Debe solicitar o importar el certificado en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`).

Para obtener más información, consulte Solicitud de un certificado público mediante la consola e Importación de un certificado en AWS Certificate Manager en la Guía del usuario de AWS Certificate Manager.

2. Si no ha creado el inquilino de distribución de destino, créelo ahora. Como parte de la creación del inquilino de distribución, asocie el certificado con el inquilino de distribución. Para obtener más información, consulte Creación de una distribución.

   Si ya tiene un inquilino de distribución de destino, asocie el certificado con el inquilino de distribución. Para obtener más información, consulte Agregación de un dominio y un certificado (inquilino de distribución).

3. Si va a mover nombres de dominio alternativos en la misma Cuenta de AWS, omita este paso.

   Para mover un nombre de dominio alternativo de una Cuenta de AWS a otra, debe crear un registro TXT en la configuración de DNS. Este paso de verificación ayuda a evitar transferencias de dominio no autorizadas y CloudFront utiliza este registro TXT para validar la propiedad del nombre de dominio alternativo.

   En la configuración de DNS, cree un registro TXT de DNS que asocie el nombre de dominio alternativo con el inquilino de distribución de destino. El formato del registro TXT puede variar en función del tipo de dominio.

   - En el caso de los subdominios, especifique un guion bajo (_) delante del nombre de dominio alternativo. A continuación, se muestra un ejemplo de registro TXT.

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

   - En el caso de un vértice (o dominio raíz), especifique un guion bajo y un punto (`_.`) delante del nombre de dominio. A continuación, se muestra un ejemplo de registro TXT.

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

A continuación, consulte el tema siguiente para encontrar la distribución estándar o el inquilino de distribución de origen que ya está asociado con el nombre de dominio alternativo.

Búsqueda de la distribución estándar o el inquilino de distribución de origen

Para poder mover un nombre de dominio alternativo de una distribución (estándar o inquilino) a otra, busque la distribución de origen. Este es el recurso al que ya está asociado el nombre de dominio alternativo. Cuando conozca el ID de Cuenta de AWS de los recursos de distribución de origen y destino, podrá determinar cómo mover el nombre de dominio alternativo.

> **Notas**
>
> - Le recomendamos que utilice la operación de la API ListDomainConflicts, ya que admite tanto distribuciones estándar como inquilinos de distribución.
> - La operación de la API ListConflictingAliases solo admite distribuciones estándar.

Siga estos ejemplos para buscar la distribución de origen (estándar o inquilino).

list-domain-conflicts

> **Tip**
>
> - Para una distribución estándar, debe tener los permisos `cloudfront:GetDistribution` y `cloudfront:ListDomainConflicts`.
> - Para un inquilino de distribución, debe tener los permisos `cloudfront:GetDistributionTenant` y `cloudfront:ListDomainConflicts`.

Uso de **`list-domain-conflicts`** para buscar la distribución estándar o el inquilino de distribución de origen

1. Utilice el comando `list-domain-conflicts`, tal y como se muestra en el ejemplo siguiente.

   a. Reemplace *`www.example.com`* por el nombre de dominio.

   b. Para `domain-control-validation-resource`, especifique el ID de la distribución estándar o del inquilino de distribución de origen que ha configurado anteriormente.

Debe tener una distribución estándar o un inquilino de distribución que esté asociado a un certificado que cubra el dominio especificado.

c. Ejecute este comando mediante las credenciales que están en la misma Cuenta de AWS que las de la distribución estándar o el inquilino de distribución de origen.

Solicitud

En este ejemplo se especifica un inquilino de distribución.

```
aws cloudfront list-domain-conflicts \
--domain www.example.com \
--domain-control-validation-resource
 "DistributionTenantId=dt_2x9GhoK0TZRsohWzv1b9It8JABC"
```

Respuesta

Para cada nombre de dominio en la salida del comando, puede ver lo siguiente:

- El tipo de recurso con el que está asociado el dominio
- El ID del recurso
- El ID de la Cuenta de AWS que posee el recurso

El ID del recurso y el ID de la cuenta están parcialmente ocultos. Esto le permite identificar la distribución estándar o el inquilino de distribución que pertenece a la cuenta y ayuda a proteger la información de los que no posee.

```
{
    "DomainConflicts": [
        {
            "Domain": "www.example.com",
            "ResourceType": "distribution-tenant",
            "ResourceId": "***************ohWzv1b9It8JABC",
            "AccountId": "******112233"
        }
    ]
}
```

La respuesta enumera todos los nombres de dominio que entran en conflicto o se superponen con el que ha especificado.

Ejemplo

- Si especifica `tenant1.example.com`, la respuesta incluye tenant1.example.com y el nombre de dominio alternativo comodín superpuesto (*.example.com si existe).
- Si especifica `*.tenant1.example.com`, la respuesta incluye *.tenant1.example.com y cualquier nombre de dominio alternativo cubierto por ese comodín (por ejemplo, test.tenant1.example.com, dev.tenant1.example.com, etc.).

2. En la respuesta, busque la distribución estándar o el inquilino de distribución de origen correspondiente al nombre de dominio alternativo que va a mover y anote el ID de Cuenta de AWS.
3. Compare el ID de cuenta de la distribución estándar o del inquilino de distribución de origen con el ID de cuenta donde creó la distribución estándar o el inquilino de distribución de destino en el paso anterior. A continuación, puede determinar si el origen y el destino están en la misma Cuenta de AWS. Esto le ayuda a determinar cómo mover el nombre de dominio alternativo.

   Para obtener más información, consulte el comando list-domain-conflicts en la Referencia de la AWS Command Line Interface.

list-conflicting-aliases (standard distributions only)

> **Tip**
>
> Debe tener los permisos `cloudfront:GetDistribution` y `cloudfront:ListConflictingAliases` en la distribución estándar de destino.

Uso de **`list-conflicting-aliases`** para buscar la distribución estándar de origen

1. Utilice el comando `list-conflicting-aliases`, tal y como se muestra en el ejemplo siguiente.

a. Reemplace *www.example.com* por el nombre de dominio alternativo y *EDFDVBD6EXAMPLE* por el ID de la distribución estándar de destino que ha configurado anteriormente.

b. Ejecute este comando con credenciales que están en la misma Cuenta de AWS que la distribución estándar de destino.

Solicitud

En este ejemplo se especifica una distribución estándar.

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

Respuesta

Para cada nombre de dominio alternativo en la salida del comando, puede ver el ID de la distribución estándar con la que está asociado y el ID de la Cuenta de AWS que posee la distribución estándar. Los ID de la distribución estándar y de la cuenta están parcialmente ocultos, lo que le permite identificar las distribuciones estándar y las cuentas que posee, y ayuda a proteger la información de las que no posee.

```
{
    "ConflictingAliasesList": {
        "MaxItems": 100,
        "Quantity": 1,
        "Items": [
            {
                "Alias": "www.example.com",
                "DistributionId": "*******EXAMPLE",
                "AccountId": "******112233"
            }
        ]
    }
}
```

La respuesta enumera los nombres de dominio alternativos que están en conflicto o se superponen con el que ha especificado.

Ejemplo

- Si especifica `www.example.com`, la respuesta incluye www.example.com y el nombre de dominio alternativo comodín superpuesto (*.example.com), si existe.
- Si especifica `*.example.com`, la respuesta incluye *.example.com y cualquier nombre de dominio alternativo cubierto por ese comodín (por ejemplo, www.example.com, test.example.com, dev.example.com, etc.).

2. Busque la distribución estándar para el nombre de dominio alternativo que está moviendo y anote el ID de Cuenta de AWS. Compare este ID de cuenta con el ID de cuenta donde ha creado la distribución estándar de destino en el paso anterior. A continuación, puede determinar si estas dos distribuciones estándar están en la misma Cuenta de AWS y cómo mover el nombre de dominio alternativo.

   Para obtener más información, consulte el comando list-conflicting-aliases en la Referencia de la AWS Command Line Interface.

A continuación, consulte el tema siguiente para mover el nombre de dominio alternativo.

Mueva el nombre de dominio alternativo

Dependiendo de su situación, elija una de las siguientes maneras de mover el nombre de dominio alternativo:

Las distribuciones de origen y destino (estándar o inquilino) están en la misma Cuenta de AWS

Utilice el comando update-domain-association en la AWS Command Line Interface (AWS CLI) para mover el nombre de dominio alternativo.

Este comando funciona para todos los movimientos en la misma cuenta, incluso cuando el nombre de dominio alternativo es un dominio de vértice (también denominado dominio raíz, como ejemplo.com).

Las distribuciones de origen y destino (estándar o inquilino) están en diferentes Cuentas de AWS

Si tiene acceso a la distribución estándar o al inquilino de distribución de origen, el nombre de dominio alternativo no es un dominio de vértice y aún no está utilizando un carácter comodín que se superponga con ese nombre de dominio alternativo, utilice un carácter comodín para mover el

nombre de dominio alternativo. Para obtener más información, consulte the section called “Utilice un comodín para mover un nombre de dominio alternativo”.

Si no tiene acceso a la Cuenta de AWS que la distribución estándar o el inquilino de distribución de origen, puede intentar utilizar el comando update-domain-association para mover el nombre de dominio alternativo. La distribución estándar o el inquilino de distribución de origen deben estar deshabilitados para poder mover el nombre de dominio alternativo. Para obtener ayuda adicional, consulte the section called “Contacte a AWS Support para mover un nombre de dominio alternativo”.

> **Note**
>
> Puede utilizar el comando associate-alias, pero este comando solo admite distribuciones estándar. Consulte AssociateAlias en la Referencia de la API de Amazon CloudFront.

update-domain-association (standard distributions and distribution tenants)

Uso de **`update-domain-association`** para mover un nombre de dominio alternativo

1. Utilice el comando `update-domain-association`, tal y como se muestra en el ejemplo siguiente.

   a. Reemplace *`example.com`* por el nombre de dominio alternativo y especifique el ID de la distribución estándar o del inquilino de distribución de destino.

   b. Ejecute este comando con credenciales que estén en la misma Cuenta de AWS que la distribución estándar o el inquilino de distribución de destino.

> **Tenga en cuenta las siguientes restricciones**
>
> - Además del permiso `cloudfront:UpdateDomainAssociation`, debe tener el permiso `cloudfront:UpdateDistribution` para actualizar una distribución estándar. Para actualizar un inquilino de distribución, debe tener el permiso `cloudfront:UpdateDistributionTenant`.
> - Si las distribuciones de origen y destino (estándar o inquilino) se encuentran en diferentes Cuentas de AWS, debe deshabilitar el origen para poder mover el dominio.

- La distribución de destino debe configurarse tal y como se describe en the section called “Configuración de la distribución estándar o el inquilino de distribución de destino”.

Solicitud

```
aws cloudfront update-domain-association \
  --domain "www.example.com" \
  --target-resource DistributionTenantId=dt_9Fd3xTZq7Hl2KABC \
  --if-match E3UN6WX5ABC123
```

Respuesta

```
{
    "ETag": "E7Xp1Y3N9DABC",
    "Domain": "www.example.com",
    "ResourceId": "dt_9Fd3xTZq7Hl2KABC"
}
```

Este comando elimina el nombre de dominio alternativo de la distribución estándar o del inquilino de distribución de origen y lo agrega a la distribución estándar o al inquilino de distribución de destino.

2. Una vez que la distribución de destino se haya implementado por completo, actualice la configuración de DNS para que el nombre de dominio apunte al punto de conexión de enrutamiento de CloudFront. Por ejemplo, el registro DNS apuntaría el nombre de dominio alternativo (`www.example.com`) al nombre de dominio proporcionado por CloudFront d111111abcdef8.cloudfront.net. Si el destino es un inquilino de distribución, especifique el punto de conexión del grupo de conexión. Para obtener más información, consulte Dirección de dominios a CloudFront.

associate-alias (standard distributions only)

Uso de **`associate-alias`** para mover un nombre de dominio alternativo

1. Utilice el comando `associate-alias`, tal y como se muestra en el ejemplo siguiente.

a. Reemplace *www.example.com* por el nombre de dominio alternativo y *EDFDVBD6EXAMPLE* por el ID de distribución estándar de destino.

b. Ejecute este comando con credenciales que están en la misma Cuenta de AWS que la distribución estándar de destino.

> Tenga en cuenta las siguientes restricciones
>
> - Debe tener los permisos `cloudfront:AssociateAlias` y `cloudfront:UpdateDistribution` en la distribución estándar de destino.
> - Si la distribución estándar de origen y la de destino están en la misma Cuenta de AWS, debe tener el permiso `cloudfront:UpdateDistribution` en la distribución estándar de origen.
> - Si la distribución estándar de origen y la de destino están en diferentes Cuentas de AWS, debe deshabilitar primero la distribución estándar de origen.
> - La distribución estándar de destino debe configurarse tal y como se describe en the section called "Configuración de la distribución estándar o el inquilino de distribución de destino".

Solicitud

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

Este comando elimina el nombre de dominio alternativo de la distribución estándar de origen y lo mueve a la distribución estándar de destino.

2. Una vez que la distribución estándar de destino esté completamente implementada, actualice la configuración de DNS para apuntar el registro DNS del nombre de dominio alternativo al nombre de dominio de distribución de la distribución estándar de destino. Por ejemplo, el registro DNS apuntaría el nombre de dominio alternativo (`www.example.com`) al nombre de dominio proporcionado por CloudFront d111111abcdef8.cloudfront.net.

Para obtener más información, consulte el comando associate-alias en la Referencia de comandos de la AWS CLI.

Utilice un comodín para mover un nombre de dominio alternativo

Si la distribución de origen está en una Cuenta de AWS diferente a la distribución de destino y la distribución de origen está habilitada, puede utilizar un comodín para mover el nombre de dominio alternativo.

> **Note**
>
> No puede utilizar un comodín para mover un dominio apex (como ejemplo.com). Para mover un dominio de vértice cuando las distribuciones de origen y destino están en diferentes Cuentas de AWS, póngase en contacto con Soporte. Para obtener más información, consulte the section called “Contacte a AWS Support para mover un nombre de dominio alternativo”.

Utilizar un comodín para mover un nombre de dominio alternativo

> **Note**
>
> Este proceso implica varias actualizaciones de sus distribuciones. Espere a que cada distribución implemente completamente el último cambio antes de continuar con el siguiente paso.

1. Actualice la distribución de destino para añadir un nombre de dominio alternativo comodín que cubra el nombre de dominio alternativo que está moviendo. Por ejemplo, si el nombre de dominio alternativo que está moviendo es www.ejemplo.com, añada el nombre de dominio alternativo *.ejemplo.com a la distribución de destino. Para ello, el certificado SSL/TLS en la distribución de destino debe incluir el nombre de dominio comodín. Para obtener más información, consulte the section called “Actualizar una distribución”.
2. Actualice la configuración de DNS del nombre de dominio alternativo para que apunte al nombre de dominio de la distribución de destino. Por ejemplo, si el nombre de dominio alternativo que está moviendo es www.ejemplo.com, actualice el registro de DNS de www.ejemplo.com para dirigir el tráfico al nombre de dominio de la distribución de destino (por ejemplo, d111111abcdef8.cloudfront.net).

> **Note**
>
> Incluso después de actualizar la configuración de DNS, el nombre de dominio alternativo sigue siendo atendido por la distribución de origen, ya que allí es donde el nombre de dominio alternativo está configurado actualmente.

3. Actualice la distribución de origen para eliminar el nombre de dominio alternativo Para obtener más información, consulte Actualizar una distribución.
4. Actualice la distribución de destino para añadir el nombre de dominio alternativo Para obtener más información, consulte Actualizar una distribución.
5. Utilice dig (o una herramienta de consulta de DNS similar) para validar que el registro de DNS para el nombre de dominio alternativo se resuelve en el nombre de dominio de la distribución de destino.
6. (Opcional) Actualice la distribución de destino para eliminar el nombre de dominio alternativo comodín.

Contacte a AWS Support para mover un nombre de dominio alternativo

Si las distribuciones de origen y destino están en diferentes Cuentas de AWS y no tiene acceso a la Cuenta de AWS de la distribución de origen o no puede deshabilitar la distribución de origen, puede ponerse en contacto con Soporte para mover el nombre de dominio alternativo.

Para contactar a Soporte para mover un nombre de dominio alternativo

1. Configure una distribución de destino, incluido el registro TXT de DNS que apunte a la distribución de destino. Para obtener más información, consulte Configuración de la distribución estándar o el inquilino de distribución de destino.
2. Contacte a Soporte para solicitarles que verifiquen que es propietario del dominio y que muevan el dominio a una nueva distribución de CloudFront.
3. Una vez que la distribución de destino esté completamente implementada, actualice la configuración de DNS para apuntar el registro DNS del nombre de dominio alternativo al nombre de dominio de distribución de la distribución de destino.

Eliminación de un nombre de dominio alternativo

Si desea dejar de direccionar tráfico para un dominio o subdominio a una distribución de CloudFront, siga los pasos de esta sección para actualizar la configuración de DNS y la distribución de CloudFront.

Es importante que elimine los nombres de dominio alternativos desde la distribución, además de actualizar su configuración de DNS. Esto ayuda a evitar problemas más tarde si desea asociar el nombre de dominio con otra distribución de CloudFront. Si un nombre de dominio alternativo ya está asociado a una distribución, no se puede configurar con otra.

> **Note**
>
> Si desea eliminar el nombre de dominio alternativo de esta distribución para que pueda añadirlo a otra, siga los pasos que se indican en Desplazamiento de un nombre de dominio alternativo. Si sigue los pasos que se indican aquí (para eliminar un dominio) y, a continuación, agrega el dominio a otra distribución, habrá un periodo de tiempo durante el cual el dominio no se enlazará con la nueva distribución ya que CloudFront se está propagando a las actualizaciones a las ubicaciones de borde.

Para eliminar un nombre de dominio alternativo de una distribución

1. Para empezar, dirija el tráfico de Internet de su dominio a otro recurso que no sea la distribución de CloudFront, como un balanceador de carga de Elastic Load Balancing. O bien, puede eliminar el registro DNS que está dirigiendo tráfico a CloudFront.

   Lleve a cabo una de las siguientes acciones, en función del servicio DNS para su dominio:

   - Si utiliza Route 53, actualice o elimine registros de alias o registros CNAME. Para obtener más información, consulte Edición de registros o Eliminación de registros.
   - Si utiliza otro proveedor de servicios de DNS, utilice el método proporcionado por el proveedor del servicio DNS para actualizar o eliminar el registro CNAME que dirige el tráfico hacia CloudFront. Para obtener más información, consulte la documentación de su proveedor de servicios de DNS.
2. Después de actualizar los registros DNS de su dominio, espere hasta que los cambios se hayan propagado y los servicios de resolución de nombres DNS redirigen el tráfico al nuevo recurso.

Puede comprobar cuando se completa esto mediante la creación de algunos enlaces de prueba que utilicen su dominio en la URL.

3. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home y actualice su distribución de CloudFront para eliminar el nombre de dominio haciendo lo siguiente:

   a. Elija la ID de la distribución que desea actualizar.

   b. En la pestaña General, seleccione Edit.

   c. En Alternate Domain Names (CNAMEs) (Nombres de dominio alternativos (CNAMEs)), elimine los nombres de dominio alternativos (o nombres de dominio) que ya no desee utilizar para su distribución.

   d. Elija Yes, Edit (Sí, editar).

Uso de comodines en nombres de dominio alternativos

Al añadir nombres de dominio alternativos, puede utilizar el comodín * al principio de un nombre de dominio en lugar de añadir subdominios individualmente. Por ejemplo, con un nombre de dominio alternativo *.ejemplo.com, puede utilizar cualquier nombre de dominio que termine en ejemplo.com en sus URL, como www.ejemplo.com, nombre-producto.ejemplo.com, marketing.nombre-producto.ejemplo.com, etc. La ruta hacia el objeto es la misma, independientemente del nombre de dominio, por ejemplo:

- www.ejemplo.com/imágenes/imagen.jpg
- nombre-producto.ejemplo.com/imágenes/imagen.jpg
- marketing.nombre-producto.ejemplo.com/imágenes/imagen.jpg

Siga estos requisitos para nombres de dominio alternativos que incluyan comodines:

- El nombre de dominio alternativo debe empezar con un asterisco y un punto (*.).
- No puede utilizar un comodín para reemplazar parte de un nombre de subdominio, como este: *dominio.ejemplo.com
- No puede sustituir un subdominio en el medio de un nombre de dominio, como este: subdominio.*.ejemplo.com.

- Todos los nombres de dominio alternativos, incluidos los nombres de dominio alternativos que utilizan comodines, deben quedar cubiertos por el nombre alternativo de asunto (SAN) en el certificado.

Un nombre de dominio alternativo comodín, tal como *.ejemplo.com, puede incluir otro nombre de dominio alternativo que esté en uso, tal como ejemplo.com.

Uso de WebSockets con distribuciones de CloudFront

Amazon CloudFront admite el uso de WebSocket, un protocolo basado en TCP que resulta útil cuando se necesitan conexiones bidireccionales de larga duración entre clientes y servidores. Una conexión persistente suele ser un requisito con aplicaciones en tiempo real. Las situaciones en las que puede utilizar WebSockets incluyen plataformas de chat sociales, espacios de trabajo de colaboración en línea, juegos de varios jugadores, y servicios que proporcionan fuentes de distribución de datos en tiempo real como las plataformas de comercio financiero. Los datos a través de una conexión WebSocket pueden fluir en ambas direcciones para la comunicación de dúplex completo.

La funcionalidad WebSocket se habilita automáticamente para operar con cualquier distribución. Para usar WebSockets, configure una de las siguientes opciones en el comportamiento de caché que se adjunta a la distribución:

- Reenviar todos los encabezados de solicitud de lector al origen. Puede utilizar la política de solicitud de origen administrada por AllViewer.
- Reenviar específicamente los encabezados de solicitud `Sec-WebSocket-Key` y `Sec-WebSocket-Version` en la política de solicitud de origen.

Cómo funciona el protocolo WebSocket

El protocolo WebSocket es un protocolo independiente, basado en TCP que le permite evitar cierta sobrecarga (y potencialmente mayor latencia) de HTTP.

Para establecer una conexión WebSocket regular, el cliente envía una solicitud HTTP que utiliza actualización de semántica de HTTP para cambiar el protocolo. El servidor puede completar el protocolo de enlace. La conexión WebSocket permanece abierta y el cliente o el servidor puede enviar marcos de datos entre sí sin tener que establecer nuevas conexiones cada vez.

De forma predeterminada, el protocolo WebSocket utiliza el puerto 80 para conexiones WebSocket regulares y puerto 443 para conexiones WebSocket sobre TLS. Las opciones que elija para CloudFront Política de protocolo para lectores y Protocolo (solo orígenes personalizados) se aplican a las conexiones WebSocket y también al tráfico HTTP.

Requisitos de WebSocket

Las solicitudes de WebSocket deben cumplir con RFC 6455 en los siguientes formatos estándar.

Example Ejemplo de solicitud del cliente

```
GET /chat HTTP/1.1
Host: server.example.com
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: dGhlIHNhbXBsZSBub25jZQ==
Origin: https://example.com
Sec-WebSocket-Protocol: chat, superchat
Sec-WebSocket-Version: 13
```

Example Ejemplo de respuesta de servidor

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: s3pPLMBiTxaQ9kYGzzhZRbK+xOo=
Sec-WebSocket-Protocol: chat
```

Si la conexión WebSocket la desconecta el cliente o el servidor, o mediante una interrupción de red, se espera que las aplicaciones cliente vuelvan a iniciar la conexión con el servidor.

Encabezados de WebSocket recomendados

Para evitar problemas inesperados relacionados con la compresión al utilizar WebSockets, le recomendamos que incluya los siguientes encabezados en una política de solicitud de origen:

- `Sec-WebSocket-Key`
- `Sec-WebSocket-Version`
- `Sec-WebSocket-Protocol`

- `Sec-WebSocket-Accept`
- `Sec-WebSocket-Extensions`

> **Note**
>
> Actualmente, CloudFront solo admite conexiones WebSocket a través del protocolo HTTP/1.1.

Solicitud de direcciones IP estáticas de anycast para utilizarlas en las listas de permitidos

Puede solicitar direcciones IP estáticas de anycast a CloudFront para usarlas con sus distribuciones. Las listas de direcciones IP estáticas de anycast solo pueden contener direcciones IP IPv4 o direcciones IP IPv4 e IPv6. Estas direcciones IP están dedicadas a la Cuenta de AWS y están distribuidas por regiones geográficas.

Puede solicitar 21 direcciones IP estáticas de anycast para listas de permitidos con proveedores de red de forma que pueda eximir del pago de tarifas de datos a los lectores que accedan a la aplicación. De forma alternativa, puede utilizar estas IP estáticas en firewalls de seguridad salientes para controlar el intercambio de tráfico con aplicaciones aprobadas. Las listas de IP estáticas de anycast pueden utilizarse con una o varias distribuciones.

Si desea habilitar el enrutamiento de dominios apex (como example.com) directamente a las distribuciones de CloudFront, puede solicitar tres direcciones IP estáticas de anycast para este caso de uso. A continuación, agregue registros A en el DNS para apuntar el dominio apex a CloudFront.

Las IP estáticas de anycast funcionan con indicación del nombre de servidor (SNI). Para obtener más información, consulte Uso de SNI para atender solicitudes HTTPS (funciona en la mayoría de los clientes).

Requisitos previos

Para usar listas de direcciones IP estáticas de anycast con la distribución de CloudFront, debe seleccionar Usar todas las ubicaciones periféricas para la clase de precio de la distribución. Para obtener más información sobre los precios, consulte Precios de CloudFront.

Solicitud de una lista de direcciones IP estáticas de anycast

Solicite una lista de direcciones IP estáticas de anycast para usarla con su distribución de CloudFront.

Para solicitar una lista de direcciones IP estáticas de anycast

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija IP estáticas.
3. En Solicitar, elija el enlace para ponerse en contacto con el departamento de ingeniería de soporte de CloudFront.
4. Proporcione la información de su carga de trabajo (solicitudes de bytes por segundo y solicitudes por segundo).
5. Los ingenieros de soporte de CloudFront revisan su solicitud. El proceso de revisión puede tardar hasta dos días.

Una vez aprobada la solicitud, puede crear una lista de direcciones IP estáticas de anycast y asociarla a una o varias distribuciones.

Creación de una lista de direcciones IP estáticas de anycast

Antes de empezar, solicite una lista de direcciones IP estáticas de anycast como se explica en la sección anterior.

Para crear una lista de direcciones IP estáticas de anycast

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija IP estáticas.
3. Seleccione Crear lista de IP de anycast.
4. En Nombre, ingrese un nombre.
5. Para Casos de uso de IP estáticas, seleccione el caso de uso adecuado.
6. Para Tipo de dirección IP, elija una de las siguientes opciones:
   - IPv4: asigne una lista de solo direcciones IPv4
   - Dualstack: asigne una lista de direcciones IPv4 e IPv6

7. Revise los términos y precios del servicio y seleccione Enviar.

Una vez creada la lista de direcciones IP estáticas, puede ver las direcciones IP asignadas en la página de detalles de la lista de direcciones IP estáticas. También puede asociar distribuciones a la lista de direcciones IP estáticas.

Asociación de una lista de direcciones IP estáticas de anycast a una distribución existente

Antes de empezar, solicite y cree una lista de direcciones IP estáticas de anycast como se explica en las secciones anteriores.

Compruebe que la siguiente configuración de distribución sea compatible con la lista de IP estáticas de anycast:

- Clase de precio tiene la configuración Usar todas las ubicaciones periféricas (mejor rendimiento).
- Si IPv6 está habilitado, puede asociar una lista de direcciones IP estáticas de anycast de doble pila. Una lista de IP estáticas de anycast que solo tenga direcciones IPv4 no se puede asociar a distribuciones con IPv6 habilitado.

Para asociar una lista de direcciones IP estáticas de anycast a una distribución existente

- Realice una de las siguientes acciones:
  - Asocie la lista de direcciones IP estáticas de la página de detalles de la lista de direcciones IP estáticas:
    1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
    2. En el panel de navegación izquierdo, elija IP estáticas.
    3. Elija el nombre de su lista de direcciones IP estáticas.
    4. Elija Asociar distribuciones.
    5. Seleccione una o varias distribuciones y elija Asociar distribuciones.
  - Asocie la lista de direcciones IP estáticas de la página de detalles de la distribución:
    1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
    2. En el panel de navegación izquierdo, elija Distribuciones.

3. Elija el nombre de su distribución.
4. En Configuración de la pestaña General, elija Editar.
5. En Lista de IP de anycast, seleccione la lista de direcciones IP estáticas de anycast para utilizarla con esta distribución.
6. Seleccione Save changes (Guardar cambios).

Asociación de una lista de direcciones IP estáticas de anycast a una nueva distribución

Antes de empezar, solicite y cree una lista de direcciones IP estáticas de anycast como se explica en las secciones anteriores.

Para asociar una lista de direcciones IP estáticas de anycast a una nueva distribución

- Cree una distribución de nueva. Para obtener más información, consulte Creación de una distribución de CloudFront en la consola. En Configuración, debe seleccionar lo siguiente para usar su lista de direcciones IP estáticas de anycast:
  - En Lista de IP de anycast, seleccione su lista de direcciones IP estáticas de anycast en la lista desplegable.
  - En Clase de precio, seleccione Usar todas las ubicaciones periféricas (mejor rendimiento).
  - Nota: Si la IP estática de Anycast solo utiliza IPv4 y no dualstack, para IPv6, seleccione Desactivar.

Termine de crear su distribución. Puede elegir otros ajustes y configuraciones que no sean necesarios para las listas de direcciones IP estáticas de anycast en función de sus necesidades.

Para obtener más información sobre las cuotas relacionadas con las listas de direcciones IP estáticas de anycast, consulte Amazon CloudFront endpoints and quotas en Referencia general de AWS.

Asociación de una lista de direcciones IP estáticas de anycast a un grupo de conexión

Antes de empezar, solicite y cree una lista de direcciones IP estáticas de anycast como se explica en las secciones anteriores.

Asociación de una lista de direcciones IP estáticas de anycast a un grupo de conexión nuevo

1. Asegúrese de haber habilitado los grupos de conexiones en Configuración.
2. Cree un grupo de conexiones. Para obtener más información, consulte Creación de un grupo de conexiones personalizado.
3. En Configuración, debe seleccionar lo siguiente para usar la lista de direcciones IP estáticas de Anycast.
   - En Lista de IP de anycast, seleccione su lista de direcciones IP estáticas de anycast en la lista desplegable.
4. Termine de crear el grupo de conexión.

> **Note**
>
> Si la IP estática de Anycast solo utiliza IPv4 y no dualstack, para IPv6, seleccione Desactivar.

Para obtener más información sobre las cuotas relacionadas con las listas de direcciones IP estáticas de anycast, consulte Amazon CloudFront endpoints and quotas en Referencia general de Amazon Web Services.

Actualización de una lista de direcciones IP estáticas de Anycast

Una vez que haya creado la dirección IP estática de Anycast y la haya asociado a una distribución, puede cambiar el tipo de dirección IP de la lista de IP estáticas de Anycast.

Actualización de una lista de direcciones IP estáticas de Anycast

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija IP estáticas.
3. Elija el nombre de su lista de direcciones IP estáticas.
4. Elija Edit (Edición de).
5. Para Tipo de dirección IP, elija una de las siguientes opciones:
   - IPv4: asigne una lista de solo direcciones IPv4
   - Dualstack: asigne una lista de direcciones IPv4 e IPv6

> **Note**
>
> No puede elegir IPv4 si la distribución asociada ya ha habilitado IPv6. Para ello, desactive IPv6 antes de poder actualizar el tipo de dirección IP de la IP estática de Anycast. Para obtener más información, consulte Habilitación de IPv6 para las distribuciones de CloudFront.

6. Elija Enviar para guardar los cambios y actualizar la lista de IP estáticas de Anycast.

Incorporación de su propia IP a CloudFront mediante IPAM

Este tutorial muestra cómo utilizar IPAM para administrar sus CIDR de BYOIP para listas de direcciones IP estáticas de Anycast de CloudFront.

Temas

- ¿Qué es BYOIP para las IP estáticas de Anycast?
- ¿Por qué usar esta característica?
- Requisitos previos
- Paso 1: solicitud de una lista de direcciones IP estáticas de Anycast
- Paso 2: creación de una lista de direcciones IP estáticas de Anycast
- Paso 3: Crear una distribución de CloudFront
- Paso 4: asociación con los recursos de CloudFront
- Paso 5: prepare todo para la migración
- Paso 6: anuncio de CIDR a nivel mundial

¿Qué es BYOIP para las IP estáticas de Anycast?

CloudFront permite incorporar las propias direcciones IPv4 a través del BYOIP de IPAM para servicios globales. A través de la interfaz unificada de IPAM, los clientes pueden crear grupos de direcciones IP dedicados con sus propias direcciones IP (BYOIP) y asignarlos a las distribuciones de CloudFront, al tiempo que aprovechan la red mundial de entrega de contenido de AWS para entregar sus aplicaciones y contenido. Las direcciones IP se anuncian desde varias ubicaciones periféricas de CloudFront simultáneamente mediante el enrutamiento de anycast.

¿Por qué usar esta característica?

Controle el acceso de red en las listas de permitidos para:

- Permitir incluir direcciones IP en las listas de los proveedores de red para eximir de cargos por uso de datos a los espectadores autorizados
- Configurar los firewalls de seguridad salientes para restringir el tráfico solo a las aplicaciones aprobadas

Simplificar las operaciones y las migraciones

- Enrutar los dominios Apex (example.com) directamente a CloudFront agregando registros A que apunten a las IP estáticas
- Migrar desde otras CDN sin actualizar la infraestructura de IP ni las configuraciones de firewall
- Mantener las listas de IP permitidas existentes con los socios y clientes
- Compartir una sola lista de direcciones IP estáticas de Anycast en varias distribuciones de CloudFront

Marca coherente

- Mantener el espacio de direcciones IP actual para una marca coherente al pasar a AWS

Requisitos previos

Para usar listas de direcciones IP estáticas de anycast con la distribución de CloudFront, debe seleccionar Usar todas las ubicaciones periféricas para la clase de precio de la distribución. Para obtener más información sobre los precios, consulte Precios de CloudFront. Para traiga su propia IP (BYOIP), también debe desactivar IPv6 para el grupo de distribución o conexión.

Complete estos pasos antes de empezar:

- Configuración de IPAM: consulte Integración de IPAM con las cuentas y Creación de un IPAM.
- Verificación del dominio: Verificación del control de dominio.
- Cree un grupo de nivel superior: siga los pasos 1 a 2 en Lleve su propio CIDR de IPv4 a IPAM.
- Cree un grupo de IPAM con la configuración local como global para usarlo con CloudFront. Para obtener más información, consulte Lleve su propia IP a CloudFront mediante IPAM.

> **Note**
>
> Requiere tres bloques de CIDR de IPv4 de /24.

Paso 1: solicitud de una lista de direcciones IP estáticas de Anycast

Solicite una lista de direcciones IP estáticas de anycast para usarla con su distribución de CloudFront.

Para solicitar una lista de direcciones IP estáticas de anycast

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija IP estáticas.
3. En Solicitar, elija el enlace para ponerse en contacto con el departamento de ingeniería de soporte de CloudFront.
4. Proporcione la información de su carga de trabajo (solicitudes de bytes por segundo y solicitudes por segundo).
5. Los ingenieros de soporte de CloudFront revisan su solicitud. El proceso de revisión puede tardar hasta dos días.
6. Una vez aprobada la solicitud, puede crear una lista de direcciones IP estáticas de anycast y asociarla a una o varias distribuciones.

Paso 2: creación de una lista de direcciones IP estáticas de Anycast

Antes de empezar, solicite una lista de direcciones IP estáticas de anycast como se explica en la sección anterior.

Para crear una lista de direcciones IP estáticas de anycast

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija IP estáticas.
3. Seleccione Crear lista de IP de anycast.
4. En Nombre, ingrese un nombre.

5. Para Casos de uso de IP estática, seleccione BYOIP como caso de uso.

Los siguientes pasos difieren del proceso de BYOIP regional estándar y establecen el patrón de los servicios globales:

AWS CLI

Instalación o actualización de la versión más reciente de la CLI de AWS. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

1. Recupere IpamPoolArn del grupo de IPAM en el que se aprovisionaron los bloques de CIDR. Para obtener más información, consulte Lleve su propio CIDR de IPv4 público a IPAM solo por medio de la CLI de AWS.
2. Cree una lista de IP de Anycast con sus bloques de CIDR y la configuración de IPAM:

```
aws cloudfront create-anycast-ip-list \
    --name byoip-aip-1 \
    --ip-count 3 \
    --region us-east-1 \
    --ip-address-type ipv4 \
    --ipam-cidr-configs
 '[{"Cidr":"1.1.1.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"2.2.2.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"3.3.3.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"}]'
```

> **Note**
>
> No puede seleccionar la dirección IP específica desde el grupo. CloudFront hará esto automáticamente.

Paso 3: Crear una distribución de CloudFront

Para CloudFront, puede seguir las instrucciones para crear una distribución estándar o utilizar distribuciones multiusuario.

Paso 4: asociación con los recursos de CloudFront

- Asociación de una lista de direcciones IP estáticas de anycast a una distribución existente
- Asociación de una lista de direcciones IP estáticas de anycast a una nueva distribución
- Asociación de una lista de direcciones IP estáticas de anycast a un grupo de conexión

Paso 5: prepare todo para la migración

Para obtener más información, consulte el Paso 4: preparación para la migración en la Guía del usuario de Amazon VPC.

Paso 6: anuncio de CIDR a nivel mundial

Para obtener más información, consulte el Paso 5: anuncio de CIDR a nivel mundial en la Guía del usuario de Amazon VPC.

Uso de gRPC con distribuciones de CloudFront

Amazon CloudFront es compatible con gRPC, un marco de llamadas a procedimientos remotos (RPC) de código abierto basado en HTTP/2. gRPC ofrece streaming bidireccional y protocolo binario que almacena en búfer cargas útiles, lo que lo hace adecuado para aplicaciones que requieren comunicaciones de baja latencia.

CloudFront recibe las solicitudes de gRPC y las entrega directamente a sus orígenes. Puede usar CloudFront para entregar cuatro tipos de servicios de gRPC:

- RPC unitario
- RPC de streaming de servidores
- RPC de streaming de cliente
- RPC de streaming bidireccional

Cómo funciona gRPC en CloudFront

Para configurar gRPC en CloudFront, defina un origen que proporcione un servicio de gRPC como origen de la distribución. Puede usar orígenes que proporcionen servicios de gRPC y que no sean de

gRPC. CloudFront determina si la solicitud entrante es una solicitud de gRPC o una solicitud HTTP/HTTPS en función del encabezado de `Content-Type`. Si el encabezado de `Content-Type` de una solicitud tiene un valor de `application/grpc`, la solicitud se considera una solicitud de gRPC y CloudFront la entregará al origen.

> **Note**
>
> Para activar una distribución para administrar solicitudes de gRPC, incluya HTTP/2 como una de las versiones HTTP compatibles y permita los métodos HTTP, como `POST`. El punto de conexión de origen de gRPC debe estar configurado para admitir HTTPS, ya que CloudFront solo admite conexiones gRPC seguras (basadas en HTTPS). gRPC solo admite HTTPS de punto a punto. Si utiliza un origen personalizado, compruebe que la configuración de su protocolo sea compatible con HTTPS.

Para activar la compatibilidad con gRPC en su distribución, complete los siguientes pasos:

1. Actualice el comportamiento de la caché de su distribución para permitir los métodos HTTP, como el método `POST`.
2. Seleccione la casilla de verificación de gRPC que aparece después de seleccionar el método `POST`.
3. Especifique HTTP/2 como una de las versiones HTTP compatibles.

Para obtener más información, consulte los temas siguientes:

- Cómo permitir solicitudes de gRPC a través de HTTP/2
- GrpcConfig en la Referencia de la API de Amazon CloudFront

Como gRPC se usa solo para el tráfico de API que no se puede almacenar en caché, las configuraciones de la caché no afectarán a las solicitudes de gRPC. Puede usar una política de solicitud de origen para agregar encabezados personalizados a las solicitudes de gRPC que se envían al origen de gRPC. Puede usar AWS WAF con CloudFront para administrar el acceso a la distribución de gRPC, controlar los bots y proteger las aplicaciones de gRPC de las vulnerabilidades de la web. CloudFront gRPC admite CloudFront Functions.

Además del estado HTTPS, recibirá grpc-status junto con la respuesta de gRPC. Para obtener una lista de los posibles valores de grpc-status, consulte: Status codes and their use in gRPC.

Notas

gRPC no admite las siguientes características de CloudFront:

- Respuestas de error personalizadas
- La conmutación por error de origen no es compatible con gRPC, ya que gRPC utiliza el método `POST`. CloudFront conmuta por error al origen secundario solo cuando el método HTTP de la solicitud del lector es `GET`, `HEAD` u `OPTIONS`.
- CloudFront entrega las solicitudes de gRPC directamente al origen y evita la caché perimetral regional (REC). Como gRPC omite REC, gRPC no es compatible con Lambda@Edge ni con Origin Shield.
- gRPC no admite las reglas de inspección del cuerpo de la solicitud de AWS WAF. Si habilitó estas reglas en la ACL web para una distribución, cualquier solicitud que utilice gRPC ignorará las reglas de inspección del cuerpo de la solicitud. Se seguirán aplicando todas las demás reglas de AWS WAF. Para obtener más información, consulte Habilitación de AWS WAF para distribuciones.

Trabajo con recursos compartidos en CloudFront

Amazon CloudFront se integra con AWS Resource Access Manager (AWS RAM) para permitir el uso compartido de recursos. AWS RAM lo habilita para compartir algunos recursos de CloudFront con otras Cuentas de AWS o a través de AWS Organizations. Con AWS RAM, puede compartir recursos de su propiedad creando un uso compartido de recursos. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los consumidores pueden incluir lo siguiente:

- Cuentas de AWS específicas dentro o fuera de su organización en AWS Organizations
- Una unidad organizativa dentro de la organización en AWS Organizations
- Toda la organización en AWS Organizations

Para obtener más información sobre AWS RAM, consulte la Guía del usuario de AWS RAM.

En este tema se explica cómo compartir los recursos que le pertenecen y cómo utilizar los recursos que se comparten con usted.

Contenido

- Requisitos previos para compartir recursos
- Uso compartido de un origen de la VPC
- Uso de un origen de VPC compartido
- Identificación de un origen de la VPC compartido
- Desactivación de un origen de la VPC compartido
- Responsabilidades y permisos de orígenes de la VPC compartidos
- Facturación y medición
- Cuotas de recursos compartidos

Requisitos previos para compartir recursos

- Debe tener la política administrada AWSRAMDefaultPermissionCloudFront para conceder acceso de solo lectura al recurso compartido. Para obtener más información, consulte AWSRAMDefaultPermissionCloudFront.

- Para compartir un origen de VPC, debe ser el propietario en la Cuenta de AWS. Esto significa que el recurso debe asignarse o suministrarse en su cuenta. No puede compartir un recurso que le han compartido a usted.
- Para compartir un recurso con su organización o con una unidad organizativa en AWS Organizations, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM.

Uso compartido de un origen de la VPC

> **Note**
>
> Actualmente, CloudFront admite el uso compartido de orígenes de VPC. Si aún no ha creado uno, consulte Restricción del acceso con orígenes de la VPC.

Al compartir un origen de la VPC que posee con otras Cuentas de AWS, las habilita para usar ese recurso como origen de sus distribuciones de CloudFront.

Para compartir un origen de VPC, debe agregarlo a un recurso compartido. Un recurso compartido es un recurso de AWS RAM que le permite compartir los recursos a través de Cuentas de AWS.

Un recurso compartido especifica lo siguiente:

- Los recursos que desea compartir.
- Los consumidores con los que se comparten.
- La política administrada del servicio que determina los permisos a los recursos.

Cuando comparte un origen de VPC con la consola de CloudFront, la agrega a un recurso compartido existente. Si aún no tiene un recurso compartido, puede crear uno al compartir un origen de la VPC desde la consola de CloudFront. También puede usar la consola de AWS RAM o AWS CLI para crear uno de forma independiente.

Puede compartir los orígenes de la VPC con otras Cuentas de AWS y AWS Organizations.

- Si comparte el recurso con una organización de AWS, todos los consumidores de esa organización específica pueden acceder al origen de la VPC.

- Si comparte el recurso con una organización de Cuenta de AWS de la que no forma parte, los consumidores recibirán una invitación para aceptar el recurso compartido. Una vez aceptado, pueden utilizar el origen de VPC.

Puede compartir un origen de VPC que posea con la consola de CloudFront, la consola de AWS RAM o la AWS CLI.

Creación de un recurso compartido mediante la consola de CloudFront

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Orígenes de VPC.
3. Seleccione uno o más recursos y elija Compartir origen de VPC.
4. Elija Crear recurso compartido.
5. Para Nombre, ingrese un nombre descriptivo para el recurso compartido.
6. Para Tipo de entidad principal, elija una de las siguientes opciones:
   - Cuenta de AWS: conceda acceso a una Cuenta de AWS específica.
   - Unidad organizativa: conceda acceso a una unidad organizativa (UO) específica.
   - Organización: conceda acceso a toda la organización, incluidas las unidades organizativas secundarias y Cuentas de AWS.

   a. Si elige Cuenta de AWS, ingrese el número de ID de la cuenta. Puede elegir Agregar nueva cuenta para agregar hasta 5 Cuentas de AWS.
   b. Si elige Unidad organizativa, ingrese el ARN de la unidad OU. Solo puede ingresar una unidad organizativa.
   c. Si ha elegido Organización, ingrese el ARN de la organización. Solo puede ingresar una organización.
7. Elija Compartir recursos.

   De forma predeterminada, CloudFront aplica la política administrada AWSRAMDefaultPermissionCloudFront AWS al recurso compartido. Esta política permite realizar acciones de solo lectura en el recurso compartido, de modo que las cuentas consumidoras no pueden actualizar ni eliminar el recurso compartido. No puede editar ni eliminar esta política del recurso compartido.

> **Tip**
>
> Tras crear el recurso compartido, puede agregar más Cuentas de AWS desde la consola de AWS RAM. Para obtener más información, consulte Actualizar un recurso compartido en AWS RAM en la Guía del usuario de AWS RAM.

Cómo compartir un origen de la VPC que posea mediante la consola de CloudFront

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Orígenes de VPC.
3. Seleccione un recurso y elija Compartir origen de VPC.
4. En la página Compartir origen de VPC, puede seleccionar un recurso compartido existente al que desee agregar este origen de VPC.
5. Elija Compartir recurso.

   En la página de detalles del recurso, en Compartido con, puede ver que el origen de la VPC se comparte con los siguientes detalles:

   - Nombres de recursos compartidos
   - Estado de uso compartido
   - Hora de la última modificación

Tras crear y compartir el recurso compartido con las cuentas consumidoras, estas disponen de 12 horas para aceptar la invitación. Para obtener más información, consulte Aceptar y rechazar invitaciones a recursos compartidos en la Guía del usuario de AWS RAM.

> **Important**
>
> Para permitir que las cuentas consumidoras utilicen el origen de la VPC para su distribución de CloudFront, también debe proporcionar el Elastic Load Balancing de origen de la VPC o el punto de conexión de Amazon EC2.

Cómo compartir un origen de la VPC que posea mediante la consola de AWS RAM

Cree un recurso compartido y, a continuación, elija los recursos de CloudFront que desee agregarlo. Para obtener más información, consulte Creación de un recurso compartido en la Guía del usuario de AWS RAM.

Cómo compartir un origen de la VPC que posea mediante la AWS CLI

Utilice el comando create-resource-share.

Uso de un origen de VPC compartido

Para usar un origen de la VPC compartido, la cuenta que recibe la invitación debe aceptar el recurso compartido. Para ello, acceda a la consola de AWS Resource Access Manager de la región Este de EE. UU. (Norte de Virginia) y acepte las solicitudes pendientes en la pestaña Pendientes. Para obtener más información, consulte Aceptar recursos compartidos en la Guía del usuario de AWS RAM.

Tras aceptar el recurso compartido, podrá utilizar el origen de la VPC como origen de las distribuciones de CloudFront.

Uso de un origen de la VPC compartido

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, para Distribuciones, realice alguna de las siguientes acciones:
   - Para una distribución nueva, elija Crear distribución.
   - Para una distribución existente, elija el ID de distribución.
3. Para Tipo de origen, elija Origen de la VPC y, a continuación, especifique el origen de la VPC que se compartió con usted.
4. Para el Punto de conexión de origen de la VPC, ingrese el nombre de DNS privado de la instancia de Amazon EC2, del equilibrador de carga de Elastic Load Balancing o del dominio de origen. Si aún no tiene este valor, debe obtenerlo de la Cuenta de AWS que posee el origen de la VPC. Si aún no tiene este punto de conexión, debe obtenerlo de la Cuenta de AWS que posee el origen de la VPC.
5. Siga los pasos de la consola para crear o actualizar la distribución.

Identificación de un origen de la VPC compartido

Los propietarios y consumidores pueden identificar orígenes de la VPC compartidos mediante la consola de CloudFront y la AWS CLI.

Cómo identificar un origen de la VPC compartido con la consola de CloudFront

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Orígenes de VPC. Puede usar la columna de ID de propietario para identificar la Cuenta de AWS a la que pertenece el recurso.
3. Seleccione un recurso.
4. En la página de detalles del recurso, en Compartido con, puede ver que el origen de la VPC se comparte con los siguientes detalles:
   - Nombres de recursos compartidos
   - Estado de uso compartido
   - Hora de la última modificación

Desactivación de un origen de la VPC compartido

Al dejar de compartir un recurso, las Cuentas de AWS (cuentas consumidoras) ya no pueden usar ese recurso para nuevas distribuciones ni actualizar las distribuciones existentes.

> **Note**
>
> Si deja de compartir un recurso, las distribuciones existentes que todavía utilizan ese recurso permanecen activas y seguirán atendiendo el tráfico. Sin embargo, estas distribuciones no se pueden editar hasta que se elimine el recurso no compartido como origen. Recomendamos asegurarse de que las cuentas consumidoras dejen de usar el recurso no compartido antes de dejar de compartirlo.

Para dejar de compartir un origen de la VPC compartido que posee, debe quitarlo del recurso compartido. Para ello, puede utilizar la consola de CloudFront, la consola de AWS RAM o la AWS CLI.

Cómo dejar de compartir un origen de la VPC compartido que posee mediante la consola de CloudFront

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Orígenes de VPC.
3. Seleccione un recurso y elija Dejar de compartir.
4. Revise los detalles en el cuadro de diálogo Dejar de compartir un recurso y, a continuación, elija Dejar de compartir. Las entidades principales mostradas ya no tendrán acceso al recurso compartido.

Cómo dejar compartir un origen de la VPC compartido que posee mediante la consola de AWS RAM

Consulte Actualización de un recurso compartido en la Guía del usuario de AWS RAM.

Cómo dejar compartir un origen de la VPC compartido que posee mediante la AWS CLI

Utilice el comando disassociate-resource-share.

Responsabilidades y permisos de orígenes de la VPC compartidos

Permisos de los propietarios

Como cuenta propietaria del recurso, asegúrese de que cualquier cuenta que consuma recursos deje de usar el recurso antes de dejar de compartirlo o eliminarlo.

Permisos de los consumidores

Las cuentas consumidoras pueden usar recursos compartidos como orígenes de las distribuciones de CloudFront, pero no pueden editar ni eliminar los recursos. De forma predeterminada, la política AWSRAMDefaultPermissionCloudFront de AWS administrada se aplica al recurso compartido de la cuenta compartida (la cuenta propietaria del recurso).

AWSRAMDefaultPermissionCloudFront

Al crear un recurso compartido en CloudFront, CloudFront utiliza la política administrada AWSRAMDefaultPermissionCloudFront AWS y la aplica al recurso compartido. Esta política otorga permisos de solo lectura a recursos de CloudFront que pueden compartirse entre el propietario del recurso y la cuenta que consume.

Para obtener más información sobre administración de permisos en AWS RAM, consulte Administración de permisos en AWS RAM en la Guía del usuario de AWS Resource Access Manager.

Facturación y medición

No hay cargos adicionales por compartir los orígenes de la VPC con otras Cuentas de AWS. Los costos de uso del tráfico de una distribución que utiliza un origen de la VPC compartido se destinarán a la cuenta consumidora propietaria de la distribución.

Cuotas de recursos compartidos

CloudFront utiliza las mismas cuotas de recursos compartidos que las especificadas por AWS RAM. Desde la consola de CloudFront, puede agregar hasta 5 Cuentas de AWS, 1 OU o 1 organización. Para agregar más, utilice la consola de AWS RAM o la API de AWS RAM.

Para obtener más información, consulte Service Quotas para AWS RAM en la Guía del usuario deAWS RAM.

Almacenamiento en caché y disponibilidad

Puede utilizar CloudFront para reducir la cantidad de solicitudes a las que debe responder directamente el servidor de origen. Con el almacenamiento en caché de CloudFront, se atienden más objetos desde ubicaciones periférica de CloudFront, que están más cerca de los usuarios. Esto reduce la carga en su servidor de origen y reduce la latencia.

Cuantas más solicitudes pueda atender CloudFront desde cachés de borde, menos solicitudes de lector debe reenviar CloudFront al origen para obtener la versión más reciente o una versión única de un objeto. Para optimizar CloudFront y realizar el menor número posible de solicitudes al origen, considere la posibilidad de utilizar CloudFront Origin Shield. Para obtener más información, consulte Uso de Amazon CloudFront Origin Shield.

La proporción de solicitudes que se atienden directamente desde la caché de CloudFront en comparación con todas las solicitudes se denomina tasa de aciertos de caché. Puede consultar el porcentaje de aciertos, fallos y errores de solicitudes de lectores en la consola de CloudFront. Para obtener más información, consulte Visualización de informes estadísticos de la caché de CloudFront.

Hay una serie de factores que afectan a la tasa de aciertos de caché. Puede ajustar la configuración de distribución de CloudFront para mejorar la tasa de aciertos de caché siguiendo las instrucciones de Incremento de la proporción de solicitudes que se atienden directamente desde las cachés de CloudFront (tasa de aciertos de caché).

Para obtener información sobre cómo agregar y eliminar el contenido que desea que CloudFront distribuya, consulte Agregación, eliminación o sustitución de contenido que distribuye CloudFront.

Temas

- Incremento de la proporción de solicitudes que se atienden directamente desde las cachés de CloudFront (tasa de aciertos de caché)
- Uso de Amazon CloudFront Origin Shield
- Optimización de alta disponibilidad con conmutación por error de origen de CloudFront
- Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento)
- Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta
- Almacenamiento en caché de contenido en función de cookies
- Almacenamiento en caché de contenido en función de encabezados de solicitud

Incremento de la proporción de solicitudes que se atienden directamente desde las cachés de CloudFront (tasa de aciertos de caché)

Puede mejorar el rendimiento aumentando la proporción de las solicitudes de lector que se atienden directamente desde la caché de CloudFront en lugar de acceder a los servidores de origen para obtener contenido. Esto se conoce como mejora de la tasa de aciertos de caché.

En las secciones siguientes se explica cómo mejorar la tasa de aciertos de la caché.

Temas

- Especificación de cuánto tiempo CloudFront almacena en caché los objetos
- Uso del escudo de origen
- Almacenamiento en caché en función de parámetros de cadenas de consulta
- Almacenamiento en caché en función de valores de cookies
- Almacenamiento en caché en función de encabezados de solicitud
- Eliminación del encabezado Accept-Encoding cuando no sea necesario comprimir
- Distribución de contenido multimedia a través de HTTP

Especificación de cuánto tiempo CloudFront almacena en caché los objetos

Para incrementar la tasa de aciertos de caché, puede configurar su origen para agregar una directiva Cache-Control max-age a sus objetos y especificar el mayor valor práctico de `max-age`. Cuanto más corta sea la duración de la caché, más frecuentemente reenvía CloudFront las solicitudes al origen para determinar si un objeto ha cambiado y para obtener la versión más reciente. Puede complementar `max-age` con las directivas `stale-while-revalidate` y `stale-if-error` para mejorar aún más la proporción de aciertos de la caché en determinadas condiciones. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Uso del escudo de origen

CloudFront Origin Shield puede contribuir a mejorar la tasa de aciertos de caché de la distribución de CloudFront, porque proporciona una capa adicional de almacenamiento en caché frente al origen. Cuando utiliza Origin Shield, todas las solicitudes de todas las capas de almacenamiento en caché

de CloudFront en el origen provienen de una sola ubicación. CloudFront puede recuperar cada objeto mediante una sola solicitud de origen de Origin Shield y todas las demás capas de la caché de CloudFront (ubicaciones periférica y cachés regionales de borde) pueden recuperar el objeto desde Origin Shield.

Para obtener más información, consulte Uso de Amazon CloudFront Origin Shield.

Almacenamiento en caché en función de parámetros de cadenas de consulta

Si configura CloudFront para almacenar en caché en función de los parámetros de cadenas de consulta, puede mejorar el almacenamiento en la caché si hace lo siguiente:

- Configure CloudFront para reenviar solo los parámetros de cadenas de consulta para los que el origen devolverá objetos únicos.
- Utilice el mismo tipo de letra (mayúscula o minúscula) para todas las instancias del mismo parámetro. Por ejemplo, si una solicitud contiene `parameter1=A` y otra contiene `parameter1=a`, CloudFront reenvía solicitudes independientes al origen cuando una solicitud contiene `parameter1=A` y otra contiene `parameter1=a`. A continuación, CloudFront almacena en caché de forma independiente los objetos correspondientes devueltos por el origen por separado incluso si los objetos son idénticos. Si utiliza solo `A` o `a`, CloudFront reenvía menos solicitudes al origen.
- Enumere los parámetros en el mismo orden. Al igual que con las diferencias de mayúsculas y minúsculas, si una solicitud de un objeto contiene la cadena de consulta `parameter1=a&parameter2=b` y otra solicitud del mismo objeto contiene `parameter2=b&parameter1=a`, CloudFront reenvía ambas solicitudes al origen y almacena en caché los objetos correspondientes de forma independiente aunque sean idénticos. Si ordena los parámetros siempre de la misma manera, CloudFront reenvía menos solicitudes al origen.

Para obtener más información, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta. Si desea revisar las cadenas de consulta que CloudFront reenvía al origen, consulte los valores en la columna `cs-uri-query` de los archivos de registro de CloudFront. Para obtener más información, consulte Registros de acceso (registros estándar).

Almacenamiento en caché en función de valores de cookies

Si configura CloudFront para almacenar en caché en función de los valores de las cookies, puede mejorar el almacenamiento en la caché si hace lo siguiente:

- Configure CloudFront para reenviar solo las cookies especificadas en lugar de todas. Para las cookies que configura que CloudFront reenvíe al origen, CloudFront reenvía cada combinación de nombre y valor de las cookies. A continuación, almacena en caché por separado los objetos que devuelve su origen, incluso si todos son idénticos.

  Supongamos que los espectadores incluyen dos cookies en cada solicitud, que cada cookie tiene tres valores posibles y que todas las combinaciones de valores de cookie son posibles. CloudFront reenvía hasta nueve solicitudes diferentes al origen para cada uno de los objetos. Si el origen devuelve distintas versiones de un objeto en función de solo una de las cookies, CloudFront reenvía más solicitudes al origen de lo necesario y almacena en caché varias versiones idénticas del objeto innecesariamente.
- Cree diferentes comportamientos de la caché para contenido estático y dinámico y configure CloudFront para reenviar las cookies al origen solo para contenido dinámico.

  Por ejemplo, supongamos que tiene un comportamiento de la caché para la distribución y que utiliza la distribución para contenido dinámico, como archivos `.js` y para archivos `.css` que raramente cambian. CloudFront almacena en caché versiones independientes de los archivos `.css` en función de los valores de cookies, de modo que cada ubicación periférica de CloudFront reenvía una solicitud al origen por cada nuevo valor de cookie o por cada combinación de valores de cookies.

  Si crea un comportamiento de la caché cuyo patrón de ruta es `*.css` y para el que CloudFront no almacena en caché en función de los valores de las cookies, CloudFront reenviará las solicitudes de archivos `.css` al origen solo para la primera solicitud que reciba desde una ubicación periférica de un archivo `.css` determinado y para la primera solicitud después de que un archivo `.css` venza.
- Si es posible, cree diferentes comportamientos de la caché para contenido dinámico cuyos valores de cookie sean exclusivos para cada usuario (como un ID de usuario) y para contenido dinámico que varíe en función de una cantidad más reducida de valores únicos.

Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies. Si desea revisar las cookies que CloudFront reenvía al origen, consulte los valores en la columna `cs(Cookie)` de los archivos de registro de CloudFront. Para obtener más información, consulte Registros de acceso (registros estándar).

Almacenamiento en caché en función de encabezados de solicitud

Si configura CloudFront para almacenar en caché en función de encabezados de solicitud, puede mejorar el almacenamiento en la caché si hace lo siguiente:

- Configure CloudFront para reenviar y almacenar en caché solo en función de encabezados especificados en lugar de reenviar y almacenar en caché en función de todos los encabezados. Para los encabezados que especifique, CloudFront reenvía todas las combinaciones de nombre y valor de encabezado. A continuación, almacena en caché por separado los objetos que devuelve su origen, incluso si todos son idénticos.

  > **Note**
  >
  > CloudFront siempre reenvía al origen los encabezados especificados en los siguientes temas:
  >
  > - Cómo CloudFront procesa y reenvía solicitudes al servidor de origen de Amazon S3 > Encabezados de solicitud HTTP que CloudFront elimina o actualiza
  > - Cómo CloudFront procesa y reenvía solicitudes al servidor de origen personalizado > Encabezados de solicitudes HTTP y comportamiento de CloudFront (personalizado y orígenes de Amazon S3)

  Cuando configura CloudFront para almacenar en caché en función de encabezados de solicitud, no cambia los encabezados que reenvía CloudFront, solo si CloudFront almacena en caché objetos en función de los valores de encabezado.

- Intente evitar el almacenamiento en caché en función de encabezados de solicitud con un gran número de valores únicos.

  Por ejemplo, si desea enviar diferentes tamaños de una imagen en función del dispositivo del usuario, no configura CloudFront para almacenar en caché en función del encabezado `User-Agent`, que tiene gran cantidad de valores posibles. En su lugar, configure CloudFront para almacenar en caché en función de los encabezados de tipo de dispositivo de CloudFront `CloudFront-Is-Desktop-Viewer`, `CloudFront-Is-Mobile-Viewer`, `CloudFront-Is-SmartTV-Viewer` y `CloudFront-Is-Tablet-Viewer`. Además, si va a devolver la misma versión de la imagen para tablets y equipos de escritorio, reenvíe solo el encabezado `CloudFront-Is-Tablet-Viewer`, no el `CloudFront-Is-Desktop-Viewer`.

Para obtener más información, consulte Almacenamiento en caché de contenido en función de encabezados de solicitud.

Eliminación del encabezado **`Accept-Encoding`** cuando no sea necesario comprimir

Si la compresión no está habilitada, porque el origen no la admite, CloudFront no la admite o el contenido no es compresible, puede aumentar la tasa de aciertos de caché asociando un comportamiento de caché en la distribución con un origen que establezca Custom Origin Header como se muestra a continuación:

- Nombre del encabezado: `Accept-Encoding`
- Valor de encabezado: (mantener en blanco)

Cuando utiliza esta configuración, CloudFront elimina el encabezado `Accept-Encoding` de la clave de caché y no incluye el encabezado en las solicitudes de origen. Esta configuración se aplica a todo el contenido que CloudFront sirve con la distribución desde ese origen.

Distribución de contenido multimedia a través de HTTP

Para obtener más información acerca de cómo optimizar el contenido de vídeo bajo demanda (VOD) y en streaming, consulte Video bajo demanda y streaming de video en directo con CloudFront.

Uso de Amazon CloudFront Origin Shield

CloudFront Origin Shield es una capa adicional en la infraestructura de almacenamiento en caché de CloudFront que contribuye a minimizar la carga en el origen, mejorar su disponibilidad y reducir los costos de explotación. Con CloudFront Origin Shield, obtendrá los siguientes beneficios:

Mejor tasa de aciertos de caché

Origin Shield puede contribuir a mejorar la tasa de aciertos de caché de su distribución de CloudFront, ya que proporciona una capa adicional de almacenamiento en caché delante del origen. Cuando utiliza Origin Shield, todas las solicitudes de todas las capas de almacenamiento en caché de CloudFront a su origen pasan por Origin Shield, lo que aumenta la probabilidad de que se produzca un acierto de caché. CloudFront puede recuperar cada objeto con una sola solicitud de origen desde Origin Shield al origen, y todas las demás capas de la caché de

CloudFront (ubicaciones de borde y cachés de borde regionales) pueden recuperar el objeto desde Origin Shield.

Carga de origen reducida

El escudo de origen puede reducir aún más el número de solicitudes simultáneas que se envían a su origen para el mismo objeto. Las solicitudes de contenido que no están en la caché del escudo de origen se consolidan con otras solicitudes para el mismo objeto, por lo que solo una solicitud va a su origen. La gestión de menos solicitudes en su origen puede preservar la disponibilidad del origen durante las cargas máximas o picos de tráfico inesperados y puede reducir los costos de cosas como el empaquetado justo a tiempo, las transformaciones de imágenes y la transferencia de datos (DTO).

Mejor rendimiento de red

Cuando se habilita el escudo de origen en la región de AWS que tiene la latencia más baja a su origen, puede obtener un mejor rendimiento de red. Para los orígenes de una región de AWS, el tráfico de red de CloudFront permanece en la red de alto rendimiento de CloudFront hasta el origen. Para los orígenes fuera de AWS, el tráfico de red de CloudFront permanece en la red de CloudFront hasta el escudo de origen, que tiene una conexión de baja latencia con su origen.

Se incurre en cargos adicionales por usar el escudo de origen. Para obtener más información, consulte los precios de CloudFront.

> **Note**
>
> Origin Shield no es compatible con las solicitudes de gRPC. Si una distribución compatible con gRPC tiene Origin Shield activado, las solicitudes de gRPC seguirán funcionando. Sin embargo, las solicitudes se distribuirán directamente al origen de gRPC sin pasar por Origin Shield. Para obtener más información, consulte Uso de gRPC con distribuciones de CloudFront.

Temas

- Casos de uso para el escudo de origen
- Elección de la región de AWS para Origin Shield
- Habilitar Origin Shield
- Estimación de los costos de Origin Shield

- Alta disponibilidad del escudo de origen
- Cómo interactúa Origin Shield con otras características de CloudFront

Casos de uso para el escudo de origen

CloudFront Origin Shield puede ser beneficioso en muchos casos de uso, incluidos los siguientes:

- Los lectores que se distribuyen en diferentes regiones geográficas
- Orígenes que proporcionan empaquetado justo a tiempo para streaming o procesamiento de imágenes sobre la marcha
- Orígenes en las instalaciones con limitaciones de capacidad o de ancho de banda
- Cargas de trabajo que utilizan varias redes de entrega de contenido (CDN)

El escudo de origen puede no ser adecuado en otros casos, como el contenido dinámico que se remite al origen, el contenido con poca capacidad de caché o el contenido que se solicita con poca frecuencia.

En las siguientes secciones se explican los beneficios del escudo de origen para los siguientes casos de uso.

Casos de uso

- Lectores en distintas regiones geográficas
- Varias CDN

Lectores en distintas regiones geográficas

Con Amazon CloudFront, obtiene de forma inherente una carga reducida en su origen porque las solicitudes que CloudFront puede atender desde la caché no van a su origen. Además de la red global de ubicaciones de borde de CloudFront, las cachés regionales de borde sirven como capa de almacenamiento en caché de nivel intermedio para proporcionar aciertos de caché y consolidar solicitudes de origen para los lectores de regiones geográficas cercanas. Las solicitudes de lector se dirigen primero a una ubicación de borde de CloudFront cercana y, si el objeto no está almacenado en caché en esa ubicación, la solicitud se envía a una caché de borde regional.

Cuando los lectores se encuentran en distintas regiones geográficas, las solicitudes se pueden dirigir a través de distintas cachés de borde regionales, cada una de las cuales puede enviar una solicitud

a su origen para el mismo contenido. Pero con el escudo de origen, obtiene una capa adicional de almacenamiento en caché entre las cachés de borde regionales y su origen. Todas las solicitudes de todas las cachés de borde regionales pasan por el escudo de origen, lo que reduce aún más la carga en su origen. Los siguientes diagramas lo ilustran. En los siguientes diagramas, el origen es AWS Elemental MediaPackage.

Sin escudo de origen

Sin escudo de origen, es posible que su origen reciba solicitudes duplicadas para el mismo contenido, como se muestra en el siguiente diagrama.

Con escudo de origen

El uso del escudo de origen puede contribuir a reducir la carga sobre el origen, como se muestra en el siguiente diagrama.

Varias CDN

Para ofrecer eventos de vídeo en directo o contenido popular bajo demanda, puede utilizar varias redes de entrega de contenido (CDN). El uso de varias CDN puede ofrecer ciertos beneficios, pero también significa que su origen puede recibir muchas solicitudes duplicadas para el mismo contenido, cada una proveniente de CDN diferentes o diferentes ubicaciones dentro de la misma CDN. Estas solicitudes redundantes podrían afectar negativamente a la disponibilidad de su origen o conllevar costos operativos adicionales para procesos como el empaquetado justo a tiempo o la transferencia de datos (DTO) a Internet.

Al combinar Origin Shield con el uso de su distribución de CloudFront como origen para otras CDN, puede obtener los siguientes beneficios:

- Menos solicitudes redundantes recibidas en su origen, lo que ayuda a reducir los efectos negativos del uso de varias CDN.
- Una clave de caché común en las CDN y administración centralizada para características orientadas al origen.
- Mejora del rendimiento de la red. El tráfico de red de otras CDN finaliza en una ubicación de borde de CloudFront cercana, lo que podría proporcionar un acierto de la caché local. Si el objeto solicitado no está en la caché de ubicación de borde, la solicitud al origen permanece en la red de

CloudFront hasta Origin Shield, lo que proporciona un alto rendimiento y una baja latencia en el origen. Si el objeto solicitado está en la caché del escudo de origen, la solicitud a su origen se evita por completo.

> **Important**
>
> Si le interesa utilizar el escudo de origen en una arquitectura de CDN múltiples y tiene precios reducidos, contacte con nosotros o con su representante de ventas de AWS para obtener más información. Podrían aplicarse cargos adicionales.

Los siguientes diagramas muestran cómo puede ayudar esta configuración a minimizar la carga en su origen cuando se ofrecen eventos de vídeo en vivo populares con varias CDN. En los siguientes diagramas, el origen es AWS Elemental MediaPackage.

Sin escudo de origen (varias CDN)

Sin el escudo de origen, es posible que su origen reciba muchas solicitudes duplicadas para el mismo contenido, cada una proveniente de una CDN diferente, como se muestra en el siguiente diagrama.

Con escudo de origen (varias CDN)

Usar Origin Shield con CloudFront como origen para las demás CDN puede ayudar a reducir la carga en su origen, como se muestra en el siguiente diagrama.

Elección de la región de AWS para Origin Shield

Amazon CloudFront ofrece el escudo de origen en las regiones de AWS en las que CloudFront tiene una caché de borde regional. Al activar el escudo de origen, elija la región de AWS para el Escudo de origen. Debe elegir la región de AWS que tenga la latencia más baja a su origen. Puede utilizar el escudo de origen con orígenes que se encuentren en una región de AWS y con orígenes que no estén en AWS.

Para los orígenes de una región de AWS

Si su origen se encuentra en una región de AWS, determine primero si este se encuentra en una región en la que CloudFront ofrece el escudo de origen. CloudFront ofrece el escudo de origen en las siguientes regiones de AWS.

- EE. UU. Este (Ohio) – `us-east-2`
- EE.UU. Este (Norte de Virginia) – `us-east-1`
- EE.UU. Oeste (Oregón) – `us-west-2`
- Asia-Pacífico (Bombay) – `ap-south-1`
- Asia-Pacífico (Seúl) – (`ap-northeast-2`)
- Asia Pacífico (Singapur) – `ap-southeast-1`
- Asia-Pacífico (Sídney) – `ap-southeast-2`
- Asia-Pacífico (Tokio) – `ap-northeast-1`

- Europa (Fráncfort) – `eu-central-1`
- Europa (Irlanda) – `eu-west-1`
- Europa (Londres) – `eu-west-2`
- América del Sur (São Paulo) – `sa-east-1`
- Medio Oriente (EAU) – `me-central-1`

Si su origen se encuentra en una región de AWS en la que CloudFront ofrece el escudo de origen

Si el origen se encuentra en una región de AWS en la que CloudFront ofrece el escudo de origen (véase la lista anterior), habilite el escudo de origen en la misma región que el origen.

Si el origen no se encuentra en una región de AWS en la que CloudFront ofrece el escudo de origen

Si el origen no se encuentra en una región de AWS en la que CloudFront ofrece el escudo de origen, consulte la siguiente tabla para determinar en qué región debe habilitarlo.

Si su origen está en ...	Habilite el escudo de origen en ...
EE.UU. Oeste (Norte de California) – `us-west-1`	EE.UU. Oeste (Oregón) – `us-west-2`
África (Ciudad del Cab) – `af-south-1`	Europa (Irlanda) – `eu-west-1`
Asia-Pacífico (Hong Kon) – `ap-east-1`	Asia Pacífico (Singapur) – `ap-southeast-1`
Canadá (Centra) – `ca-central-1`	EE.UU. Este (Norte de Virginia) – `us-east-1`
Europa (Milá) – `eu-south-1`	UE (Fráncfort) – `eu-central-1`
Europa (Parí) – `eu-west-3`	UE (Londres) – `eu-west-2`
Europa (Estocolm) – `eu-north-1`	UE (Londres) – `eu-west-2`
Medio Oriente (Baréi) – `me-south-1`	Asia-Pacífico (Mumbai) – `ap-south-1`

Para orígenes fuera de AWS

Puede utilizar el escudo de origen con un origen en las instalaciones o que no esté en una región de AWS. En este caso, habilite el escudo de origen en la región de AWS que tenga la latencia más baja

para su origen. Si no está seguro de qué región de AWS tiene la latencia más baja para su origen, puede utilizar las siguientes sugerencias para ayudarle a tomar una decisión.

- Puede consultar la tabla anterior para obtener una aproximación de la región de AWS que podría tener la menor latencia para su origen, en función de la ubicación geográfica de su origen.
- Puede lanzar instancias Amazon EC2 en diferentes regiones de AWS que estén geográficamente próximas a su origen y ejecutar algunas pruebas utilizando `ping` para medir las latencias de red típicas entre esas regiones y el origen.

Habilitar Origin Shield

Puede habilitar el escudo de origen para mejorar su tasa de aciertos de caché, reducir la carga en el origen y ayudar a mejorar el rendimiento. Para habilitar Origin Shield, cambie la configuración de origen de una distribución de CloudFront. El escudo de origen es una propiedad del origen. Para cada origen de sus distribuciones de CloudFront, puede habilitar el escudo de origen por separado en cualquier región de AWS que ofrezca el mejor rendimiento para dicho origen.

Puede habilitar Origin Shield en la consola de CloudFront, con CloudFormation, o con la API de CloudFront.

Console

Para habilitar el escudo de origen para un origen existente (consola)

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la distribución que tiene el origen que desea actualizar.
3. Elija la pestaña Orígenes.
4. Elija el origen que desea actualizar y, a continuación, seleccione Edit (Editar).
5. En Enable Origin Shield (Activar escudo de origen), elija Yes (Sí).
6. En Origin Shield Region (Región de escudo de origen), elija la región de AWS donde desea activar el escudo de origen. Para obtener ayuda para elegir una región, consulte Elección de la región de AWS para Origin Shield.
7. Seleccione Save changes (Guardar cambios).

Cuando el estado de distribución esté Deployed (Implementado), el escudo de origen estará listo. Esto lleva unos minutos.

Para habilitar el escudo de origen para un nuevo origen (consola)

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Para crear el nuevo origen en una distribución existente, haga lo siguiente:

   1. Elija la distribución en la que desea crear el origen.
   2. Elija Create Origin (Crear origen), y, a continuación, continúe con el paso 3.

   Para crear el nuevo origen en una nueva distribución estándar, haga lo siguiente:

   1. Siga estos pasos para crear una distribución estándar en la consola. Para obtener más información, consulte Creación de una distribución de CloudFront en la consola.
   2. En la sección Configuración, elija Personalizar configuración de origen. Continúe con el paso 3.
3. En Enable Origin Shield (Activar escudo de origen), elija Yes (Sí).
4. En Origin Shield Region (Región de escudo de origen), elija la región de AWS donde desea activar el escudo de origen. Para obtener ayuda para elegir una región, consulte Elección de la región de AWS para Origin Shield.
5. Siga los pasos de la consola para terminar de crear el origen o la distribución.

Cuando el estado de distribución esté Deployed (Implementado), el escudo de origen estará listo. Esto lleva unos minutos.

CloudFormation

Para habilitar el escudo de origen con CloudFormation, utilice la propiedad `OriginShield` en el tipo de propiedad `Origin` en un recurso `AWS::CloudFront::Distribution`. Puede agregar la propiedad `OriginShield` a un `Origin` existente o incluirla al crear un nuevo `Origin`.

En el siguiente ejemplo se muestra la sintaxis, en formato YAML, para habilitar `OriginShield` en la región EE. UU. Oeste (Oregón) (`us-west-2`). Para obtener ayuda para elegir una región, consulte the section called “Elección de la región de AWS para Origin Shield”.
En este ejemplo se muestra solo el tipo de propiedad `Origin`, no todo el recurso `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
```

Para obtener más información, consulte AWS::CloudFront::Distribution Origin en la sección de referencia de recursos y propiedades de la Guía del usuario de AWS CloudFormation.

API

Para habilitar el escudo de origen con la API de CloudFront mediante los SDK de AWS o la AWS Command Line Interface (AWS CLI), utilice el tipo `OriginShield`. Se especifica `OriginShield` en un `Origin`, en una `DistributionConfig`. Para obtener información sobre el tipo `OriginShield`, consulte la siguiente información en la Referencia de la API de Amazon CloudFront.

- OriginShield (tipo)
- Origin (tipo)
- DistributionConfig (tipo)
- UpdateDistribution (operación)
- CreateDistribution (operación)

La sintaxis específica para usar estos tipos y operaciones varía en función del SDK, de la CLI o cliente de API. Para obtener más información, consulte la documentación de referencia de su SDK, CLI o cliente.

Estimación de los costos de Origin Shield

Se acumulan cargos por escudo de origen en función del número de solicitudes que van al escudo de origen como capa incremental.

Para las solicitudes dinámicas (no almacenables en caché) que se envían como proxy al origen, el escudo de origen es siempre una capa incremental. Las solicitudes dinámicas utilizan los métodos HTTP `PUT`, `POST`, `PATCH` y `DELETE`.

Las solicitudes `GET` y `HEAD` que tienen una configuración de tiempo de vida (TTL) inferior a 3600 segundos se consideran solicitudes dinámicas. Además, las solicitudes `GET` y `HEAD` que deshabilitan el almacenamiento en caché también se consideran solicitudes dinámicas.

Para calcular los cargos del escudo de origen para solicitudes dinámicas, utilice la siguiente fórmula:

Número total de solicitudes dinámicas x cargo de escudo de origen por 10 000 solicitudes / 10 000

Para las solicitudes no dinámicas con los métodos HTTP `GET`, `HEAD` y `OPTIONS`, Origin Shield es a veces una capa incremental. Al activar Origin Shield, elija la región de Región de AWS para esa función. Para las solicitudes que van naturalmente a la memoria caché periférica regional en la misma región que Origin Shield, no se trata de una capa incremental. No acumula cargos de Origin Shield por estas solicitudes. En el caso de las solicitudes que van a una memoria caché periférica regional en una región diferente de Origin Shield y, a continuación, van a Origin Shield, sí es una capa incremental. Se acumulan cargos del escudo de origen por estas solicitudes.

Para calcular los cargos del escudo de origen para solicitudes que se pueden almacenar en caché, utilice la siguiente fórmula:

Número total de solicitudes que se pueden almacenar en caché x (1: tasa de aciertos de caché) x porcentaje de solicitudes que van a Origin Shield desde una caché de borde regional en una región diferente x cargo de Origin Shield por 10 000 solicitudes / 10 000

Para obtener más información sobre el cargo por cada 10 000 solicitudes de Origin Shield, consulte Precios de CloudFront.

Alta disponibilidad del escudo de origen

Origin Shield utiliza la característica de memorias cachés periféricas regionales de CloudFront. Cada una de estas cachés de borde se crea en una región de AWS usando al menos tres zonas de disponibilidad con flotas de instancias Amazon EC2 de escalado automático. Las conexiones originadas en las ubicaciones de CloudFront hacia Origin Shield también usan el seguimiento activo de errores en cada solicitud para direccionar automáticamente la solicitud a una ubicación de Origin Shield secundaria si la principal no está disponible.

Cómo interactúa Origin Shield con otras características de CloudFront

En las secciones siguientes se explica cómo interactúa Origin Shield con otras características de CloudFront.

Registro de Origin Shield y CloudFront

Para ver cuándo ha gestionado una solicitud el escudo de origen, debe habilitar una de las siguientes opciones:

- Registros estándar de CloudFront (registros de acceso). Los registros estándar se proporcionan de forma gratuita.
- Registros de acceso en tiempo real de CloudFront. Se incurre en cargos adicionales por el uso de registros de acceso en tiempo real. Consulte Precios de Amazon CloudFront.

Los aciertos de caché de Origin Shield se muestran como `OriginShieldHit` en el campo `x-edge-detailed-result-type` de los registros de CloudFront. Origin Shield utiliza las cachés regionales de borde de Amazon CloudFront. Si una solicitud se dirige desde una ubicación de borde de CloudFront a la caché de borde regional que actúa como Origin Shield, se notifica como un `Hit` en los registros, no como un `OriginShieldHit`.

Escudo de origen y grupos de origen

Origin Shield es compatible con los grupos de orígenes de CloudFront. Dado que el escudo de origen es una propiedad del origen, las solicitudes siempre viajan a través del escudo de origen para cada origen, incluso cuando el origen forma parte de un grupo de origen. Para una solicitud determinada, CloudFront dirige la solicitud al origen principal en el grupo de origen a través de la instancia de Origin Shield del origen principal. Si esa solicitud devuelve un error (según los criterios de conmutación por error del grupo de orígenes), CloudFront dirige la solicitud al origen secundario a través de la instancia de Origin Shield del origen secundario.

Escudo de origen y Lambda@Edge

El escudo de origen no afecta a la funcionalidad de las funciones de Lambda @Edge pero puede afectar a la región de AWS donde se ejecutan esas funciones.

Cuando utiliza el escudo de origen con Lambda @Edge, los desencadenadores orientados al origen (solicitud de origen y respuesta de origen) se ejecutan en la región de AWS donde está habilitado el

escudo de origen. Si la ubicación de Origin Shield principal no está disponible y CloudFront enruta las solicitudes a una ubicación de Origin Shield secundaria, los desencadenadores orientados al origen de Lambda@Edge también cambiarán para utilizar la ubicación de Origin Shield secundaria.

Los desencadenadores orientados al lector no se ven afectados.

Optimización de alta disponibilidad con conmutación por error de origen de CloudFront

Puede configurar CloudFront con conmutación por error de origen en los casos en los que se requiera alta disponibilidad. Para empezar, cree un grupo de origen con dos orígenes: uno primario y otro secundario. Si el origen principal no está disponible o devuelve códigos de estado de respuesta HTTP específicos que indican un error, CloudFront cambia automáticamente al origen secundario.

Para configurar la conmutación por error de origen, debe tener una distribución con al menos dos orígenes. A continuación, cree un grupo de origen para su distribución que incluya dos orígenes, configurando uno como principal. Por último, cree o actualice un comportamiento de caché para utilizar el grupo de origen.

Para consultar los pasos para configurar grupos de origen y configurar opciones de conmutación por error de origen específicas, consulte Creación de un grupo de origen.

Después de configurar la conmutación por error de origen para un comportamiento de la caché, CloudFront hace lo siguiente para las solicitudes del lector:

- Cuando hay un acierto de caché, CloudFront devuelve el objeto solicitado.
- Cuando hay un error de caché, CloudFront dirige la solicitud al origen principal en el grupo de origen.
- Cuando el origen principal devuelve un código de estado que no está configurado para conmutación por error, como un código de estado HTTP 2xx o 3xx, CloudFront envía el objeto solicitado al lector.
- Cuando se produce cualquiera de las siguientes situaciones:
  - El origen principal devuelve un código de estado HTTP que ha configurado para la conmutación por error
  - CloudFront no se conecta al origen principal (cuando se establece 503 como código de conmutación por error)

- La respuesta del origen principal tarda demasiado (se agota el tiempo de espera) (cuando se establece 504 como código de conmutación por error)

A continuación, CloudFront dirige la solicitud al origen secundario del grupo de origen.

> **Note**
>
> En algunos casos de uso, como el streaming de contenido de vídeo, es posible que CloudFront conmute por error rápidamente al origen secundario. Para ajustar la rapidez con la que CloudFront conmuta por error al origen secundario, consulte Control de tiempos de espera e intentos de origen.

CloudFront dirige todas las solicitudes entrantes al origen principal, incluso cuando una solicitud anterior ha conmutado por error al origen secundario. CloudFront solo envía solicitudes al origen secundario después de que se produzca un error en una solicitud al origen principal.

CloudFront conmuta por error al origen secundario solo cuando el método HTTP de la solicitud del lector es `GET`, `HEAD` u `OPTIONS`. CloudFront no realiza una conmutación por error cuando el lector envía un método HTTP diferente (por ejemplo `POST`, `PUT`, etc.).

El siguiente diagrama ilustra el funcionamiento de la conmutación por error de origen.

Temas

- Creación de un grupo de origen
- Control de tiempos de espera e intentos de origen
- Utilizar la conmutación por error de origen con funciones de Lambda@Edge
- Utilizar páginas de error personalizadas con conmutación por error de origen

Creación de un grupo de origen

Para crear un grupo de origen

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la distribución para la que desea crear el grupo de origen.
3. Elija la pestaña Orígenes.
4. Asegúrese de que la distribución tenga más de un origen. Si no lo tiene, agregue un segundo origen.
5. En la pestaña Origins (Orígenes), en el panel Origin Groups (Grupos de origen), elija Create origin group (Crear grupo de origen).
6. Elija los orígenes del grupo de origen. Después de agregar orígenes, utilice las flechas para establecer la prioridad, es decir, qué origen es primario y cuál secundario.
7. Ingrese un nombre para el grupo de origen.
8. Elija los códigos de estado HTTP que desea utilizar como criterios de conmutación por error. Puede elegir cualquier combinación de los siguientes códigos de estado: 400, 403, 404, 416, 500, 502, 503 o 504. Cuando CloudFront recibe una respuesta con uno de los códigos de estado especificados, conmuta por error al origen secundario.

   > **Note**
   >
   > CloudFront conmuta por error al origen secundario solo cuando el método HTTP de la solicitud del lector es `GET`, `HEAD` u `OPTIONS`. CloudFront no realiza una conmutación por error cuando el lector envía un método HTTP diferente (por ejemplo `POST`, `PUT`, etc.).

9. En Criterios de selección de origen, especifique cómo se seleccionan sus orígenes cuando lo solicite el espectador de rutas de distribución. Puede elegir las opciones siguientes.

Predeterminado/a

CloudFront utilizará la prioridad de origen predeterminada que especifique en la página Configuración.

Puntuación de calidad multimedia

CloudFront rastrea y usa esta puntuación para determinar el primer origen al que reenviar la solicitud. Esto también autoriza a CloudFront a realizar solicitudes `HEAD` asincrónicas al origen alternativo del grupo de origen para determinar su nivel de calidad multimedia. Solo puede elegir esta opción para los orígenes v2 de AWS Elemental MediaPackage. Para obtener más información, consulte Resiliencia basada en la calidad multimedia.

10. Elija Create origin group (Crear grupo de origen).

Asegúrese de asignar su grupo de origen como el origen del comportamiento de caché de la distribución. Para obtener más información, consulte Nombre.

Control de tiempos de espera e intentos de origen

De forma predeterminada, CloudFront intenta conectarse al origen primario de un grupo de orígenes durante 30 segundos (3 intentos de conexión de 10 segundos cada uno) antes de conmutar por error al origen secundario. En algunos casos de uso, como el streaming de contenido de vídeo, es posible que desee que CloudFront conmute por error más rápidamente al origen secundario. Puede ajustar la siguiente configuración para que afecte a la rapidez con la que CloudFront conmuta por error al origen secundario. Si el origen es un origen secundario o un origen que no forma parte de un grupo de orígenes, esta configuración afecta a la rapidez con la que CloudFront devuelve una respuesta HTTP 504 al lector.

Para conmutar por error más rápidamente, especifique un tiempo de espera de conexión más breve, menos intentos de conexión o ambas opciones. Para orígenes personalizados (incluidos los orígenes de bucket de Amazon S3 configurados con alojamiento de sitio web estático), también puede ajustar el tiempo de espera de respuesta de origen.

Tiempo de espera de conexión de origen

La configuración de tiempo de espera de conexión de origen afecta al tiempo que CloudFront espera al intentar establecer una conexión con el origen. De forma predeterminada, CloudFront espera 10 segundos para establecer una conexión, pero puede especificar de 1 a 10 segundos (inclusive). Para obtener más información, consulte Tiempo de espera de conexión.

Intentos de conexión de origen

La configuración de intentos de conexión de origen afecta al número de veces que CloudFront intenta conectarse al origen. De forma predeterminada, CloudFront intenta conectarse 3 veces, pero puede especificar de 1 a 3 (inclusive). Para obtener más información, consulte Intentos de conexión.

Para un origen personalizado (incluido un bucket de Amazon S3 configurado con alojamiento de sitios web estático), esta configuración también afecta al número de veces que CloudFront intenta obtener una respuesta del origen en el caso de un tiempo de espera de respuesta del origen.

Tiempo de espera de respuesta de origen

El tiempo de espera de respuesta del origen, también conocido como tiempo de espera de lectura del origen, afecta al tiempo que CloudFront espera para recibir una respuesta (o para recibir la respuesta completa) del origen. De forma predeterminada, CloudFront espera 30 segundos, pero puede especificar de 1 a 120 segundos (ambos inclusive). Para obtener más información, consulte Tiempo de espera de respuesta.

Cómo cambiar esta configuración

Para cambiar esta configuración en la consola de CloudFront

- Para un nuevo origen o una nueva distribución, especifique estos valores al crear el recurso.
- En el caso de un origen existente en una distribución existente, debe especificar estos valores al editar el origen.

Para obtener más información, consulte Referencia de toda la configuración de distribución.

Utilizar la conmutación por error de origen con funciones de Lambda@Edge

Puede utilizar las funciones Lambda@Edge con distribuciones de CloudFront que haya configurado con grupos de origen. Para utilizar una función Lambda, especifíquela en una solicitud de origen o un desencadenador de respuesta de origen para un grupo de origen al crear el comportamiento de la caché. Cuando se utiliza una función Lambda@Edge con un grupo de origen, la función se puede activar dos veces para una sola solicitud de visor. Por ejemplo, considere esta situación:

1. Se crea una función Lambda@Edge con un desencadenador de solicitud de origen.

2. La función Lambda se desencadena una vez cuando CloudFront envía una solicitud al origen principal (en un error de caché).
3. El origen principal responde con un código de estado HTTP configurado para la conmutación por error.
4. La función Lambda se desencadena de nuevo cuando CloudFront envía la misma solicitud al origen secundario.

El siguiente diagrama ilustra cómo funciona la conmutación por error de origen cuando se incluye una función de Lambda@Edge en una solicitud de origen o desencadenador de respuesta.

Para obtener más información sobre el uso de desencadenadores de Lambda@Edge, consulte the section called “Adición de desencadenadores para una función de Lambda@Edge”.

Para obtener más información sobre la administración de la conmutación por error de DNS, consulte Configuring DNS failover en la Guía para desarrolladores de Amazon Route 53.

Utilizar páginas de error personalizadas con conmutación por error de origen

Puede utilizar páginas de error personalizadas con grupos de origen de forma similar a cómo utilizarlos con orígenes que no están configuradas para la conmutación por error de origen.

Cuando se utiliza la conmutación por error de origen, puede configurar CloudFront para que devuelva una página de error personalizada para el origen principal o secundario (o ambos):

- Devolver una página de error personalizada para el origen principal: si el origen principal devuelve un código de estado HTTP que no está configurado para la conmutación por error, CloudFront devuelve la página de error personalizada a los lectores.
- Devolver una página de error personalizada para el origen secundario: si CloudFront recibe un código de estado de error del origen secundario, CloudFront devuelve la página de error personalizada.

Para obtener más información acerca del uso de páginas de error personalizadas con CloudFront, consulte Generación de respuestas de error personalizadas.

Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento)

Puede controlar cuánto tiempo se mantienen los archivos en una caché de CloudFront antes de que CloudFront reenvíe otra solicitud al origen. Reducir la duración le permite ofrecer contenido dinámico. Aumentar la duración implica que sus usuarios podrán disfrutar de un mejor rendimiento ya que es más probable que sus archivos se ofrezcan directamente desde la caché perimetral. Una mayor duración también reduce la carga en el origen.

Normalmente, CloudFront ofrece un archivo desde una ubicación periférica durante el tiempo de almacenamiento en caché especificado por usted, es decir, hasta que el archivo venza. Después de que venza, la próxima vez que la ubicación periférica reciba una solicitud de un archivo, CloudFront reenviará la solicitud al servidor de origen para comprobar que la caché contiene la versión más reciente del archivo. La respuesta del origen depende de si el archivo ha cambiado:

- Si la caché de CloudFront ya tiene la versión más reciente, el origen devuelve un código de estado `304 Not Modified`.
- Si la caché de CloudFront no tiene la versión más reciente, el origen devuelve un código de estado `200 OK` y la versión más reciente del archivo.

Si un archivo de una ubicación periférica no se solicita con frecuencia, es posible que CloudFront lo desaloje (lo elimine antes de su fecha de vencimiento) con el fin de dejar espacio para otros archivos que se hayan solicitado más recientemente.

Le recomendamos que actualice la política de caché de su distribución para administrar la duración de la caché. Si opta por no utilizar una política de caché, el TTL (período de vida) predeterminado es de 24 horas, pero puede actualizar la siguiente configuración para anular el predeterminado:

- Para cambiar la duración del almacenamiento en caché de todos los archivos que coinciden con el mismo patrón de ruta, puede cambiar la configuración de CloudFront para Minimum TTL (TTL mínimo), Maximum TTL (TTL máximo) y Default TTL (TTL predeterminado) de un comportamiento de la caché. Para obtener información sobre las opciones de configuración individuales, consulte Tiempo de vida mínimo, Tiempo de vida máximo y Tiempo de vida (TTL) predeterminado.
- Para cambiar la duración del almacenamiento en caché de un archivo individual, puede configurar el origen para agregar un encabezado `Cache-Control` con la política `max-age` o `s-maxage`, o un campo de encabezado `Expires` en el archivo. Para obtener más información, consulte Uso de encabezados para controlar la duración del almacenamiento en caché de objetos individuales.

Para obtener más información acerca de cómo Minimum TTL (TTL mínimo), Default TTL (TTL predeterminado) y Maximum TTL (TTL máximo) interactúan con las políticas `max-age` y `s-maxage` y con el campo de encabezado `Expires`, consulte the section called “Especificación de cuánto tiempo CloudFront almacena objetos en caché”.

También puede controlar durante cuánto tiempo los errores (como `404 Not Found`) permanecen en una caché de CloudFront antes de que CloudFront intente obtener de nuevo el objeto solicitado reenviando otra solicitud al origen. Para obtener más información, consulte the section called “Procesamiento de CloudFront de los códigos de estado HTTP 4xx y 5xx desde el origen”.

Temas

- Uso de encabezados para controlar la duración del almacenamiento en caché de objetos individuales
- Distribución de contenido obsoleto (caducado)
- Especificación de cuánto tiempo CloudFront almacena objetos en caché
- Agregación de encabezados a los objetos con la consola de Amazon S3

Uso de encabezados para controlar la duración del almacenamiento en caché de objetos individuales

Puede utilizar los encabezados `Cache-Control` y `Expires` para controlar durante cuánto tiempo permanecen los objetos en la caché. La configuración de Minimum TTL (Tiempo de vida mínimo),

Default TTL (Tiempo de vida predeterminado) y Maximum TTL (Tiempo de vida máximo) también afecta la duración del almacenamiento en caché, pero a continuación encontrará información general acerca de cómo los encabezados pueden influir en la duración de la caché:

- La política `Cache-Control max-age` le permite especificar durante cuánto tiempo (en segundos) desea que un objeto permanezca en la caché antes de que CloudFront obtenga el objeto de nuevo del servidor de origen. El tiempo mínimo de caducidad compatible con CloudFront es de 0 segundos. El valor máximo es 100 años. Especifique el valor en el siguiente formato:

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

  Por ejemplo, la siguiente política indica a CloudFront que debe mantener el objeto asociado en la caché durante 3600 segundos (una hora):

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

  Si desea que los objetos permanezcan en las cachés de borde de CloudFront por un tiempo distinto del que permanecen en las cachés de navegadores, puede utilizar las políticas `Cache-Control max-age` y `Cache-Control s-maxage` de forma conjunta. Para obtener más información, consulte Especificación de cuánto tiempo CloudFront almacena objetos en caché.
- El campo del encabezado `Expires` le permite especificar una fecha y hora de vencimiento con el formato indicado en RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1 Section 3.3.1, Full Date, por ejemplo:

  ```
  Sat, 27 Jun 2015 23:59:59 GMT
  ```

Le recomendamos que utilice la directiva `Cache-Control max-age` en lugar del campo de encabezado `Expires` para controlar el almacenamiento de objetos en caché. Si especifica valores para `Cache-Control max-age` y para `Expires`, CloudFront utiliza solo el valor de `Cache-Control max-age`.

Para obtener más información, consulte Especificación de cuánto tiempo CloudFront almacena objetos en caché.

No puede utilizar los campos de encabezado HTTP `Cache-Control` ni `Pragma` en una solicitud `GET` de un lector para obligar a CloudFront a volver al servidor de origen para obtener el objeto. CloudFront ignora los campos de encabezado de las solicitudes de los lectores.

Para obtener más información acerca de los campos de encabezado `Cache-Control` y `Expires`, visite las siguientes secciones de RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1:

- Section 14.9 Cache Control
- Section 14.21 Expires

Distribución de contenido obsoleto (caducado)

CloudFront admite las directivas de control de la caché `Stale-While-Revalidate` y `Stale-If-Error`. Puede usar estas directivas para especificar durante cuánto tiempo estará disponible el contenido obsoleto para los lectores.

Temas

- Stale-While-Revalidate
- Stale-If-Error
- Uso de ambas directivas

`Stale-While-Revalidate`

Esta directiva permite a CloudFront distribuir contenido obsoleto desde la caché mientras CloudFront obtiene de forma asíncrona una versión nueva del origen. Esto mejora la latencia, ya que los lectores reciben respuestas inmediatamente desde las ubicaciones periféricas sin tener que esperar a la recuperación en segundo plano. El contenido nuevo se carga en segundo plano para futuras solicitudes.

Example Ejemplo: **`Stale-While-Revalidate`**

CloudFront hace lo siguiente al configurar el encabezado `Cache-Control` para que utilice estas directivas.

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

1. CloudFront almacenará en caché una respuesta durante una hora (`max-age=3600`).
2. Si se realiza una solicitud después de este tiempo, CloudFront distribuye el contenido obsoleto y, al mismo tiempo, envía una solicitud al origen para revalidar y actualizar el contenido almacenado en caché.

3. Mientras el contenido se vuelve a validar, CloudFront distribuye el contenido obsoleto durante un máximo de 10 minutos (`stale-while-revalidate=600`).

> **Note**
>
> CloudFront distribuirá el contenido obsoleto hasta el valor de la directiva `stale-while-revalidate` o el valor del TTL máximo de CloudFront, el valor que sea menor. Una vez transcurrida la duración máxima de TTL, el objeto obsoleto no estará disponible en la caché perimetral, independientemente del valor `stale-while-revalidate`.

`Stale-If-Error`

Esta directiva permite a CloudFront distribuir contenido obsoleto desde la memoria caché si no se puede acceder al origen o devuelve el código de error que está entre 500 y 600. Esto garantiza que los espectadores puedan acceder al contenido incluso durante una interrupción del origen.

Example Ejemplo: **`Stale-If-Error`**

CloudFront hace lo siguiente al configurar el encabezado `Cache-Control` para que utilice estas directivas.

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

1. CloudFront almacena en caché la respuesta durante una hora (`max-age=3600`).
2. Si el origen no funciona o devuelve un error después de este tiempo, CloudFront seguirá distribuyendo el contenido obsoleto durante un máximo de 24 horas (`stale-if-error=86400`)
3. Si configuró respuestas de error personalizadas, CloudFront intentará distribuir el contenido obsoleto si se encuentra un error dentro de la duración de `stale-if-error` especificada.
   Si el contenido obsoleto no está disponible, CloudFront distribuirá las respuestas de error personalizadas configuradas para el código de estado del error correspondiente. Para obtener más información, consulte Generación de respuestas de error personalizadas.

Notas

- CloudFront distribuirá el contenido obsoleto hasta el valor de la directiva `stale-if-error` o el valor del TTL máximo de CloudFront, el valor que sea menor. Una vez transcurrida la duración máxima de TTL, el objeto obsoleto no estará disponible en la caché perimetral, independientemente del valor `stale-if-error`.
- Si no configura `stale-if-error` ni respuestas de error personalizadas, CloudFront devolverá el objeto obsoleto o reenviará la respuesta de error al lector, en función de si el objeto solicitado está en la caché perimetral o no. Para obtener más información, consulte Cómo CloudFront procesa los errores si no ha configurado las páginas de error personalizadas.

Uso de ambas directivas

`stale-while-revalidate` y `stale-if-error` son directivas de control de caché independientes que se pueden usar juntas para reducir la latencia y agregar un búfer para que el origen responda o se recupere.

Example Ejemplo: Uso de ambas directivas

CloudFront hace lo siguiente al configurar el encabezado `Cache-Control` para que utilice las siguientes directivas.

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

1. CloudFront almacena en caché la respuesta durante una hora (`max-age=3600`).
2. Si se realiza una solicitud después de este tiempo, CloudFront distribuye el contenido obsoleto durante un máximo de 10 minutos (`stale-while-revalidate=600`) mientras se vuelve a validar el contenido.
3. Si el servidor de origen devuelve un error mientras CloudFront intenta revalidar el contenido, CloudFront seguirá distribuyendo el contenido obsoleto durante un máximo de 24 horas (`stale-if-error=86400`).

El almacenamiento en caché es un equilibrio entre rendimiento y actualización. El uso de directivas como `stale-while-revalidate` y `stale-if-error` puede mejorar el rendimiento y la experiencia del usuario, pero asegúrese de que las configuraciones se ajusten a la actualización que

desea que tenga el contenido. Las directivas de contenido obsoletas son las más adecuadas para casos de uso en los que es necesario actualizar el contenido, pero no es esencial tener la versión más reciente. Además, si el contenido no cambia o cambia con poca frecuencia, `stale-while-revalidate` podría agregar solicitudes de red innecesarias. En su lugar, considere establecer una duración de caché larga.

Especificación de cuánto tiempo CloudFront almacena objetos en caché

Para controlar la cantidad de tiempo que CloudFront mantiene un objeto en la caché antes de enviar otra solicitud al origen, puede:

- Establecer los valores TTL mínimo, máximo y predeterminado en el comportamiento de la caché de una distribución de CloudFront. Puede establecer estos valores en una política de caché adjunta al comportamiento de caché (recomendado) o en la configuración de caché heredada.
- Incluya el encabezado `Cache-Control` o `Expires` en las respuestas del origen. Estos encabezados también ayudan a determinar cuánto tiempo un explorador mantiene un objeto en la caché del explorador antes de enviar otra solicitud a CloudFront.

En la tabla siguiente se explica cómo los encabezados `Cache-Control` y `Expires` enviados desde el origen funcionan junto con la configuración TTL en un comportamiento de caché para afectar al almacenamiento en caché.

Encabezados de origen	Tiempo de vida mínimo = 0	Tiempo de vida mínimo > 0
El origen agrega una directiva de **`Cache-Control: max-age`** al objeto	Almacenamiento en caché de CloudFront CloudFront almacena en caché el objeto para el menor valor de la directiva `Cache-Control: max-age` o el valor de TTL máximo de CloudFront. Almacenamiento en caché de navegadores	Almacenamiento en caché de CloudFront El almacenamiento en caché de CloudFront depende de los valores del TTL mínimo y TTL máximo de CloudFront y de la directiva `Cache-Control max-age`: • Si TTL mínimo < `max-age` < TTL máximo, CloudFron

Encabezados de origen	Tiempo de vida mínimo = 0	Tiempo de vida mínimo > 0
	Los navegadores almacenan en caché el objeto para el valor de la directiva `Cache-Control: max-age` .	t almacena en caché el objeto para el valor de la directiva `Cache-Control: max-age` . • Si `max-age` < TTL mínimo, CloudFront almacena en caché el objeto para el valor del TTL mínimo de CloudFront. • Si `max-age` > TTL máximo, CloudFront almacena en caché el objeto para el valor del TTL máximo de CloudFront. Almacenamiento en caché de navegadores Los navegadores almacenan en caché el objeto para el valor de la directiva `Cache-Control: max-age` .

Encabezados de origen	Tiempo de vida mínimo = 0	Tiempo de vida mínimo > 0
El origen no agrega una directiva **`Cache-Control: max-age`** al objeto	Almacenamiento en caché de CloudFront CloudFront almacena en caché el objeto para el valor del TTL predeterminado de CloudFront. Almacenamiento en caché de navegadores Depende del navegador.	Almacenamiento en caché de CloudFront CloudFront almacena en caché el objeto para el mayor valor del TTL mínimo de CloudFront o TTL predeterm inado. Almacenamiento en caché de navegadores Depende del navegador.

Encabezados de origen	Tiempo de vida mínimo = 0	Tiempo de vida mínimo > 0
El origen agrega directivas **`Cache-Control: max-age`** y **`Cache-Control: s-maxage`** al objeto	Almacenamiento en caché de CloudFront CloudFront almacena en caché el objeto para el menor valor de la directiva `Cache-Control: s-maxage` o el valor de TTL máximo de CloudFront. Almacenamiento en caché de navegadores Los navegadores almacenan en caché el objeto para el valor de la directiva `Cache-Control max-age` .	Almacenamiento en caché de CloudFront El almacenamiento en caché de CloudFront depende de los valores del TTL mínimo y TTL máximo de CloudFront y de la directiva `Cache-Control: s-maxage`: • Si TTL mínimo < `s-maxage` < TTL máximo, CloudFront almacena en caché el objeto para el valor de la directiva `Cache-Control: s-maxage` . • Si `s-maxage` < TTL mínimo, CloudFront almacena en caché el objeto para el valor del TTL mínimo de CloudFront. • Si `s-maxage` > TTL máximo, CloudFront almacena en caché el objeto para el valor del TTL máximo de CloudFront. Almacenamiento en caché de navegadores

Encabezados de origen	Tiempo de vida mínimo = 0	Tiempo de vida mínimo > 0
		Los navegadores almacenan en caché el objeto para el valor de la directiva `Cache-Control: max-age` .

Encabezados de origen	Tiempo de vida mínimo = 0	Tiempo de vida mínimo > 0
El origen añade un encabezado **`Expires`** al objeto	Almacenamiento en caché de CloudFront CloudFront almacena en caché el objeto hasta la fecha del encabezado `Expires` o el valor del TTL máximo de CloudFront, lo que suceda antes. Almacenamiento en caché de navegadores Los navegadores almacenan el objeto en la caché hasta la fecha del encabezado `Expires`.	Almacenamiento en caché de CloudFront El almacenamiento en caché de CloudFront depende de los valores de los TTL mínimo y máximo de CloudFront y del encabezado `Expires`: • Si TTL mínimo < `Expires` < TTL máximo, CloudFront almacena en caché el objeto hasta la fecha y hora del encabezado `Expires`. • Si `Expires` < TTL mínimo, CloudFront almacena en caché el objeto para el valor del TTL mínimo de CloudFront. • Si `Expires` > TTL máximo, CloudFront almacena en caché el objeto para el valor del TTL máximo de CloudFront. Almacenamiento en caché de navegadores Los navegadores almacenan el objeto en la caché hasta la

Encabezados de origen	Tiempo de vida mínimo = 0	Tiempo de vida mínimo > 0
		fecha y hora del encabezado `Expires`.
El origen agrega directivas **`Cache-Control: no-cache`**, **`no-store`** o **`private`** al objeto	CloudFront y los navegadores respetan los encabezados.	Almacenamiento en caché de CloudFront CloudFront almacena en caché el objeto para el valor del TTL mínimo de CloudFron t. Consulte la advertencia debajo de esta tabla. Almacenamiento en caché de navegadores Los navegadores respetan los encabezados.

Warning

- Si el TTL mínimo es superior a 0, CloudFront utiliza el TTL mínimo de la política de caché, aunque las directivas `Cache-Control: no-cache`, `no-store` o `private` estén presentes en los encabezados de origen.
  - Si se puede acceder al origen, CloudFront obtiene el objeto del origen y lo devuelve al lector.
  - Si no se puede acceder al origen o el TTL máximo es mayor que 0, CloudFront servirá el objeto que obtuvo del origen anteriormente.

  Para evitar este comportamiento, incluya la directiva `Cache-Control: stale-if-error=0` con el objeto devuelto desde el origen. Esto hace que CloudFront devuelva un error en respuesta a solicitudes futuras si el origen es inalcanzable, en lugar de devolver el objeto que obtuvo del origen anteriormente.
- CloudFront no almacena en caché el código de estado HTTP 501 (no implementado) de un origen de S3 cuando los encabezados de origen incluyen las directivas `Cache-Control:`

`no-cache`, `no-store` o `private`. Este es el comportamiento predeterminado de un origen de S3, incluso si la configuración de TTL mínima es superior a 0.

Para obtener información acerca de cómo cambiar la configuración de distribuciones mediante la consola de CloudFront, consulte Actualizar una distribución. Para obtener información sobre cómo cambiar la configuración de las distribuciones con la API de Cloudfront; consulte UpdateDistribution.

Agregación de encabezados a los objetos con la consola de Amazon S3

Puede agregar el campo de encabezado `Cache-Control` o `Expires` a los objetos de Amazon S3. Para ello, debe modificar los campos de metadatos del objeto.

Agregación de un campo de encabezado **`Cache-Control`** o **`Expires`** a objetos de Amazon S3

1. Siga el procedimiento de la sección Sustitución de metadatos definidos por el sistema en el tema Edición de metadatos de objetos en la consola de Amazon S3 de la Guía del usuario de Amazon S3.
2. Para Key (Clave), elija el nombre del encabezado que agregará (Cache-Control o Expires).
3. En Value (Valor), introduzca un valor de encabezado. Por ejemplo, para un encabezado `Cache-Control`, introduzca `max-age=86400`. Para `Expires`, introduzca una fecha y hora de caducidad tal como `Wed, 30 Jun 2021 09:28:00 GMT`.
4. Siga el resto del procedimiento para guardar los cambios en los metadatos.

Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta

Algunas aplicaciones web utilizan cadenas de consulta para enviar información al origen. Una cadena de consulta es la parte de una solicitud web que aparece después de un carácter ? y puede contener uno o varios parámetros, separados por caracteres &. En el siguiente ejemplo, la cadena de consulta incluye dos parámetros, *`color=red`* y *`size=large`*:

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

Para distribuciones, puede elegir si desea que CloudFront reenvíe cadenas de consultas al origen y si desea almacenar en caché el contenido en función de todos los parámetros o de los parámetros seleccionados. ¿Por qué podría resultar útil? Considere el siguiente ejemplo.

Supongamos que su sitio web está disponible en cinco idiomas. La estructura de directorios y los nombres de archivo de las cinco versiones del sitio web son idénticos. Cuando un usuario consulta el sitio web, las solicitudes que se reenvían a CloudFront incluyen un parámetro de cadena de consulta de idioma en función del idioma elegido por el usuario. Puede configurar CloudFront para reenviar cadenas de consulta al origen y almacenar en caché en función del parámetro de idioma. Si configura el servidor web para devolver la versión de una página determinada que se corresponda con el idioma seleccionado, CloudFront almacena en la caché cada versión del idioma por separado, en función del valor del parámetro de cadena de consulta del idioma.

En este ejemplo, si la página principal para el sitio web es `main.html`, las siguientes cinco solicitudes hacen que CloudFront almacene cinco veces en la caché `main.html`, una vez por cada valor de parámetro de cadena de consulta de idioma:

- `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`

Tenga en cuenta lo siguiente:

- Algunos servidores HTTP no procesan parámetros de cadenas de consulta y, por lo tanto, no devuelven distintas versiones de un objeto en función de los valores de los parámetros. Para estos orígenes, si configura CloudFront para reenviar los parámetros de cadenas de consulta al origen, CloudFront sigue almacenando en caché en función de los valores de los parámetros a pesar de que el origen devuelva versiones idénticas del objeto a CloudFront para cada valor del parámetro.
- Para que los parámetros de cadenas de consulta funcionen tal y como se describe en el ejemplo anterior con los idiomas, debe utilizar el carácter & como delimitador entre parámetros de cadenas de consulta. Si utiliza un delimitador diferente, es posible que obtenga resultados imprevistos, en función de los parámetros que especifique para que CloudFront utilice como base para el almacenamiento en caché y del orden en el que aparecen los parámetros en la cadena de consulta.

  Los siguientes ejemplos muestran lo que ocurre si utiliza un delimitador diferente y configura CloudFront para almacenar en caché solo en función del parámetro `color`:

- En la siguiente solicitud, CloudFront almacena en caché el contenido en función del valor del parámetro `color`, pero CloudFront interpreta el valor como *`red;size=large`*:

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

- En la siguiente solicitud, CloudFront almacena en caché el contenido pero no en función de los parámetros de cadenas de consulta. Esto se debe a que ha configurado CloudFront para almacenar en caché en función del parámetro `color`, pero CloudFront interpreta la siguiente cadena como que contiene solo un parámetro `size` con el valor *`large;color=red`*:

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

Puede configurar CloudFront para que realice una de las siguientes acciones:

- No enviar cadenas de consultas al origen. Si no reenvía cadenas de consultas, CloudFront no almacena en caché en función de parámetros de cadenas de consulta.
- Reenviar cadenas de consulta al origen y almacenar en caché en función de todos los parámetros de la cadena de consulta.
- Reenviar cadenas de consulta al origen y almacenar en caché en función de parámetros especificados en la cadena de consulta.

Para obtener más información, consulte the section called “Optimización del almacenamiento en caché”.

Temas

- Configuración de la consola y de la API para el reenvío de cadenas de consulta y almacenamiento en caché
- Optimización del almacenamiento en caché
- Parámetros de cadena de consulta y registros estándar de CloudFront (registros de acceso)

Configuración de la consola y de la API para el reenvío de cadenas de consulta y almacenamiento en caché

Al crear una distribución en la consola de CloudFront, CloudFront configura el reenvío y el almacenamiento en caché de cadenas de consulta en función del tipo de origen. Si lo desea, puede editar manualmente esta configuración. Para obtener más información, consulte la siguiente configuración en la the section called “Toda la configuración de distribución”:

- the section called “Reenvío de cadenas de consulta y almacenamiento en caché”
- the section called “Lista de permitidos de cadenas de consulta”

Para configurar el reenvío y el almacenamiento en caché de cadenas de consulta con la API de CloudFront, consulte CachePolicy y OriginRequestPolicy en la referencia de la API de Amazon CloudFront.

Optimización del almacenamiento en caché

Cuando se configura CloudFront para almacenar en caché en función de parámetros de cadenas de consulta, puede realizar los siguientes pasos para reducir el número de solicitudes que CloudFront reenvía al origen. Cuando las ubicaciones periférica de CloudFront sirven objetos, se reduce la carga en el servidor de origen y se reduce la latencia porque los objetos se sirven desde ubicaciones más cercanas a los usuarios.

Almacene en caché solo en función de parámetros por los que su origen devuelve diferentes versiones de un objeto

Por cada parámetro de cadena de consulta que la aplicación web reenvía a CloudFront, CloudFront reenvía solicitudes al origen por cada valor del parámetro y almacena en caché una versión independiente del objeto por cada valor del parámetro. Esto ocurre incluso si el origen siempre devuelve el mismo objeto independientemente del valor del parámetro. Para varios parámetros, el número de solicitudes y el número de objetos se multiplican.

Le recomendamos configurar CloudFront para almacenar en caché solo los parámetros de cadenas de consulta para los que el origen devuelve distintas versiones y que piense detenidamente en las ventajas de almacenar en caché en función de cada parámetro. Supongamos que tiene un sitio web de venta al por menor. Dispone de imágenes de una chaqueta en seis colores diferentes y la chaqueta está disponible en diez tallas distintas. Sus

imágenes de la chaqueta muestran los distintos colores, pero no las distintas tallas. Para optimizar el almacenamiento en caché, debe configurar CloudFront para almacenar en caché solo en función del parámetro de color, no el de tamaño. Esto aumenta la probabilidad de que CloudFront pueda atender una solicitud de la caché, lo que mejora el rendimiento y reduce la carga en el origen.

Organice los parámetros siempre en el mismo orden

El orden de los parámetros de cadenas de consulta es importante. En el siguiente ejemplo, las cadenas de consulta son idénticas, salvo que los parámetros están en órdenes diferentes. Esto hace que CloudFront reenvíe dos solicitudes de image.jpg independientes al origen y que almacene en caché dos versiones independientes del objeto:

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

Le recomendamos enumerar los nombres de los parámetros siempre en el mismo orden, por ejemplo, por orden alfabético.

Utilice siempre el mismo tipo de letra (mayúsculas o minúsculas) para los nombres y valores de parámetros

CloudFront diferencia mayúsculas de minúsculas en los valores y nombres de los parámetros al almacenar en caché en función de los parámetros de cadenas de consulta. En el siguiente ejemplo, las cadenas de consulta son idénticas, salvo por las mayúsculas y minúsculas de los nombres y valores del parámetro. Esto hace que CloudFront reenvíe cuatro solicitudes de image.jpg independientes al origen y que almacene en caché cuatro versiones independientes del objeto:

- `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`

Recomendamos utilizar mayúsculas o minúsculas de forma consistente en los valores y nombres de parámetros, como todo en minúsculas.

No utilice nombres de parámetros que entren en conflicto con URL firmadas

Si utiliza URL firmadas para restringir el acceso al contenido (si ha agregado signatarios de confianza a la distribución), CloudFront elimina los siguientes parámetros de cadenas de consulta antes de reenviar el resto de la URL al origen:

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

Si utiliza URL firmadas y desea configurar CloudFront para reenviar cadenas de consulta al origen, sus propios parámetros de cadenas de consulta no pueden denominarse `Expires`, `Key-Pair-Id`, `Policy` ni `Signature`.

Parámetros de cadena de consulta y registros estándar de CloudFront (registros de acceso)

Si habilita el registro, CloudFront registra la URL completa, incluidos los parámetros de cadenas de consulta. Esto ocurre independientemente de si ha configurado CloudFront para reenviar cadenas de consulta al origen. Para obtener más información acerca del registro de CloudFront, consulte the section called “Registros de acceso (registros estándar)”.

Almacenamiento en caché de contenido en función de cookies

De forma predeterminada, CloudFront no tiene en cuenta las cookies al procesar solicitudes y respuestas, ni al almacenar en caché los objetos en ubicaciones periférica. Si CloudFront recibe dos solicitudes que sean idénticas excepto por lo que está en el encabezado de `Cookie`, de forma predeterminada, CloudFront trata las solicitudes como idénticas y devuelve el mismo objeto para ambas solicitudes.

Puede configurar CloudFront para reenviar al origen algunas o todas las cookies de las solicitudes de los lectores y para almacenar en caché diferentes versiones de los objetos en función de los valores de las cookies de las solicitudes que reenvía. Al hacerlo, CloudFront utiliza algunas o todas las cookies de las solicitudes de lectores (las que esté configurado para reenviar) para identificar de forma única un objeto en la caché.

Supongamos que las solicitudes de `locations.html` contienen una cookie `country` con un valor de `uk` o `fr`. Al configurar CloudFront para almacenar los objetos en la caché en función del valor de la cookie `country`, CloudFront reenvía al origen las solicitudes de `locations.html` e incluye la cookie `country` y su valor. El origen devuelve `locations.html` y CloudFront almacena el objeto una vez en la caché para las solicitudes cuyo valor de la cookie `country` sea `uk` y otra vez para las solicitudes cuyo valor de la cookie sea `fr`.

> **Important**
>
> Amazon S3 y algunos servidores HTTP no procesan cookies. No configure CloudFront para reenviar cookies a un origen que no procese cookies o que no varíe su respuesta en función de las cookies. Esto puede hacer que CloudFront reenvíe más solicitudes al origen para el mismo objeto, lo que ralentiza el rendimiento y aumenta la carga en el origen. Si, teniendo en cuenta el ejemplo anterior, su origen no procesa la cookie `country` o siempre devuelve la misma versión de `locations.html` a CloudFront independientemente del valor de la cookie `country`, no configure CloudFront para que reenvíe esa cookie.
> Por el contrario, si el origen personalizado depende de una cookie en particular o envía diferentes respuestas en función de una cookie, asegúrese de configurar CloudFront para que reenvíe esa cookie al origen. De lo contrario, CloudFront elimina la cookie antes de reenviar la solicitud al origen.

Para configurar el reenvío de cookies, actualice el comportamiento de la caché de su distribución. Para obtener más información acerca de los comportamientos de caché, consulte Configuración del comportamiento de la caché y, en particular, las secciones Reenvío de cookies y Cookies de lista de permitidos.

Puede configurar cada comportamiento de la caché para realizar una de las siguientes acciones:

- Reenviar todas las cookies al origen: CloudFront incluye todas las cookies enviadas por el lector cuando reenvía las solicitudes al origen. Cuando el origen devuelve una respuesta, CloudFront almacena en caché la respuesta utilizando los nombres y valores de las cookies en la solicitud del lector. Si la respuesta de origen incluye encabezados `Set-Cookie`, CloudFront los devuelve al lector con el objeto solicitado. CloudFront también almacena en caché los encabezados `Set-Cookie` con el objeto devuelto desde el origen y envía esos encabezados `Set-Cookie` a los lectores en todos los aciertos de caché.
- Reenviar un conjunto de cookies que especifique: CloudFront elimina las cookies que el lector envía y que no están en la lista blanca antes de que reenvíe una solicitud al origen. CloudFront

almacena en caché la respuesta mediante el uso de los nombres y los valores de las cookies enumerados en la solicitud del lector. Si la respuesta de origen incluye encabezados `Set-Cookie`, CloudFront los devuelve al lector con el objeto solicitado. CloudFront también almacena en caché los encabezados `Set-Cookie` con el objeto devuelto desde el origen y envía esos encabezados `Set-Cookie` a los lectores en todos los aciertos de caché.

Para obtener información acerca de la especificación de comodines en nombres de cookies, consulte Cookies de lista de permitidos.

Para consultar la cuota actual de la cantidad de nombres de cookies que puede reenviar para cada comportamiento de la caché o para solicitar una ampliación de la cuota, consulte Cuotas en cadenas de consulta (configuración de caché heredada).

- No reenviar las cookies al origen: CloudFront no almacena los objetos en caché según las cookies enviadas por el lector. Además, CloudFront elimina las cookies antes de reenviar las solicitudes al origen y elimina los encabezados `Set-Cookie` de las respuestas antes de devolver las respuestas a los lectores. Como esta no es la forma óptima de utilizar los recursos de origen, al seleccionar este comportamiento de caché, debe asegurarse de que el origen no incluya cookies en las respuestas de origen de forma predeterminada.

Tenga en cuenta lo siguiente acerca de especificar las cookies que desea reenviar:

Logs de acceso

Si configura CloudFront para registrar solicitudes y registrar cookies, CloudFront registra todas las cookies y todos los atributos de cookies, incluso si configura CloudFront para no reenviar cookies al origen o si configura CloudFront para reenviar solo cookies específicas. Para obtener más información acerca del registro de CloudFront, consulte Registros de acceso (registros estándar).

Sensibilidad de mayúsculas y minúsculas

Los nombres y valores de las cookies distinguen entre mayúsculas y minúsculas. Por ejemplo, si se configura CloudFront para reenviar todas las cookies y dos solicitudes de lector para el mismo objeto tienen cookies que son idénticas excepto por el caso, CloudFront almacena el objeto dos veces en la caché.

CloudFront ordena las cookies

Si se configura CloudFront para reenviar las cookies (todas o un subconjunto), CloudFront ordena las cookies en orden natural por nombre de cookie antes de reenviar la solicitud al origen.

> **Note**
>
> No se admiten nombres de cookies que empiecen por el carácter $. CloudFront eliminará la cookie antes de reenviar la solicitud al origen. Puede eliminar el carácter $ o especificar otro distinto al principio del nombre de la cookie.

`If-Modified-Since` y `If-None-Match`

Las solicitudes condicionales `If-Modified-Since` y `If-None-Match` no son compatibles cuando CloudFront se configura para reenviar cookies (todas o un subconjunto).

Formato necesario de pares de nombre-valor estándar

CloudFront reenvía un encabezado de cookie solo si el valor se ajusta al formato estándar de pares de nombre-valor, por ejemplo: `"Cookie: cookie1=value1; cookie2=value2"`

Deshabilitar el almacenamiento en caché de los encabezados **`Set-Cookie`**

Si se configura CloudFront para reenviar cookies al origen (ya sean todas o cookies específicas), también almacena en caché los encabezados `Set-Cookie` recibidos en la respuesta de origen. CloudFront incluye estos encabezados `Set-Cookie` en la respuesta al lector original y también los incluye en las respuestas posteriores que se sirven desde la caché de CloudFront.

Si desea recibir cookies en el origen pero no desea que CloudFront almacene en caché los encabezados `Set-Cookie` en las respuestas del origen, configure el origen para agregar un encabezado `Cache-Control` con una política de `no-cache` que especifique `Set-Cookie` como nombre de campo. Por ejemplo: `Cache-Control: no-cache="Set-Cookie"`. Para obtener más información, consulte Directivas de respuesta de control de caché en el protocolo de transferencia de hipertexto (HTTP/1.1): almacenamiento en caché estándar.

Longitud máxima de los nombres de las cookies

Si configura CloudFront para reenviar cookies específicas al origen, la cantidad total de bytes en todos los nombres de cookies que configure para que CloudFront los reenvíe no puede superar los 512 menos la cantidad de cookies que reenvía. Por ejemplo, si configura CloudFront para reenviar 10 cookies al origen, la longitud combinada de los nombres de las 10 cookies no puede superar los 502 bytes (512-10).

Si configura CloudFront para reenviar todas las cookies al origen, la longitud de los nombres de las cookies no importa.

Para obtener más información acerca del uso de la consola de CloudFront para actualizar una distribución de modo que CloudFront reenvíe las cookies al origen, consulte Actualizar una distribución. Para obtener información sobre el uso de la API de CloudFront para actualizar una distribución, consulte UpdateDistribution en la Referencia de la API de Amazon CloudFront.

Almacenamiento en caché de contenido en función de encabezados de solicitud

CloudFront le permite elegir si desea que CloudFront reenvíe los encabezados al origen y almacene en caché diferentes versiones de un objeto especificado en función de los valores de encabezado de las solicitudes de los lectores. Esto le permite ofrecer distintas versiones del contenido en función del dispositivo del usuario, la ubicación del espectador, su idioma y otros criterios.

Temas

- Encabezados y distribuciones: información general
- Selección de los encabezados para basar el almacenamiento en caché
- Configuración de CloudFront para que respete la configuración de CORS
- Configuración del almacenamiento en caché en función del tipo de dispositivo
- Configuración del almacenamiento en caché en función del idioma del lector
- Configuración del almacenamiento en caché en función de la ubicación del lector
- Configuración del almacenamiento en caché en función del protocolo de la solicitud
- Configuración del almacenamiento en caché para archivos comprimidos
- Cómo afecta al rendimiento el almacenamiento en caché en función de los encabezados
- Cómo afectan al almacenamiento en caché las mayúsculas o minúsculas de los encabezados y sus valores
- Encabezados que CloudFront devuelve al lector

Encabezados y distribuciones: información general

De forma predeterminada, CloudFront no tiene en cuenta los encabezados al almacenar los objetos en la caché en ubicaciones periférica. Si el origen devuelve dos objetos que se diferencian solo por los valores de los encabezados de solicitud, CloudFront almacena solo una versión del objeto en la caché.

Puede configurar CloudFront para reenviar los encabezados al origen, lo que hace que CloudFront almacene en caché varias versiones de un objeto en función de los valores en uno o varios encabezados de solicitud. Para configurar CloudFront para almacenar en caché los objetos en función de los valores de encabezados específicos, se especifica la configuración del comportamiento de la caché para la distribución. Para obtener más información, consulte Caché en función de encabezados de solicitud seleccionados.

Supongamos que las solicitudes de espectadores de `logo.jpg` contienen un encabezado personalizado `Product` con un valor de `Acme` o `Apex`. Al configurar CloudFront para que almacene en caché los objetos en función del valor del encabezado `Product`, CloudFront reenvía solicitudes de `logo.jpg` al origen e incluye el encabezado `Product` y los valores del encabezado. CloudFront almacena en caché `logo.jpg` una vez por cada solicitud cuyo valor del encabezado `Product` es `Acme` y otra vez por cada solicitud cuyo valor es `Apex`.

Puede configurar cada comportamiento de la caché en una distribución para realizar una de las siguientes acciones:

- Reenviar todos los encabezados al origen

> **Note**
>
> Para configuraciones de caché heredadas: si configura CloudFront para reenviar todos los encabezados al origen, CloudFront no almacena en caché los objetos asociados con este comportamiento de la caché. En su lugar, envía todas las solicitudes al origen.

- Reenvíe una lista de encabezados que especifique. CloudFront almacena en caché los objetos en función de los valores de todos los encabezados especificados. CloudFront también reenvía los encabezados que reenvía de forma predeterminada, pero almacena en caché los objetos solo según los encabezados que especifique.
- Reenviar solo los encabezados predeterminados. En esta configuración, CloudFront no almacena los objetos en caché en función de los valores de los encabezados de solicitudes.

Para consultar la cuota actual de la cantidad de encabezados que puede reenviar para cada comportamiento de la caché o para solicitar una ampliación de la cuota, consulte Cuotas en encabezados.

Para obtener información acerca del uso de la consola de CloudFront para actualizar una distribución de modo que CloudFront reenvíe encabezados al origen, consulte Actualizar una distribución. Para

obtener información sobre el uso de la API de CloudFront para actualizar una distribución existente, consulte Actualizar distribución en la Referencia de la API de Amazon CloudFront.

Selección de los encabezados para basar el almacenamiento en caché

Los encabezados que puede reenviar al origen y en los que CloudFront basa el almacenamiento en caché dependen de si el origen es un bucket de Amazon S3 o un origen personalizado.

- Amazon S3: puede configurar CloudFront para reenviar y almacenar en caché los objetos en función de un número de encabezados específicos (consulte la lista de excepciones que se muestra a continuación). Sin embargo, le recomendamos que evite reenviar encabezados con un origen de Amazon S3, excepto que necesite implementar el uso compartido de recursos entre orígenes (CORS) o desee personalizar contenido mediante Lambda@Edge en eventos producidos en el origen.
  - Para configurar CORS, debe reenviar encabezados que permitan a CloudFront distribuir contenido para sitios web que están habilitados para el uso compartido de recursos entre orígenes (CORS). Para obtener más información, consulte Configuración de CloudFront para que respete la configuración de CORS.
  - Para personalizar el contenido mediante el uso de encabezados que reenvía al origen de Amazon S3, debe escribir y agregar funciones Lambda@Edge y asociarlas a la distribución de CloudFront para desencadenarlas mediante un evento producido en el origen. Para obtener más información acerca del uso de encabezados para personalizar contenido, consulte Personalización de contenido por encabezados de tipo de dispositivo o país: ejemplos.

    Le recomendamos que evite reenviar encabezados que no esté utilizando para la personalización de contenido, ya que el reenvío de encabezados adicionales puede reducir la tasa de aciertos de caché. Es decir, CloudFront; no puede atender tantas solicitudes de cachés perimetrales, como una proporción de todas las solicitudes.
- Origen personalizado: puede configurar CloudFront para almacenar en caché en función del valor de cualquier encabezado de solicitud, excepto los siguientes:
  - `Connection`
  - `Cookie`: si desea reenviar y almacenar en caché en función de las cookies, utilice otra configuración diferente en la distribución. Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.
  - `Host (for Amazon S3 origins)`
  - `Proxy-Authorization`

- `TE`
- `Upgrade`

Puede configurar CloudFront para almacenar en caché los objetos en función de los valores de los encabezados `Date` y `User-Agent`, pero no lo recomendamos. Estos encabezados tienen muchos valores posibles y el almacenamiento en caché en función de los valores podría hacer que CloudFront reenvíe una cantidad de solicitudes significativamente mayor al origen.

Para obtener una lista completa de encabezados de solicitudes HTTP y cómo los procesa CloudFront, consulte Encabezados de solicitudes HTTP y comportamiento de CloudFront (personalizado y orígenes de Amazon S3).

Configuración de CloudFront para que respete la configuración de CORS

Si ha habilitado el uso compartido de recursos entre orígenes (CORS) en un bucket de Amazon S3 o en un origen personalizado, debe elegir encabezados específicos para reenviar, para respetar la configuración CORS. Los encabezados que debe reenviar difieren en función del origen (Amazon S3 o personalizado) y si desea almacenar las respuestas de `OPTIONS` en caché.

Amazon S3

- Si desea que las respuestas `OPTIONS` se almacenen en caché, haga lo siguiente:
  - Elija las opciones para la configuración de comportamiento de la caché predeterminado que habilitan el almacenamiento en caché para respuestas de `OPTIONS`.
  - Configure CloudFront para reenviar los siguientes encabezados: `Origin`, `Access-Control-Request-Headers`, y `Access-Control-Request-Method`.
- Si no desea que las respuestas de `OPTIONS` se almacenen en caché, configure CloudFront para reenviar el encabezado `Origin`, junto con los demás encabezados requeridos por el origen (por ejemplo `Access-Control-Request-Headers`, `Access-Control-Request-Method` u otros).

Orígenes personalizados: reenvíe el encabezado `Origin` junto con los demás encabezados exigidos por el origen.

Para configurar CloudFront con el fin de que almacene en caché en caché en función de CORS, debe configurar CloudFront para reenviar los encabezados mediante una política de caché. Para obtener más información, consulte Control de la clave de caché con una política.

Para obtener más información sobre CORS y Amazon S3, consulte Uso compartido de recursos entre orígenes (CORS) en la Guía del usuario de Amazon Simple Storage Service.

Configuración del almacenamiento en caché en función del tipo de dispositivo

Si desea que CloudFront almacene en caché diferentes versiones de los objetos en función del dispositivo que el usuario utilice para consultar el contenido, configure CloudFront para reenviar los encabezados aplicables al origen personalizado:

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

En función del valor del encabezado `User-Agent`, CloudFront establece el valor de estos encabezados en `true` o `false` antes de reenviar la solicitud al origen. Si un dispositivo entra en más de una categoría, más de un valor podría ser `true`. Por ejemplo, en el caso de algunas tabletas, CloudFront podría establecer tanto `CloudFront-Is-Mobile-Viewer` como `CloudFront-Is-Tablet-Viewer` en `true`.

Configuración del almacenamiento en caché en función del idioma del lector

Si desea que CloudFront almacene en caché distintas versiones de los objetos en función del idioma especificado en la solicitud, configure CloudFront para reenviar el encabezado `Accept-Language` al origen.

Configuración del almacenamiento en caché en función de la ubicación del lector

Si desea que CloudFront almacene en caché distintas versiones de los objetos en función del país del que provino la solicitud, configure CloudFront para reenviar el encabezado `CloudFront-Viewer-Country` al origen. CloudFront convierte automáticamente la dirección IP de la que provino la solicitud en un código de país de dos letras. Para obtener una lista sencilla de códigos de país, organizable por código y por nombre de país, consulte la entrada de Wikipedia ISO 3166-1 alpha-2.

Configuración del almacenamiento en caché en función del protocolo de la solicitud

Si desea que CloudFront almacene en caché distintas versiones de los objetos en función del protocolo de la solicitud (HTTP o HTTPS), configure CloudFront para reenviar el encabezado `CloudFront-Forwarded-Proto` al origen.

Configuración del almacenamiento en caché para archivos comprimidos

Si el origen admite compresión Brotli, puede almacenar en caché en función del encabezado `Accept-Encoding`. Configure el almacenamiento en caché en función de `Accept-Encoding` solo si el origen ofrece contenido en función del encabezado.

Cómo afecta al rendimiento el almacenamiento en caché en función de los encabezados

Si configura CloudFront para almacenar en caché en función de uno o varios encabezados y los encabezados tienen más de un valor posible, CloudFront reenvía más solicitudes al servidor de origen para el mismo objeto. Esto afecta negativamente el desempeño y aumenta la carga en su servidor de origen. Si el servidor de origen devuelve el mismo objeto independientemente del valor de un encabezado determinado, le recomendamos que no configure CloudFront para almacenar en caché en función de ese encabezado.

Si configura CloudFront para reenviar más de un encabezado, el orden de los encabezados de las solicitudes de los lectores no afecta al almacenamiento en caché siempre y cuando los valores sean los mismos. Por ejemplo, si una solicitud contiene los encabezados A:1,B:2 y otra solicitud contiene B:2,A:1, CloudFront almacena en caché solo una copia del objeto.

Cómo afectan al almacenamiento en caché las mayúsculas o minúsculas de los encabezados y sus valores

Cuando CloudFront almacena en caché en función de los valores del encabezado, pasa por alto el uso de mayúsculas y minúsculas en los nombres de encabezado, pero lo tiene en cuenta en el caso del valor de encabezado:

- Si las solicitudes de lector incluyen `Product:Acme` y `product:Acme`, CloudFront almacena en caché un objeto solo una vez. La única diferencia entre ellos es el uso de mayúsculas y minúsculas en el nombre del encabezado, lo que no afecta el almacenamiento en caché.

- Si las solicitudes de lector incluyen `Product:Acme` y `Product:acme`, CloudFront almacena en caché un objeto dos veces, porque el valor es `Acme` en algunas solicitudes y `acme` en otras.

Encabezados que CloudFront devuelve al lector

La configuración de CloudFront para reenviar y almacenar en caché los encabezados no afecta a los encabezados que CloudFront devuelve al lector. CloudFront devuelve todos los encabezados que obtiene del origen con algunas excepciones. Para obtener más información, consulte el tema correspondiente:

- Orígenes de Amazon S3: consulte Encabezados de respuesta HTTP que CloudFront elimina o actualiza.
- Orígenes personalizados: consulte Encabezados de respuesta HTTP que CloudFront elimina o reemplaza.

Control de la clave de caché con una política

Con una política de caché de CloudFront, puede especificar encabezados HTTP, cookies y cadenas de consultas que CloudFront incluye en la clave de caché para objetos que se almacenan en caché en las ubicaciones periféricas de CloudFront. La clave de caché es el identificador único de cada objeto de la caché y determina si una solicitud de lector de HTTP da como resultado un acierto de la caché.

Un acierto de caché se produce cuando una solicitud de lector genera la misma clave de caché que una solicitud anterior y el objeto de esa clave de caché está en la caché de la ubicación periférica y es válido. Cuando hay un acierto de caché, el objeto se proporciona al lector desde una ubicación periférica de CloudFront, lo que tiene los siguientes beneficios:

- Carga reducida en el servidor de origen
- Latencia reducida para el lector

La inclusión de menos valores en la clave de caché aumenta la probabilidad de un acierto de caché. Así puede obtener un mejor rendimiento de su sitio web o aplicación, ya que tiene una proporción de aciertos de caché más alta (una mayor proporción de solicitudes de lectores que da como resultado un acierto de caché). Para obtener más información, consulte Descripción de la clave de caché.

Para controlar la clave de caché, se utiliza una política de caché de CloudFront. Puede asociar una política de caché a uno o más comportamientos de caché en una distribución de CloudFront.

También puede utilizar la política de caché para especificar la configuración del periodo de vida (TTL) de los objetos de la caché de CloudFront y habilitar CloudFront para que solicite y almacene en caché objetos comprimidos.

> **Note**
>
> La configuración de la caché no afecta a las solicitudes de gRPC porque el tráfico de gRPC no se puede almacenar en caché. Para obtener más información, consulte Uso de gRPC con distribuciones de CloudFront.

Temas

- Descripción de las políticas de caché

- Creación de políticas de caché
- Uso de políticas de caché administradas
- Descripción de la clave de caché

Descripción de las políticas de caché

Puede utilizar una política de caché para mejorar la proporción de aciertos de caché controlando los valores (cadenas de consulta de URL, encabezados HTTP y cookies) que se incluyen en la clave de caché. CloudFront proporciona algunas políticas de caché predefinidas, conocidas como políticas administradas, para casos de uso comunes. Puede usar estas políticas administradas o puede crear su propia política de caché que sea específica para sus necesidades. Para obtener más información sobre las políticas administradas, consulte Uso de políticas de caché administradas.

Una política de caché contiene la siguiente configuración, que se clasifica en información de política, configuración del tiempo de vida (TTL) y configuración de clave de caché.

Información de políticas

Nombre

Un nombre para identificar la política de caché. En la consola, se utiliza el nombre para asociar la política de caché a un comportamiento de caché.

Descripción

Un comentario para describir la política de caché. Esto es opcional, pero puede ayudarle a identificar el propósito de la política de caché.

Configuración del tiempo de vida (TTL)

La configuración del tiempo de vida (TTL) funciona junto con los encabezados HTTP `Cache-Control` y `Expires` (si están en la respuesta de origen) para determinar cuánto tiempo permanecen válidos los objetos de la caché de CloudFront.

Tiempo de vida mínimo

La cantidad de tiempo mínima, en segundos, que desea que los objetos permanezcan en la caché de CloudFront antes de que CloudFront compruebe con el origen si el objeto se ha

actualizado. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

> **Warning**
>
> Si el TTL mínimo es superior a 0, CloudFront almacenará en caché el contenido al menos durante el tiempo especificado en el TTL mínimo de la política de caché, aunque estén presentes las directivas `Cache-Control: no-cache`, `no-store` o `private` en los encabezados de origen.

Tiempo de vida máximo

La cantidad de tiempo máxima, en segundos, que los objetos permanecen en la caché de CloudFront antes de que CloudFront compruebe con el origen si el objeto se ha actualizado. CloudFront utiliza esta configuración solo cuando el origen envía los encabezados `Cache-Control` o `Expires` con el objeto. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Tiempo de vida (TTL) predeterminado

La cantidad de tiempo predeterminada, en segundos, que desea que los objetos permanezcan en la caché de CloudFront antes de que CloudFront compruebe con el origen si el objeto se ha actualizado. CloudFront utiliza este valor de configuración como TTL del objeto solo cuando el origen no envía encabezados `Cache-Control` ni `Expires` con el objeto. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

> **Note**
>
> Si los valores de TTL mínimo, TTL máximo y TTL predeterminado están establecidos en 0, se deshabilita el almacenamiento en caché de CloudFront.

Configuración de la clave de caché

La configuración de la clave de caché especifica los valores de las solicitudes de lector que CloudFront incluye en la clave de caché. Los valores pueden incluir cadenas de consulta de URL,

encabezados HTTP y cookies. Los valores que se incluyen en la clave de caché se incluyen automáticamente en las solicitudes que CloudFront envía al origen, conocidas como solicitudes de origen. Para obtener información sobre cómo controlar las solicitudes de origen sin afectar a la clave de caché, consulte Control de las solicitudes de origen con una política.

La configuración de la clave de caché incluye:

- Encabezados
- Cookies
- Cadenas de consulta
- Compatibilidad con la compresión

Encabezados

Los encabezados HTTP en las solicitudes del lector que CloudFront incluye en la clave de caché y en las solicitudes de origen. En encabezados, puede elegir una de las siguientes configuraciones:

- None (Ninguno): los encabezados HTTP en las solicitudes de lector no se incluyen en la clave de caché y no se incluyen automáticamente en las solicitudes de origen.
- Include the following headers (Incluir los siguientes encabezados): esta opción le permite especificar los encabezados HTTP en las solicitudes de lector que se incluyen en la clave de caché y, de forma automática, en las solicitudes de origen.

Cuando se utiliza la opción Include the following headers (Incluir los siguientes encabezados), se especifican los encabezados HTTP por su nombre, no por su valor. Por ejemplo, fíjese en el encabezado HTTP siguiente:

```
Accept-Language: en-US,en;q=0.5
```

En este caso, se especifica el encabezado como `Accept-Language`, no como `Accept-Language: en-US,en;q=0.5`. Sin embargo, CloudFront incluye el encabezado completo, incluido su valor, en la clave de caché y en las solicitudes de origen.

También puede incluir ciertos encabezados generados por CloudFront en la clave de caché. Para obtener más información, consulte the section called “Añadido de encabezados de solicitudes de CloudFront”.

Cookies

Las cookies en las solicitudes del lector que CloudFront incluye en la clave de caché y en las solicitudes de origen. Para cookies, puede elegir una de las siguientes configuraciones:

- None (Ninguna): las cookies en las solicitudes de lector no se incluyen en la clave de caché y no se incluyen automáticamente en las solicitudes de origen.
- All (Todas): las cookies en las solicitudes de lector se incluyen en la clave de caché y se incluyen automáticamente en las solicitudes de origen.
- Include specified cookies (Incluir las cookies especificadas): esta opción le permite especificar las cookies de las solicitudes de lector que se incluyen en la clave de caché y, de forma automática, en las solicitudes de origen.
- Include all cookies except (Incluir todas las cookies excepto): esta opción le permite especificar las cookies de las solicitudes de lector que no se incluyen en la clave de caché y no se incluyen de forma automática en las solicitudes de origen. Todas las demás cookies, excepto las que especifique, se incluyen en la clave de caché y se incluyen automáticamente en las solicitudes de origen.

Cuando utiliza la configuración Include specified cookies (Incluir las cookies especificadas) o Include all cookies except (Incluir todas las cookies excepto), se especifican las cookies por su nombre, no por su valor. Por ejemplo, fíjese en el encabezado `Cookie` siguiente:

```
Cookie: session_ID=abcd1234
```

En este caso, se especifica la cookie como `session_ID`, no como `session_ID=abcd1234`. Sin embargo, CloudFront incluye la cookie completa, incluido su valor, en la clave de caché y en las solicitudes de origen.

Cadenas de consulta

Las cadenas de consulta de URL en las solicitudes de lector que CloudFront incluye en la clave de caché y en las solicitudes de origen. Para cadenas de consulta, puede elegir una de las opciones siguientes:

- None (Ninguna): las cadenas de consulta de las solicitudes del lector no se incluyen en la clave de caché y no se incluyen automáticamente en las solicitudes de origen.
- All (Todas): todas las cadenas de consulta de las solicitudes de lector se incluyen en la clave de caché y también se incluyen automáticamente en las solicitudes de origen.

- Include specified query strings (Incluir cadenas de consulta especificadas): esta opción le permite especificar las cadenas de consulta de las solicitudes de lector que se incluyen en la clave de caché y, de forma automática, en las solicitudes de origen.
- Include all query strings except (Incluir todas las cadenas de consulta excepto): esta opción le permite especificar las cadenas de consulta de las solicitudes de lector que no se incluyen en la clave de caché y no se incluyen de forma automática en las solicitudes de origen. Todas las demás cadenas de consulta, excepto las especificadas, se incluyen en la clave de caché y se incluyen automáticamente en las solicitudes de origen.

Cuando se utiliza la configuración Include specified query strings (Incluir cadenas de consulta especificadas) o Include all query strings except (Incluir todas las cadenas de consulta excepto), se especifican cadenas de consulta por su nombre, no por su valor. Por ejemplo, fíjese en la ruta URL siguiente:

```
/content/stories/example-story.html?split-pages=false
```

En este caso, se especifica la cadena de consulta como `split-pages`, no como `split-pages=false`. Sin embargo, CloudFront incluye la cadena de consulta completa, incluido el valor, en la clave de caché y en las solicitudes de origen.

> **Note**
>
> Para la configuración de la clave de caché, CloudFront trata el carácter de asterisco (`*`) para los encabezados, las cadenas de consulta y las cookies como una cadena literal, no como un comodín.

Compatibilidad con la compresión

Esta configuración permite a CloudFront solicitar y almacenar en caché objetos comprimidos en los formatos de compresión Gzip o Brotli, cuando el lector lo admite. Esta configuración también permite que la compresión de CloudFront funcione. Los lectores indican su compatibilidad con estos formatos de compresión con el encabezado HTTP `Accept-Encoding`.

> **Note**
>
> Los navegadores web Chrome y Firefox admiten compresión Brotli solo cuando la solicitud se envía mediante HTTPS. Estos navegadores no admiten Brotli con solicitudes HTTP.

Habilite esta configuración cuando se cumpla cualquiera de las siguientes condiciones:

- Su origen devuelve objetos comprimidos Gzip cuando los lectores los admiten (las solicitudes contienen el encabezado HTTP `Accept-Encoding` con `gzip` como valor). En este caso, utilice la configuración habilitada para Gzip (establezca `EnableAcceptEncodingGzip` en `true` en la API de CloudFront, los SDK de AWS, AWS CLI o CloudFormation).
- El origen devuelve objetos comprimidos Brotli cuando los lectores los admiten (las solicitudes contienen el encabezado HTTP `Accept-Encoding` con `br` como valor). En este caso, utilice la configuración Brotli enabled (Brotli habilitado) (establezca `EnableAcceptEncodingBrotli` en `true` en la API de CloudFront, los SDK de AWS, AWS CLI o CloudFormation).
- El comportamiento de caché al que está asociada esta política de caché se configura con compresión de CloudFront. En este caso, puede habilitar el almacenamiento en caché para Gzip o Brotli, o ambos. Cuando la compresión de CloudFront está habilitada, habilitar el almacenamiento en caché para ambos formatos puede ayudar a reducir los costos de transferencia de datos salientes a Internet.

> **Note**
>
> Si habilita el almacenamiento en caché para uno de estos formatos de compresión o ambos, no incluya el encabezado `Accept-Encoding` en una política de solicitud de origen asociada con el mismo comportamiento de caché. CloudFront siempre incluye este encabezado en las solicitudes de origen cuando el almacenamiento en caché está habilitado para cualquiera de estos formatos, por lo que incluir `Accept-Encoding` en una política de solicitud de origen no tiene ningún efecto.

Si el servidor de origen no devuelve objetos comprimidos Gzip o Brotli o si el comportamiento de caché no está configurado con compresión de CloudFront, no habilite el almacenamiento en caché para objetos comprimidos. Si lo hace, es posible que provoque una disminución en la proporción de aciertos de caché.

A continuación, se explica cómo afecta esta configuración a una distribución de CloudFront. Todos los escenarios que se muestran a continuación, suponen que la solicitud del lector incluye el encabezado `Accept-Encoding`. Cuando la solicitud del lector no incluye el encabezado `Accept-Encoding`, CloudFront no incluye este encabezado en la clave de caché y no lo incluye en la solicitud de origen correspondiente.

Cuando se habilita el almacenamiento en caché de objetos comprimidos para ambos formatos de compresión

Si el lector admite Gzip y Brotli, es decir, si los valores `gzip` y `br` están en el encabezado `Accept-Encoding` de la solicitud del lector, CloudFront hace lo siguiente:

- Normaliza el encabezado en `Accept-Encoding: br,gzip` e incluye el encabezado normalizado en la clave de caché. La clave de caché no incluye otros valores que estaban en el encabezado `Accept-Encoding` enviado por el lector.
- Si la ubicación de borde tiene un objeto comprimido Brotli o Gzip en la caché que coincide con la solicitud y no ha caducado, la ubicación de borde devuelve el objeto al lector.
- Si la ubicación periférica no tiene un objeto comprimido Brotli o Gzip en la caché que coincida con la solicitud y no haya vencido, CloudFront incluye el encabezado normalizado (`Accept-Encoding: br,gzip`) en la solicitud de origen correspondiente. La solicitud de origen no incluye otros valores que estaban en el encabezado `Accept-Encoding` enviado por el lector.

Si el lector admite un formato de compresión pero no el otro, por ejemplo, si `gzip` es un valor en el encabezado `Accept-Encoding` de la solicitud del lector pero `br` no, CloudFront hace lo siguiente:

- Normaliza el encabezado en `Accept-Encoding: gzip` e incluye el encabezado normalizado en la clave de caché. La clave de caché no incluye otros valores que estaban en el encabezado `Accept-Encoding` enviado por el lector.
- Si la ubicación periférica tiene un objeto comprimido Gzip en la caché que coincide con la solicitud y no ha caducado, la ubicación de borde devuelve el objeto al lector.
- Si la ubicación periférica no tiene un objeto comprimido Gzip en la caché que coincida con la solicitud y no haya vencido, CloudFront incluye el encabezado normalizado (`Accept-Encoding: gzip`) en la solicitud de origen correspondiente. La solicitud de origen no incluye otros valores que estaban en el encabezado `Accept-Encoding` enviado por el lector.

Para entender lo que CloudFront hace si el lector admite Brotli pero no Gzip, reemplace los dos formatos de compresión entre sí en el ejemplo anterior.

Si el lector no admite Brotli ni Gzip, es decir, el encabezado `Accept-Encoding` de la solicitud del lector no contiene `br` ni `gzip` como valores, CloudFront:

- No incluye el encabezado `Accept-Encoding` en la clave de caché.
- Incluye `Accept-Encoding: identity` en la solicitud de origen correspondiente. La solicitud de origen no incluye otros valores que estaban en el encabezado `Accept-Encoding` enviado por el lector.

Cuando el almacenamiento en caché de objetos comprimidos está habilitado para un formato de compresión, pero no para el otro

Si el lector admite el formato para el que está habilitado el almacenamiento en caché, por ejemplo, si el almacenamiento en caché de objetos comprimidos está habilitado para Gzip y el lector admite Gzip (`gzip` es uno de los valores del encabezado `Accept-Encoding` de la solicitud del lector), CloudFront hace lo siguiente:

- Normaliza el encabezado en `Accept-Encoding: gzip` e incluye el encabezado normalizado en la clave de caché.
- Si la ubicación periférica tiene un objeto comprimido Gzip en la caché que coincide con la solicitud y no ha caducado, la ubicación de borde devuelve el objeto al lector.
- Si la ubicación periférica no tiene un objeto comprimido Gzip en la caché que coincida con la solicitud y no haya vencido, CloudFront incluye el encabezado normalizado (`Accept-Encoding: gzip`) en la solicitud de origen correspondiente. La solicitud de origen no incluye otros valores que estaban en el encabezado `Accept-Encoding` enviado por el lector.

Este comportamiento es el mismo cuando el lector admite Gzip y Brotli (el encabezado `Accept-Encoding` de la solicitud del lector incluye `gzip` y `br` como valores), porque en este escenario, el almacenamiento en caché de objetos comprimidos para Brotli no está habilitado.

Para entender lo que CloudFront hace si el almacenamiento en caché de objetos comprimidos está habilitado para Brotli pero no para Gzip, reemplace los dos formatos de compresión entre sí en el ejemplo anterior.

Si el lector no admite el formato de compresión para el que está habilitado el almacenamiento en caché (el encabezado `Accept-Encoding` de la solicitud del lector no contiene el valor de ese formato), CloudFront:

- No incluye el encabezado `Accept-Encoding` en la clave de caché.
- Incluye `Accept-Encoding: identity` en la solicitud de origen correspondiente. La solicitud de origen no incluye otros valores que estaban en el encabezado `Accept-Encoding` enviado por el lector.

Cuando se desactiva el almacenamiento en caché de objetos comprimidos para ambos formatos de compresión

Cuando el almacenamiento en caché de objetos comprimidos está desactivado para ambos formatos de compresión, CloudFront trata el encabezado `Accept-Encoding` igual que cualquier otro encabezado HTTP en la solicitud del lector. De forma predeterminada, no se incluye en la clave de caché y no se incluye en las solicitudes de origen. Puede incluirlo en la lista de encabezados de una política de caché o una política de solicitud de origen igual que cualquier encabezado HTTP.

Creación de políticas de caché

Puede utilizar una política de caché para mejorar la proporción de aciertos de caché controlando los valores (cadenas de consulta de URL, encabezados HTTP y cookies) que se incluyen en la clave de caché. Puede crear una política de caché en la consola de CloudFront con la AWS Command Line Interface (AWS CLI) o con la API de CloudFront.

Después de crear una política de caché, puede asociarla a uno o más comportamientos de caché en una distribución de CloudFront.

Console

Para crear una política de caché (consola)

1. Inicie sesión en Consola de administración de AWS y abra la página Policies (Políticas) en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home?#/policies.
2. Elija Create cache policy (Crear política de caché).
3. Elija la configuración deseada para esta política de caché. Para obtener más información, consulte Descripción de las políticas de caché.
4. Cuando termine, elija Create (Crear).

Después de crear una política de caché, puede asociarla a un comportamiento de caché.

Para asociar una política de caché a una distribución existente (consola)

1. Abra la página Distributions (Distribuciones) en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Elija la distribución que se va a actualizar y, a continuación, elija la pestaña Behaviors (Comportamientos).
3. Elija el comportamiento de caché que se va a actualizar y, a continuación, elija Edit (Editar).

   O bien, para crear un nuevo comportamiento de caché, elija Create behavior (Crear comportamiento).
4. En la sección Cache key and origin requests (Solicitudes de origen y clave de caché), asegúrese de elegir Cache policy and origin request policy (Política de caché y política de solicitud de origen).
5. En Cache policy (Política de caché), elija la política de caché que se va a asociar a este comportamiento de caché.
6. Elija Save changes (Guardar cambios) en la parte inferior de la página.

Para asociar una política de caché a una nueva distribución (consola)

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Create distribution (Crear distribución).
3. En la sección Solicitudes de origen y clave de caché, asegúrese de elegir Política de caché y política de solicitud de origen.
4. En Cache policy (Política de caché), elija la política de caché que se asocia al comportamiento predeterminado de la caché de esta distribución.
5. Elija la configuración deseada para el origen, el comportamiento predeterminado de la caché y la distribución. Para obtener más información, consulte Referencia de toda la configuración de distribución.
6. Cuando termine, elija Create distribution (Crear distribución).

CLI

Para crear una política de caché con AWS Command Line Interface (AWS CLI), utilice el comando aws cloudfront create-cache-policy. Puede utilizar un archivo de entrada para

proporcionar los parámetros de entrada del comando, en lugar de especificar cada parámetro individual como entrada de línea de comandos.

Para crear una política de caché (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo denominado `cache-policy.yaml` que contenga todos los parámetros de entrada del comando create-cache-policy.

```
aws cloudfront create-cache-policy --generate-cli-skeleton yaml-input > cache-
policy.yaml
```

2. Abra el archivo llamado `cache-policy.yaml` que acaba de crear. Edite el archivo para especificar la configuración de política de caché que desee y, a continuación, guarde el archivo. Puede eliminar campos opcionales del archivo, pero no eliminar los campos obligatorios.

   Para obtener más información acerca de la configuración de política de caché, consulte Descripción de las políticas de caché.

3. Utilice el siguiente comando para crear la política de caché utilizando parámetros de entrada del archivo de `cache-policy.yaml`.

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

   Anote el valor de `Id` en la salida del comando. Este es el ID de política de caché y lo necesita para asociar la política de caché al comportamiento de caché de una distribución de CloudFront.

Para asociar una política de caché a una distribución existente (CLI con archivo de entrada)

1. Utilice el comando siguiente para guardar la configuración de distribución de la distribución de CloudFront que desea actualizar. Reemplace *`distribution_ID`* por el ID de la distribución.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Abra el archivo llamado `dist-config.yaml` que acaba de crear. Edite el archivo, realizando los siguientes cambios en cada comportamiento de caché que actualice para utilizar una política de caché.

   - En el comportamiento de caché, agregue un campo denominado `CachePolicyId`. Para el valor del campo, utilice el ID de política de caché que anotó después de crear la política.
   - Elimine los campos `MinTTL`, `MaxTTL`, `DefaultTTL` y `ForwardedValues` del comportamiento de la caché. Estas configuraciones se especifican en la política de caché, por lo que no puede incluir estos campos ni una política de caché en el mismo comportamiento de caché.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución y utilizar la política de caché. Reemplace *`distribution_ID`* por el ID de la distribución.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Para asociar una política de caché a una nueva distribución (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo denominado `distribution.yaml` que contenga todos los parámetros de entrada del comando create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Abra el archivo llamado `distribution.yaml` que acaba de crear. En el comportamiento de caché predeterminado, en el campo `CachePolicyId`, escriba el ID de política de caché que anotó después de crear la política. Siga editando el archivo para especificar la configuración de distribución que desee y, a continuación, guarde el archivo cuando termine.

   Para obtener más información acerca de la configuración de distribución, consulte Referencia de toda la configuración de distribución.

3. Utilice el siguiente comando para crear la distribución mediante los parámetros de entrada del archivo de `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Para crear una política de caché con la API de CloudFront, utilice CreateCachePolicy. Para obtener más información sobre los campos que especifique en esta llamada a la API, consulte Descripción de las políticas de caché y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Después de crear una política de caché, puede asociarla a un comportamiento de caché mediante una de las siguientes llamadas a la API:

- Para asociarla a un comportamiento de caché en una distribución existente, utilice UpdateDistribution.
- Para asociarlo con un comportamiento de caché en una nueva distribución, utilice CreateDistribution.

Para estas llamadas a la API, proporcione el ID de la política de caché en el campo `CachePolicyId`, dentro de un comportamiento de caché. Para obtener más información sobre los otros campos que especifique en estas llamadas a la API, consulte Referencia de toda la configuración de distribución y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Uso de políticas de caché administradas

CloudFront proporciona un conjunto de políticas de caché administradas que puede asociar a cualquiera de los comportamientos de caché de la distribución. Con una política de caché administrada, no necesita escribir ni mantener su propia política de caché. Las políticas administradas utilizan configuraciones optimizadas para casos de uso específicos.

Para utilizar una política de caché administrada, debe asociarla a un comportamiento de caché en su distribución. El proceso es el mismo que cuando crea una política de caché, pero en lugar de crear una nueva, simplemente asocia una de las políticas de caché administradas. Se asocia la política

por nombre (con la consola) o por ID (con AWS CLI o los SDK). Los nombres e ID se muestran en la siguiente sección.

Para obtener más información, consulte Creación de políticas de caché.

En los temas siguientes, se describen las políticas de caché administradas que puede utilizar.

Temas

- Amplify
- CachingDisabled
- CachingOptimized
- CachingOptimizedForUncompressedObjects
- Elemental-MediaPackage
- UseOriginCacheControlHeaders
- UseOriginCacheControlHeaders-QueryStrings

Amplify

Consulte esta política en la consola de CloudFront

Esta política está diseñada para usarse con un origen que es una aplicación web de AWS Amplify.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`2e54312d-136d-493c-8eb9-b001f22f67d2`

Esta política tiene las siguientes opciones:

- TTL mínimo: 2 segundos
- TTL máximo: 600 segundos (10 minutos)
- TTL predeterminado: 2 segundos
- Encabezados incluidos en la clave de caché:
  - `Authorization`
  - `CloudFront-Viewer-Country`
  - `Host`

El encabezado `Accept-Encoding` normalizado también se incluye porque la configuración de objetos comprimidos en caché está habilitada. Para obtener más información, consulte Compression support (Ayuda para la compresión).

- Cookies incluidas en la clave de caché: se incluyen todas las cookies.
- Cadenas de consulta incluidas en la clave de caché: se incluyen todas las cadenas de consulta.
- Configuración de objetos comprimidos en caché: habilitada. Para obtener más información, consulte Compression support (Ayuda para la compresión).

> **Warning**
>
> Dado que esta política tiene un TTL mínimo superior a 0, CloudFront almacenará en caché el contenido durante al menos el tiempo especificado en el TTL mínimo de la política de caché, aunque las directivas `Cache-Control: no-cache`, `no-store` o `private` estén presentes en los encabezados de origen.

Políticas de caché de AWS Amplify Hosting

Amplify utiliza las siguientes políticas de caché administradas a fin de optimizar la configuración de caché predeterminada para las aplicaciones de los clientes:

- Amplify-Default
- Amplify-DefaultNoCookies
- Amplify-ImageOptimization
- Amplify-StaticContent

> **Note**
>
> Estas políticas solo las utiliza Amplify. No le recomendamos que las utilice para las distribuciones.

Para obtener más información sobre cómo administrar la configuración de la caché para la aplicación alojada en Amplify, consulte Managing cache configuration en la Guía del usuario de Amplify Hosting.

CachingDisabled

Consulte esta política en la consola de CloudFront

Esta política desactiva el almacenamiento en caché. Esta política es útil para el contenido dinámico y para las solicitudes que no se pueden almacenar en caché.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`4135ea2d-6df8-44a3-9df3-4b5a84be39ad`

Esta política tiene las siguientes opciones:

- TTL mínimo: 0 segundos
- TTL máximo: 0 segundos
- TTL predeterminado: 0 segundos
- Encabezados incluidos en la clave de caché: ninguno
- Cookies incluidas en la clave de caché: ninguna
- Cadenas de consulta incluidas en la clave de caché: ninguna
- Configuración de objetos comprimidos en caché: desactivada

CachingOptimized

Consulte esta política en la consola de CloudFront

Esta política está diseñada para optimizar la eficacia de la caché minimizando los valores que CloudFront incluye en la clave de caché. CloudFront no incluye cadenas de consulta ni cookies en la clave de caché y solo incluye el encabezado `Accept-Encoding` normalizado. Esto permite a CloudFront almacenar en caché objetos por separado en los formatos de compresión Gzip y Brotli cuando el origen los devuelve o cuando se habilita la compresión de borde de CloudFront.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`658327ea-f89d-4fab-a63d-7e88639e58f6`

Esta política tiene las siguientes opciones:

- TTL mínimo: 1 segundo

- TTL máximo: 31 536 000 segundos (365 días)
- TTL predeterminado: 86 400 segundos (24 horas)
- Encabezados incluidos en la clave de caché: no se incluye ninguno de forma explícita. El encabezado `Accept-Encoding` normalizado se incluye porque la configuración de objetos comprimidos en caché está habilitada. Para obtener más información, consulte Compression support (Ayuda para la compresión).
- Cookies incluidas en la clave de caché: ninguna.
- Cadenas de consulta incluidas en la clave de caché: ninguna.
- Configuración de objetos comprimidos en caché: habilitada. Para obtener más información, consulte Compression support (Ayuda para la compresión).

> **Warning**
>
> Dado que esta política tiene un TTL mínimo superior a 0, CloudFront almacenará en caché el contenido durante al menos el tiempo especificado en el TTL mínimo de la política de caché, aunque las directivas `Cache-Control: no-cache`, `no-store` o `private` estén presentes en los encabezados de origen.

CachingOptimizedForUncompressedObjects

Consulte esta política en la consola de CloudFront

Esta política está diseñada para optimizar la eficacia de la caché minimizando los valores incluidos en la clave de caché. No se incluyen cadenas de consulta, encabezados ni cookies. Esta política es idéntica a la anterior, pero desactiva la configuración de objetos comprimidos en caché.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`b2884449-e4de-46a7-ac36-70bc7f1ddd6d`

Esta política tiene las siguientes opciones:

- TTL mínimo: 1 segundo
- TTL máximo: 31 536 000 segundos (365 días)
- TTL predeterminado: 86 400 segundos (24 horas)

- Encabezados incluidos en la clave de caché: ninguno
- Cookies incluidas en la clave de caché: ninguna
- Cadenas de consulta incluidas en la clave de caché: ninguna
- Configuración de objetos comprimidos en caché: desactivada

> **Warning**
>
> Dado que esta política tiene un TTL mínimo superior a 0, CloudFront almacenará en caché el contenido durante al menos el tiempo especificado en el TTL mínimo de la política de caché, aunque las directivas `Cache-Control: no-cache`, `no-store` o `private` estén presentes en los encabezados de origen.

Elemental-MediaPackage

Consulte esta política en la consola de CloudFront

Esta política está diseñada para su uso con un origen que es un punto de enlace de AWS Elemental MediaPackage.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`08627262-05a9-4f76-9ded-b50ca2e3a84f`

Esta política tiene las siguientes opciones:

- TTL mínimo: 0 segundos
- TTL máximo: 31 536 000 segundos (365 días)
- TTL predeterminado: 86 400 segundos (24 horas)
- Encabezados incluidos en la clave de caché:
  - `Origin`

  El encabezado `Accept-Encoding` normalizado también se incluye porque la configuración de objetos comprimidos en caché está habilitada para Gzip. Para obtener más información, consulte Compression support (Ayuda para la compresión).
- Cookies incluidas en la clave de caché: ninguna
- Cadenas de consulta incluidas en la clave de caché:

  - `aws.manifestfilter`
  - `start`
  - `end`
  - `m`
- Configuración de objetos comprimidos en caché: habilitada para Gzip Para obtener más información, consulte Compression support (Ayuda para la compresión).

UseOriginCacheControlHeaders

Consulte esta política en la consola de CloudFront

Esta política está diseñada para usarse con un origen que devuelva encabezados de respuesta `Cache-Control` HTTP y no muestre contenido diferente en función de los valores presentes en la cadena de consulta. Si el origen ofrece contenido en función de los valores de la cadena de consulta, plantéese el uso de UseOriginCacheControlHeaders-QueryStrings.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`83da9c7e-98b4-4e11-a168-04f0df8e2c65`

Esta política tiene las siguientes opciones:

- TTL mínimo: 0 segundos
- TTL máximo: 31 536 000 segundos (365 días)
- TTL predeterminado: 0 segundos
- Encabezados incluidos en la clave de caché:
  - `Host`
  - `Origin`
  - `X-HTTP-Method-Override`
  - `X-HTTP-Method`
  - `X-Method-Override`

  El encabezado `Accept-Encoding` normalizado también se incluye porque la configuración de objetos comprimidos en caché está habilitada. Para obtener más información, consulte Compression support (Ayuda para la compresión).
- Cookies incluidas en la clave de caché: se incluyen todas las cookies.

- Cadenas de consulta incluidas en la clave de caché: ninguna.
- Configuración de objetos comprimidos en caché: habilitada. Para obtener más información, consulte Compression support (Ayuda para la compresión).

UseOriginCacheControlHeaders-QueryStrings

Consulte esta política en la consola de CloudFront

Esta política está diseñada para usarse con un origen que devuelva encabezados de respuesta `Cache-Control` HTTP y muestre contenido diferente en función de los valores presentes en la cadena de consulta. Si el origen no ofrece contenido en función de los valores de la cadena de consulta, plantéese el uso de UseOriginCacheControlHeaders.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`4cc15a8a-d715-48a4-82b8-cc0b614638fe`

Esta política tiene las siguientes opciones:

- TTL mínimo: 0 segundos
- TTL máximo: 31 536 000 segundos (365 días)
- TTL predeterminado: 0 segundos
- Encabezados incluidos en la clave de caché:
  - `Host`
  - `Origin`
  - `X-HTTP-Method-Override`
  - `X-HTTP-Method`
  - `X-Method-Override`

  El encabezado `Accept-Encoding` normalizado también se incluye porque la configuración de objetos comprimidos en caché está habilitada. Para obtener más información, consulte Compression support (Ayuda para la compresión).
- Cookies incluidas en la clave de caché: se incluyen todas las cookies.
- Cadenas de consulta incluidas en la clave de caché: se incluyen todas las cadenas de consulta.
- Configuración de objetos comprimidos en caché: habilitada. Para obtener más información, consulte Compression support (Ayuda para la compresión).

Descripción de la clave de caché

La clave de caché determina si una solicitud del lector a una ubicación de borde de CloudFront da como resultado un acierto de caché. La clave de caché es el identificador único de un objeto en la caché. Cada objeto de la caché tiene una clave de caché única.

Un acierto de caché se produce cuando una solicitud de lector genera la misma clave de caché que una solicitud anterior y el objeto de esa clave de caché está en la caché de la ubicación de borde y es válido. Cuando hay un acierto de caché, el objeto solicitado atiende al lector desde una ubicación de borde de CloudFront, lo que tiene los siguientes beneficios:

- Carga reducida en el servidor de origen
- Latencia reducida para el lector

Puede obtener un mejor rendimiento de su sitio web o aplicación cuando tiene una proporción de aciertos de caché mayor (una mayor proporción de solicitudes de lectores que dan lugar a un acierto de caché). Una forma de mejorar la proporción de aciertos de caché es incluir solo los valores mínimos necesarios en la clave de caché. Para obtener más información, consulte las siguientes secciones.

Puede modificar los valores (cadenas de consulta de URL, encabezados HTTP y cookies) en la clave de caché mediante una política de caché. (También puede modificar la clave de caché mediante una función de Lambda@Edge o una función de CloudFront cuando lo solicite un espectador). Antes de modificar la clave de caché, es importante comprender cómo se diseña la aplicación y cuándo y cómo es posible que sirva diferentes respuestas en función de las características de la solicitud del lector. Cuando un valor de la solicitud del lector determina la respuesta que devuelve el origen, debe incluir ese valor en la clave de caché. Pero si incluye un valor en la clave de caché que no afecta a la respuesta que devuelve su origen, es posible que termine almacenando en caché objetos duplicados.

Clave de caché predeterminada

De forma predeterminada, la clave de caché de una distribución de CloudFront incluye la siguiente información:

- El nombre de dominio de la distribución de CloudFront (por ejemplo, d111111abcdef8.cloudfront.net)
- La ruta URL del objeto solicitado (por ejemplo, `/content/stories/example-story.html`)

> **Note**
>
> El método `OPTIONS` se incluye en la clave de caché para solicitudes `OPTIONS`. Esto significa que las respuestas a las solicitudes `OPTIONS` se almacenan en caché por separado de las respuestas a solicitudes `GET` y `HEAD`.

Otros valores de la solicitud del lector no se incluyen en la clave de caché, de forma predeterminada. Considere la siguiente solicitud HTTP desde un navegador 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/
```

Cuando una solicitud de lector como la de este ejemplo entra en una ubicación periférica de CloudFront, CloudFront usa la clave de caché para determinar si hay un acierto de caché. De forma predeterminada, solo los siguientes componentes de la solicitud se incluyen en la clave de caché: `/content/stories/example-story.html` y `d111111abcdef8.cloudfront.net`. Si el objeto solicitado no está en la caché (un error de caché), CloudFront envía una solicitud al origen para obtener el objeto. Después de obtener el objeto, CloudFront lo devuelve al lector y lo almacena en la caché de la ubicación de borde.

Cuando CloudFront recibe otra solicitud para el mismo objeto, según lo determinado por la clave de caché, CloudFront sirve el objeto almacenado en caché al lector inmediatamente, sin enviar una solicitud al origen. Por ejemplo, considere la siguiente solicitud HTTP que aparece después de la solicitud anterior.

```
            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/
```

Esta solicitud es para el mismo objeto que la solicitud anterior, pero es diferente de la solicitud anterior. Tiene una cadena de consulta de URL diferente, encabezados `User-Agent` y `Referer` diferentes y una cookie de `session_id` diferente. Sin embargo, ninguno de estos valores forma parte de la clave de caché de forma predeterminada, por lo que esta segunda solicitud da como resultado un acierto de caché.

Personalización de la clave de caché

En algunos casos, es posible que desee incluir más información en la clave de caché, aunque al hacerlo es posible que dé como resultado menos aciertos de la caché. Se especifica qué incluir en la clave de caché mediante una política de caché.

Por ejemplo, si el servidor de origen utiliza el encabezado HTTP `Accept-Language` en las solicitudes del lector para devolver contenido diferente en función del idioma del lector, es posible que desee incluir este encabezado en la clave de caché. Al hacerlo, CloudFront utiliza este encabezado para determinar los aciertos de caché e incluye el encabezado en solicitudes de origen (solicitudes que CloudFront envía al origen cuando hay un error de caché).

Una consecuencia potencial de incluir valores adicionales en la clave de caché es que es posible que CloudFront termine almacenando en caché objetos duplicados debido a la variación que puede ocurrir en las solicitudes del lector. Por ejemplo, es posible que los lectores puedan enviar cualquiera de los siguientes valores para el encabezado `Accept-Language`:

- `en-US,en`
- `en,en-US`
- `en-US, en`
- `en-US`

Todos estos valores diferentes indican que el idioma del lector es el inglés, pero la variación puede hacer que CloudFront almacene en caché el mismo objeto varias veces. Esto puede reducir los aciertos de caché y aumentar el número de solicitudes de origen. Se puede evitar esta duplicación si no se incluye el encabezado `Accept-Language` en la clave de caché y, en su lugar, se configura

su sitio web o aplicación para utilizar diferentes URL para el contenido en diferentes idiomas (por ejemplo, `/en-US/content/stories/example-story.html`).

Para cualquier valor dado que se pretenda incluir en la clave de caché, se debe estar seguro de comprender cuántas variaciones diferentes de ese valor es posible que aparezcan en las solicitudes del lector. Para ciertos valores de solicitud, rara vez tiene sentido incluirlos en la clave de caché. Por ejemplo, el encabezado `User-Agent` puede tener miles de variaciones únicas, por lo que generalmente no es un buen candidato para incluirlo en la clave de caché. Las cookies que tienen valores específicos del usuario o específicos de la sesión y son únicas en miles (o incluso millones) de solicitudes tampoco son buenos candidatos para la inclusión de claves de caché. Si incluye estos valores en la clave de caché, cada variación única da como resultado otra copia del objeto en la caché. Si estas copias del objeto no son únicas o si termina con un número tan grande de objetos ligeramente diferentes que cada objeto solo obtiene un pequeño número de aciertos de caché, es posible que desee considerar un enfoque diferente. Puede excluir estos valores altamente variables de la clave de caché o puede marcar objetos como no almacenables en caché.

Tenga cuidado al personalizar la clave de caché. A veces es deseable, pero puede tener consecuencias no deseadas como almacenar en caché objetos duplicados, reducir la proporción de aciertos de caché y aumentar el número de solicitudes de origen. Si su sitio web o aplicación de origen necesita recibir ciertos valores de las solicitudes del lector para análisis, telemetría u otros usos, pero estos valores no cambian el objeto que devuelve el origen, utilice una política de solicitud de origen para incluir estos valores en las solicitudes de origen pero no incluirlos en la clave de caché.

Control de las solicitudes de origen con una política

Cuando una solicitud de lector en CloudFront da como resultado un error de caché (el objeto solicitado no se almacena en caché en la ubicación de borde), CloudFront envía una solicitud al origen para recuperar el objeto. Esto se denomina una solicitud de origen. La solicitud de origen siempre incluye la siguiente información de la solicitud del lector:

- La ruta de URL (solo la ruta, sin cadenas de consulta de URL ni el nombre de dominio)
- El cuerpo de la solicitud (si hay uno)
- Los encabezados HTTP que CloudFront incluye automáticamente en cada solicitud de origen, incluidos `Host`, `User-Agent` y `X-Amz-Cf-Id`

Otra información de la solicitud del lector, como cadenas de consulta de URL, encabezados HTTP y cookies, no se incluye en la solicitud de origen de forma predeterminada. (Excepción: con la configuración de caché heredada, CloudFront reenvía los encabezados a su origen de forma predeterminada). Sin embargo, es posible que desee recibir parte de esta otra información en el origen, por ejemplo, para recopilar datos para análisis o telemetría. Puede utilizar una política de solicitud de origen para controlar la información que se incluye en una solicitud de origen.

Las políticas de solicitud de origen son independientes de las políticas de caché, que controlan la clave de caché. De este modo, puede recibir información adicional en el origen y también mantener una buena proporción de aciertos de la caché (la proporción de solicitudes de lector que dan lugar a un acierto de la caché). Para ello, controle por separado qué información se incluye en las solicitudes de origen (mediante la política de solicitud de origen) y cuál se incluye en la clave de caché (mediante la política de caché).

Aunque los dos tipos de políticas son independientes, están relacionadas. Todas las cadenas de consulta de URL, encabezados HTTP y cookies que se incluyen en la clave de caché (mediante una política de caché) se incluyen automáticamente en las solicitudes de origen. Utilice la política de solicitud de origen para especificar la información que desea incluir en las solicitudes de origen, pero no en la clave de caché. Al igual que una política de caché, puede asociar una política de solicitud de origen a uno o más comportamientos de caché de una distribución de CloudFront.

También puede utilizar una política de solicitud de origen para agregar encabezados HTTP adicionales a una solicitud de origen que no se incluyeron en la solicitud del lector. CloudFront agrega estos encabezados adicionales antes de enviar la solicitud de origen, con valores de

encabezado que se determinan automáticamente en función de la solicitud del lector. Para obtener más información, consulte the section called “Añadido de encabezados de solicitudes de CloudFront”.

Temas

- Descripción de políticas de solicitud de origen
- Creación de políticas de solicitud de origen
- Uso de políticas de solicitudes de origen administradas
- Añadido de encabezados de solicitudes de CloudFront
- Descripción de cómo funcionan juntas las políticas de solicitud de origen y las políticas de caché

Descripción de políticas de solicitud de origen

CloudFront proporciona algunas políticas de solicitud de origen predefinidas, conocidas como políticas administradas, para casos de uso comunes. Puede usar estas políticas administradas o puede crear su propia política de solicitud de origen específica para sus necesidades. Para obtener más información sobre las políticas administradas, consulte Uso de políticas de solicitudes de origen administradas.

Una política de solicitud de origen contiene la siguiente configuración, que se clasifica en información de política y configuración de solicitud de origen.

Información de políticas

Nombre

Un nombre para identificar la política de solicitud de origen. En la consola, se utiliza el nombre para asociar la política de solicitud de origen a un comportamiento de caché.

Descripción

Un comentario para describir la política de solicitud de origen. Esto es opcional.

Configuración de solicitud de origen

La configuración de la solicitud de origen especifica los valores de las solicitudes de lector que se incluyen en las solicitudes que CloudFront envía al origen (conocidas como solicitudes de origen).

Los valores pueden incluir cadenas de consulta de URL, encabezados HTTP y cookies. Los valores que especifique se incluyen en las solicitudes de origen, pero no se incluyen en la clave de caché. Para obtener información sobre cómo controlar la clave de caché, consulte Control de la clave de caché con una política.

Encabezados

Los encabezados HTTP en las solicitudes del lector que CloudFront incluye en solicitudes de origen. En encabezados, puede elegir una de las siguientes configuraciones:

- None (Ninguna): los encabezados HTTP en las solicitudes de lector no se incluyen en solicitudes de origen.
- Todos los encabezados del lector: todos los encabezados HTTP de las solicitudes de lector se incluyen en las solicitudes de origen.
- Todos los encabezados del lector y los siguientes encabezados de CloudFront: todos los encabezados HTTP de las solicitudes de lector se incluyen en las solicitudes de origen. Además, se especifica cuál de los encabezados de CloudFront se desea agregar a las solicitudes de origen. Para obtener más información acerca de los encabezados de CloudFront, consulte the section called “Añadido de encabezados de solicitudes de CloudFront”.
- Incluir los siguientes encabezados: esta opción le permite especificar los encabezados HTTP que se incluyen en solicitudes de origen.

> **Note**
>
> No especifique ningún encabezado que ya esté incluido en la configuración de Encabezados personalizados de origen. Para obtener más información, consulte Configuración de CloudFront para agregar encabezados personalizados a solicitudes de origen.

- Todos los encabezados del lector excepto: usted especifica qué encabezados HTTP no se incluyen en las solicitudes de origen. Se incluyen todos los demás encabezados HTTP de las solicitudes del lector, excepto los especificados.

Cuando se utiliza la configuración Todos los encabezados del lector y los encabezados de CloudFront siguientes, Incluir los siguientes encabezados o Todos los encabezados del lector excepto, se especifican los encabezados HTTP solo por el nombre del encabezado. CloudFront incluye el encabezado completo, incluido su valor, en las solicitudes de origen.

> **Note**
>
> Al utilizar la configuración Todos los encabezados del visor excepto para eliminar el encabezado `Host` del lector, CloudFront agrega un nuevo encabezado `Host` con el nombre de dominio del origen a la solicitud de origen.

Cookies

Las cookies en las solicitudes del lector que CloudFront incluye en solicitudes de origen. Para cookies, puede elegir una de las siguientes configuraciones:

- None (Ninguna): las cookies en las solicitudes de lector no están incluidas en las solicitudes de origen.
- Todas: las cookies en las solicitudes de lector se incluyen en las solicitudes de origen.
- Incluir las siguientes cookies: se especifica qué cookies de las solicitudes de lector se incluyen en las solicitudes de origen.
- Todas las cookies excepto: puede especificar qué cookies en las solicitudes de lector no están incluidas en las solicitudes de origen. Se incluyen todas las demás cookies de las solicitudes del lector.

Cuando utiliza la configuración Incluir las cookies siguientes o Todas las cookies excepto, se especifican las cookies solo por el nombre. CloudFront incluye la cookie completa, incluido su valor, en las solicitudes de origen.

Cadenas de consulta

Las cadenas de consulta de URL en las solicitudes de lector que CloudFront incluye en las solicitudes de origen. Para cadenas de consulta, puede elegir una de las opciones siguientes:

- None (Ninguna): las cadenas de consulta en las solicitudes de lector no se incluyen en las solicitudes de origen.
- Todas: todas las cadenas de consulta de las solicitudes de lector se incluyen en las solicitudes de origen.
- Incluir cadenas de consulta especificadas: se especifica qué cadenas de consulta de las solicitudes de lector se incluyen en las solicitudes de origen.
- Todas las cadenas de consulta excepto: puede especificar qué cadenas de consulta de las solicitudes de lector no están incluidas en las solicitudes de origen. Se incluyen todas las demás cadenas de consulta.

Cuando se utiliza la configuración Incluir las cadenas de consulta siguientes o Todas las cadenas de consulta excepto, se especifican cadenas de consulta solo por el nombre. CloudFront incluye la cadena de consulta completa, incluido su valor, en las solicitudes de origen.

Creación de políticas de solicitud de origen

Puede utilizar una política de solicitud de origen para controlar los valores (cadenas de consulta de URL, encabezados HTTP y cookies) que se incluyen en las solicitudes que CloudFront envía al origen. Puede crear una política de solicitud de origen en la consola de CloudFront, con la AWS Command Line Interface (AWS CLI) o con la API de CloudFront.

Después de crear una política de solicitud de origen, puede asociarla a uno o más comportamientos de caché en una distribución de CloudFront.

Las políticas de solicitud de origen no son obligatorias. Cuando un comportamiento de caché no tiene una política de solicitud de origen asociada, la solicitud de origen incluye todos los valores especificados en la política de caché, pero nada más.

> **Note**
>
> Para utilizar una política de solicitud de origen, el comportamiento de caché también debe utilizar una política de caché. No se puede utilizar una política de solicitud de origen en un comportamiento de caché sin una política de caché.

Console

Para crear una política de solicitud de origen (consola)

1. Inicie sesión en Consola de administración de AWS y abra la página Policies (Políticas) en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home?#/policies.
2. Elija Origin request (Solicitud de origen) y, luego, Create origin request policy (Crear política de solicitud de origen).
3. Elija la configuración deseada para esta política de solicitud de origen. Para obtener más información, consulte Descripción de políticas de solicitud de origen.
4. Cuando termine, elija Create (Crear).

Después de crear una política de solicitud de origen, puede asociarla a un comportamiento de caché.

Para asociar una política de solicitud de origen a una distribución existente (consola)

1. Abra la página Distributions (Distribuciones) en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Elija la distribución que se va a actualizar y, a continuación, elija la pestaña Behaviors (Comportamientos).
3. Elija el comportamiento de caché que se va a actualizar y, a continuación, elija Edit (Editar).

   O bien, para crear un nuevo comportamiento de caché, elija Create behavior (Crear comportamiento).
4. En la sección Cache key and origin requests (Solicitudes de origen y clave de caché), asegúrese de elegir Cache policy and origin request policy (Política de caché y política de solicitud de origen).
5. En Origin request policy (Política de solicitud de origen), elija la política de solicitud de origen que se va a asociar a este comportamiento de caché.
6. Elija Save changes (Guardar cambios) en la parte inferior de la página.

Para asociar una política de solicitud de origen con una nueva distribución (consola)

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Create distribution (Crear distribución).
3. En la sección Solicitudes de origen y clave de caché, asegúrese de elegir Política de caché y política de solicitud de origen.
4. En Origin request policy (Política de solicitud de origen), elija la política de solicitud de origen que se va a asociar al comportamiento predeterminado de la caché de esta distribución.
5. Elija la configuración deseada para el origen, el comportamiento predeterminado de la caché y la distribución. Para obtener más información, consulte Referencia de toda la configuración de distribución.
6. Cuando termine, elija Create distribution (Crear distribución).

CLI

Para crear una política de solicitud de origen con la AWS Command Line Interface (AWS CLI), utilice el comando aws cloudfront create-origin-request-policy. Puede utilizar un archivo de entrada para proporcionar los parámetros de entrada del comando, en lugar de especificar cada parámetro individual como entrada de línea de comandos.

Para crear una política de solicitud de origen (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo denominado `origin-request-policy.yaml` que contenga todos los parámetros de entrada del comando create-origin-request-policy.

   ```
   aws cloudfront create-origin-request-policy --generate-cli-skeleton yaml-input >
    origin-request-policy.yaml
   ```

2. Abra el archivo llamado `origin-request-policy.yaml` que acaba de crear. Edite el archivo para especificar la configuración de política de solicitud de origen que desee y, a continuación, guarde el archivo. Puede eliminar campos opcionales del archivo, pero no eliminar los campos obligatorios.

   Para obtener más información acerca de la configuración de política de solicitud de origen, consulte Descripción de políticas de solicitud de origen.

3. Utilice el siguiente comando para crear la política de solicitud de origen utilizando parámetros de entrada del archivo de `origin-request-policy.yaml`.

   ```
   aws cloudfront create-origin-request-policy --cli-input-yaml file://origin-
   request-policy.yaml
   ```

   Anote el valor de `Id` en la salida del comando. Este es el ID de política de solicitud de origen y se necesita para asociar la política de solicitud de origen al comportamiento de caché de una distribución de CloudFront.

Para asociar una política de solicitud de origen a una distribución existente (CLI con archivo de entrada)

1. Utilice el comando siguiente para guardar la configuración de distribución de la distribución de CloudFront que desea actualizar. Reemplace *distribution_ID* por el ID de la distribución.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Abra el archivo llamado `dist-config.yaml` que acaba de crear. Edite el archivo, realizando los siguientes cambios en cada comportamiento de caché que actualice para utilizar una política de solicitud de origen.

   - En el comportamiento de caché, agregue un campo denominado `OriginRequestPolicyId`. Para el valor del campo, utilice el ID de política de solicitud de origen que anotó después de crear la política.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución para utilizar la política de solicitud de origen. Reemplace *distribution_ID* por el ID de la distribución.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Para asociar una política de solicitud de origen a una distribución nueva (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo denominado `distribution.yaml` que contenga todos los parámetros de entrada del comando create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Abra el archivo llamado `distribution.yaml` que acaba de crear. En el comportamiento de caché predeterminado, en el campo `OriginRequestPolicyId`, escriba el ID de política de solicitud de origen que anotó después de crear la política. Siga editando el archivo para especificar la configuración de distribución que desee y, a continuación, guarde el archivo cuando termine.

   Para obtener más información acerca de la configuración de distribución, consulte Referencia de toda la configuración de distribución.

3. Utilice el siguiente comando para crear la distribución mediante los parámetros de entrada del archivo de `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Para crear una política de solicitud de origen con la API de CloudFront, utilice CreateOriginRequestPolicy. Para obtener más información sobre los campos que especifique en esta llamada a la API, consulte Descripción de políticas de solicitud de origen y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Después de crear una política de solicitud de origen, puede asociarla a un comportamiento de caché mediante una de las siguientes llamadas a la API:

- Para asociarla a un comportamiento de caché en una distribución existente, utilice UpdateDistribution.
- Para asociarlo con un comportamiento de caché en una nueva distribución, utilice CreateDistribution.

Para estas llamadas a la API, proporcione el ID de la política de solicitud de origen en el campo `OriginRequestPolicyId`, dentro de un comportamiento de caché. Para obtener más información sobre los otros campos que especifique en estas llamadas a la API, consulte Referencia de toda la configuración de distribución y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Uso de políticas de solicitudes de origen administradas

CloudFront proporciona un conjunto de políticas de solicitud de origen administradas que puede asociar a cualquiera de los comportamientos de caché de la distribución. Con una política de solicitud de origen administrada, no es necesario escribir ni mantener su propia política de solicitud de origen. Las políticas administradas utilizan configuraciones optimizadas para casos de uso específicos.

Para utilizar una política de solicitud de origen administrada, debe asociarla a un comportamiento de caché en su distribución. El proceso es el mismo que cuando se crea una política de solicitud de origen, pero en lugar de crear una nueva, simplemente se asocia una de las políticas de solicitud de origen administradas. Se asocia la política por nombre (con la consola) o por ID (con AWS CLI o los SDK). Los nombres e ID se muestran en la siguiente sección.

Para obtener más información, consulte Creación de políticas de solicitud de origen.

En los temas siguientes, se describen las políticas de solicitudes de origen administradas que puede utilizar.

Temas

- AllViewer
- AllViewerAndCloudFrontHeaders-2022-06
- AllViewerExceptHostHeader
- CORS-CustomOrigin
- CORS-S3Origin
- Elemental-MediaTailor-PersonalizedManifests
- HostHeaderOnly
- UserAgentRefererHeaders

AllViewer

Consulte esta política en la consola de CloudFront

En esta política, se incluyen todos los valores (cadenas de consulta, encabezados y cookies) de la solicitud del lector.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`216adef6-5c7f-47e4-b989-5492eafa07d3`

Esta política tiene las siguientes opciones:

- Encabezados incluidos en las solicitudes de origen: todos los encabezados de la solicitud del lector
- Cookies incluidas en las solicitudes de origen: todas
- Cadenas de consulta incluidas en las solicitudes de origen: todas

AllViewerAndCloudFrontHeaders-2022-06

Consulte esta política en la consola de CloudFront

En esta política, se incluyen todos los valores (encabezados, cookies y cadenas de consulta) de la solicitud del lector y todos los encabezados de CloudFront que se publicaron hasta junio de 2022 (no se incluyen los encabezados de CloudFront que se hayan publicado después de junio de 2022).

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`33f36d7e-f396-46d9-90e0-52428a34d9dc`

Esta política tiene las siguientes opciones:

- Encabezados incluidos en las solicitudes de origen: todos los encabezados de la solicitud del lector y los siguientes encabezados de CloudFront:
  - `CloudFront-Forwarded-Proto`
  - `CloudFront-Is-Android-Viewer`
  - `CloudFront-Is-Desktop-Viewer`
  - `CloudFront-Is-IOS-Viewer`
  - `CloudFront-Is-Mobile-Viewer`
  - `CloudFront-Is-SmartTV-Viewer`
  - `CloudFront-Is-Tablet-Viewer`
  - `CloudFront-Viewer-Address`
  - `CloudFront-Viewer-ASN`
  - `CloudFront-Viewer-City`
  - `CloudFront-Viewer-Country`

- `CloudFront-Viewer-Country-Name`
- `CloudFront-Viewer-Country-Region`
- `CloudFront-Viewer-Country-Region-Name`
- `CloudFront-Viewer-Http-Version`
- `CloudFront-Viewer-Latitude`
- `CloudFront-Viewer-Longitude`
- `CloudFront-Viewer-Metro-Code`
- `CloudFront-Viewer-Postal-Code`
- `CloudFront-Viewer-Time-Zone`
- `CloudFront-Viewer-TLS`

- Cookies incluidas en las solicitudes de origen: todas
- Cadenas de consulta incluidas en las solicitudes de origen: todas

AllViewerExceptHostHeader

Consulte esta política en la consola de CloudFront

Esta política no incluye el encabezado `Host` de la solicitud del lector, pero sí incluye todos los demás valores (encabezados, cookies y cadenas de consulta) de la solicitud del lector.

Esta política también incluye encabezados de solicitud de CloudFront adicionales para el protocolo HTTP, la versión HTTP, la versión TLS y todos los encabezados de tipo de dispositivo y ubicación del lector.

Esta política está diseñada para usarse con los orígenes de URL de función de Amazon API Gateway y AWS Lambda. Estos orígenes esperan que el encabezado `Host` contenga el nombre de dominio de origen, no el nombre de dominio de la distribución de CloudFront. Reenviar el encabezado `Host` de la solicitud del lector a estos orígenes puede impedir que funcionen.

> **Note**
>
> Al utilizar esta política de solicitud de origen administrada para eliminar el encabezado `Host` del lector, CloudFront agrega un nuevo encabezado `Host` con el nombre de dominio del origen a la solicitud de origen.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`b689b0a8-53d0-40ab-baf2-68738e2966ac`

Esta política tiene las siguientes opciones:

- Encabezados incluidos en las solicitudes de origen: todos los encabezados de la solicitud del lector excepto para el encabezado de `Host`
- Cookies incluidas en las solicitudes de origen: todas
- Cadenas de consulta incluidas en las solicitudes de origen: todas

CORS-CustomOrigin

Consulte esta política en la consola de CloudFront

Esta política incluye el encabezado que habilita las solicitudes de uso compartido de recursos de origen cruzado (CORS) cuando el origen es un origen personalizado.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`59781a5b-3903-41f3-afcb-af62929ccde1`

Esta política tiene las siguientes opciones:

- Encabezados incluidos en las solicitudes de origen:
  - `Origin`
- Cookies incluidas en las solicitudes de origen: ninguna
- Cadenas de consulta incluidas en las solicitudes de origen: ninguna

CORS-S3Origin

Consulte esta política en la consola de CloudFront

Esta política incluye los encabezados que habilitan las solicitudes de uso compartido de recursos de origen cruzado (CORS) cuando el origen es un bucket de Amazon S3.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`88a5eaf4-2fd4-4709-b370-b4c650ea3fcf`

Esta política tiene las siguientes opciones:

- Encabezados incluidos en las solicitudes de origen:
  - `Origin`
  - `Access-Control-Request-Headers`
  - `Access-Control-Request-Method`
- Cookies incluidas en las solicitudes de origen: ninguna
- Cadenas de consulta incluidas en las solicitudes de origen: ninguna

Elemental-MediaTailor-PersonalizedManifests

Consulte esta política en la consola de CloudFront

Esta política está diseñada para su uso con un origen que es un punto de conexión de AWS Elemental MediaTailor.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`775133bc-15f2-49f9-abea-afb2e0bf67d2`

Esta política tiene las siguientes opciones:

- Encabezados incluidos en las solicitudes de origen:
  - `Origin`
  - `Access-Control-Request-Headers`
  - `Access-Control-Request-Method`
  - `User-Agent`
  - `X-Forwarded-For`
- Cookies incluidas en las solicitudes de origen: ninguna
- Cadenas de consulta incluidas en las solicitudes de origen: todas

HostHeaderOnly

Consulte esta política en la consola de CloudFront

Esta política incluye solo el encabezado del `Host` de la solicitud de origen. No incluye cadenas de consulta ni cookies.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`bf0718e1-ba1e-49d1-88b1-f726733018ae`

Esta política tiene las siguientes opciones:

- Encabezados incluidos en las solicitudes de origen: host
- Cookies incluidas en las solicitudes de origen: ninguna
- Cadenas de consulta incluidas en las solicitudes de origen: ninguna

UserAgentRefererHeaders

Consulte esta política en la consola de CloudFront

Esta política incluye solo los encabezados `User-Agent` y `Referer`. No incluye cadenas de consulta ni cookies.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`acba4595-bd28-49b8-b9fe-13317c0390fa`

Esta política tiene las siguientes opciones:

- Encabezados incluidos en las solicitudes de origen:
  - `User-Agent`
  - `Referer`
- Cookies incluidas en las solicitudes de origen: ninguna
- Cadenas de consulta incluidas en las solicitudes de origen: ninguna

Añadido de encabezados de solicitudes de CloudFront

Puede configurar CloudFront para añadir encabezados HTTP específicos a las solicitudes que CloudFront recibe de los lectores y reenvía a su función de origen o función perimetral. Los valores de estos encabezados HTTP se basan en las características del lector o de la solicitud del lector.

Los encabezados proporcionan información sobre el tipo de dispositivo del lector, la dirección IP, la ubicación geográfica, el protocolo de solicitud (HTTP o HTTPS), la versión de HTTP, los detalles de conexión TLS, la huella digital JA3 y la huella digital JA4. También puede configurar el comportamiento de caché de la distribución para reenviar encabezados de WebSocket. Para obtener más información, consulte Uso de WebSockets con distribuciones de CloudFront.

Con estos encabezados, su origen o su función periférica pueden recibir información sobre el lector sin necesidad de escribir su propio código para determinar esta información. Si su origen devuelve respuestas diferentes en función de la información de estos encabezados, puede incluirlas en la clave de caché para que CloudFront almacene en caché las respuestas por separado. Por ejemplo, su origen podría responder con contenido en un idioma específico según el país en el que se encuentre el lector, o con contenido adaptado a un tipo de dispositivo específico. Es posible que su origen también escriba estos encabezados en archivos de registro, que puede utilizar para determinar la información sobre dónde se encuentran sus lectores, en qué tipos de dispositivos se encuentran y mucho más.

Para incluir estos encabezados en la clave de caché, utilice una política de caché. Para obtener más información, consulte Control de la clave de caché con una política y the section called “Descripción de la clave de caché”.

Para recibir estos encabezados en el origen, pero sin incluirlos en la clave de caché, utilice una política de solicitud de origen. Para obtener más información, consulte Control de las solicitudes de origen con una política.

Temas

- Encabezados de tipo de dispositivo
- Encabezados de ubicación del espectador
- Encabezados para determinar la estructura de los encabezados del espectador
- Encabezados relacionados con TLS
- Otros encabezados de CloudFront

Encabezados de tipo de dispositivo

Puede agregar los siguientes encabezados para determinar el tipo de dispositivo del espectador. En función del valor del encabezado `User-Agent`, CloudFront establece el valor de estos encabezados en `true` o `false`. Si un dispositivo entra en más de una categoría, más de un valor puede ser `true`.

Por ejemplo, en el caso de algunas tabletas, CloudFront establece tanto `CloudFront-Is-Mobile-Viewer` como `CloudFront-Is-Tablet-Viewer` en `true`.

- `CloudFront-Is-Android-Viewer`: se establece en `true` cuando CloudFront determina que el lector es un dispositivo con el sistema operativo Android.
- `CloudFront-Is-Desktop-Viewer`: se establece en `true` cuando CloudFront determina que el lector es un dispositivo de sobremesa.
- `CloudFront-Is-IOS-Viewer`: se establece en `true` cuando CloudFront determina que el lector es un dispositivo con un sistema operativo móvil de Apple, como un iPhone, un iPod touch y algunos dispositivos iPad.
- `CloudFront-Is-Mobile-Viewer`: se establece en `true` cuando CloudFront determina que el lector es un dispositivo móvil.
- `CloudFront-Is-SmartTV-Viewer`: se establece en `true` cuando CloudFront determina que el lector es una TV inteligente.
- `CloudFront-Is-Tablet-Viewer`: se establece en `true` cuando CloudFront determina que el lector es una tableta.

Encabezados de ubicación del espectador

Puede agregar los siguientes encabezados para determinar la ubicación del espectador. CloudFront determina los valores de estos encabezados en función de la dirección IP del espectador. Para los caracteres no ASCII en los valores de estos encabezados, CloudFront aplica la codificación de porcentaje de acuerdo con la sección 1.2 de RFC 3986.

- `CloudFront-Viewer-Address`: contiene la dirección IP del espectador y el puerto de origen de la solicitud. Por ejemplo, un valor de encabezado de `198.51.100.10:46532` significa que la dirección IP del espectador es 198.51.100.10 y el puerto de origen de solicitud es 46532.
- `CloudFront-Viewer-ASN`: contiene el número de sistema autónomo (ASN) del espectador.

> **Note**
>
> Se puede agregar `CloudFront-Viewer-Address` y `CloudFront-Viewer-ASN` en una política de solicitud de origen, pero no en una política de caché.

- `CloudFront-Viewer-Country`: contiene el código de país de dos letras del país del espectador. Para obtener una lista de códigos de países, consulte ISO 3166-1 alpha-2.

- `CloudFront-Viewer-City`: contiene el nombre de la ciudad del espectador.

Cuando agrega los siguientes encabezados, CloudFront los aplica a todas las solicitudes excepto aquellas que se originan en la red de AWS:

- `CloudFront-Viewer-Country-Name`: contiene el nombre del país del espectador.
- `CloudFront-Viewer-Country-Region`: contiene un código (hasta tres caracteres) que representa la región del espectador. La región es la subdivisión de primer nivel (la más amplia o menos específica) del código ISO 3166-2.
- `CloudFront-Viewer-Country-Region-Name`: contiene el nombre de la región del espectador. La región es la subdivisión de primer nivel (la más amplia o menos específica) del código ISO 3166-2.
- `CloudFront-Viewer-Latitude`: contiene la latitud aproximada del espectador.
- `CloudFront-Viewer-Longitude`: contiene la longitud aproximada del espectador.
- `CloudFront-Viewer-Metro-Code`: contiene el código del área metropolitana del espectador. Esto solo está presente cuando el lector se encuentra en los Estados Unidos.
- `CloudFront-Viewer-Postal-Code`: contiene el código postal del espectador.
- `CloudFront-Viewer-Time-Zone` contiene la zona horaria del espectador, en formato de base de datos de zona horaria de IANA (por ejemplo, `America/Los_Angeles`).

> **Note**
>
> Es posible que `CloudFront-Viewer-City`, `CloudFront-Viewer-Metro-Code` y `CloudFront-Viewer-Postal-Code` no estén disponibles para todas las direcciones IP. Algunas direcciones IP no pueden geolocalizarse con la suficiente especificidad como para obtener esa información.

Encabezados para determinar la estructura de los encabezados del espectador

Puede añadir los siguientes encabezados para ayudar a identificar al lector en función de los encabezados que envía. Por ejemplo, diferentes navegadores pueden enviar encabezados HTTP en un orden determinado. Si el navegador especificado en el encabezado `User-Agent` no coincide

con el orden esperado de los encabezados de ese navegador, puede denegar la solicitud. Además, si el valor de `CloudFront-Viewer-Header-Count` no coincide con el número de encabezados de `CloudFront-Viewer-Header-Order`, puede denegar la solicitud.

- `CloudFront-Viewer-Header-Order`: contiene los nombres de los encabezados del lector en el orden solicitado, separados por dos puntos. Por ejemplo: `CloudFront-Viewer-Header-Order: Host:User-Agent:Accept:Accept-Encoding`. Los encabezados que superen el límite de 7680 caracteres se truncan.
- `CloudFront-Viewer-Header-Count`: contiene el número total de encabezados del lector.

Encabezados relacionados con TLS

Puede añadir los siguientes encabezados para determinar la huella digital de JA3, la huella digital de JA4 y los detalles de la conexión TLS del espectador:

- `CloudFront-Viewer-JA3-Fingerprint`: contiene la huella digital JA3 del lector. La huella digital JA3 puede ayudarle a determinar si la solicitud proviene de un cliente conocido, si se trata de malware o un bot malintencionado, o es una aplicación esperada (incluida en la lista de permitidos).
- `CloudFront-Viewer-JA4-Fingerprint`: contiene la huella digital JA4 del espectador. Similar a la huella digital JA3, la huella digital JA4 puede ayudarlo a determinar si la solicitud proviene de un cliente conocido, si se trata de malware o un bot malintencionado, o es una aplicación esperada (incluida en la lista de permitidos). Puede usar la huella digital para crear una base de datos con los agentes buenos y malos conocidos para usarlos al inspeccionar las solicitudes HTTP. A continuación, puede inspeccionar el valor del encabezado en los servidores web de la aplicación o en Lambda@Edge y CloudFront Functions para comparar el valor del encabezado con una lista de huellas digitales de malware conocidas para bloquear los clientes malintencionados.
- `CloudFront-Viewer-TLS`: contiene la versión de SSL/TLS, el cifrado e información acerca del protocolo de enlace SSL/TLS que se ha utilizado para la conexión entre el lector y CloudFront. El valor del encabezado tiene el siguiente formato:

  ```
  SSL/TLS_version:cipher:handshake_information
  ```

  En *`handshake_information`*, el encabezado puede contener uno de los siguientes valores:

  - `fullHandshake`: se aceptó correctamente el protocolo de enlace para la sesión de SSL/TLS.
  - `sessionResumed`: se reanudó una sesión SSL/TLS anterior.

- `connectionReused`: se ha reutilizado una conexión SSL/TLS anterior.

A continuación, se muestran algunos valores de ejemplo para este encabezado:

```
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
```

Para obtener la lista completa de las posibles versiones y cifrados de SSL/TLS que pueden estar en este valor de encabezado, consulte the section called “Protocolos y cifrados admitidos entre lectores y CloudFront”.

> **Notas**
>
> - Las huellas digitales JA3 y JA4 se derivan del paquete SSL/TLS `Client Hello`. Solo están presentes para las solicitudes HTTPS.
> - Para estos encabezados relacionados con TLS, puede agregarlos a una política de solicitud de origen, pero no a una política de caché.

Otros encabezados de CloudFront

Puede agregar los siguientes encabezados para determinar el URI de la solicitud original del espectador, los parámetros y valores de la cadena de consulta de la solicitud original, el protocolo, la versión:

- `CloudFront-Error-Uri`: contiene el URI de la solicitud original que se recibió del lector.
- `CloudFront-Error-Args`: contiene los parámetros y valores de la cadena de consulta de la solicitud original.
- `CloudFront-Forwarded-Proto`: contiene el protocolo de la solicitud del espectador (HTTP o HTTPS).

- `CloudFront-Viewer-Http-Version`: contiene la versión HTTP de la solicitud del espectador.

Descripción de cómo funcionan juntas las políticas de solicitud de origen y las políticas de caché

Puede usar una política de solicitud de origen de CloudFront para controlar las solicitudes que CloudFront envía al origen, que se denominan solicitudes de origen. Para utilizar una política de solicitud de origen, debe asociar una política de caché al mismo comportamiento de caché. No se puede utilizar una política de solicitud de origen en un comportamiento de caché sin una política de caché. Para obtener más información, consulte Control de las solicitudes de origen con una política.

Las políticas de solicitud de origen y las políticas de caché funcionan en conjunto para determinar los valores que CloudFront incluye en las solicitudes de origen. Todas las cadenas de consulta de URL, encabezados HTTP y cookies que especifique en la clave de caché (mediante una política de caché) se incluyen automáticamente en las solicitudes de origen. Todas las cadenas de consulta, encabezados y cookies adicionales que especifique en una política de solicitud de origen también se incluyen en las solicitudes de origen (pero no en la clave de caché).

Las políticas de solicitudes de origen y las políticas de caché tienen configuraciones que es posible que parezcan que están en conflicto entre sí. Por ejemplo, es posible que una política permita determinados valores y que otra los bloquee. La siguiente tabla explica qué valores incluye CloudFront en las solicitudes de origen cuando se utilizan juntas la configuración de una política de solicitudes de origen y una política de caché. Esta configuración generalmente se aplica a todos los tipos de valores (cadenas de consulta, encabezados y cookies), con la excepción de que no puede especificar todos los encabezados ni utilizar una lista de bloqueo de encabezados en una política de caché.

	Política de solicitud de origen			
	Ninguna	Todo	Lista de permitidos	Lista de bloqueos
Política de caché				
Ninguna	No se incluye ningún valor de solicitud	Todos los valores de la solicitud	Solo los valores especificados en la política	Todos los valores de la solicitud de

	Política de solicitud de origen			
	Ninguna	Todo	Lista de permitidos	Lista de bloqueos
	de lector en la solicitud de origen, excepto los valores predeterminados que se incluyen en todas las solicitudes de origen. Para obtener más información, consulte Control de las solicitudes de origen con una política.	de lector se incluyen en la solicitud de origen.	de solicitud de origen se incluyen en la solicitud de origen.	lector excepto aquellos especificados en la política de solicitud de origen se incluyen en la solicitud de origen.

	Política de solicitud de origen			
	Ninguna	Todo	Lista de permitidos	Lista de bloqueos
Todo Nota: No puede especificar todos los encabezados de una política de caché.	Todas las cadenas de consulta y cookies de la solicitud de lector se incluyen en la solicitud de origen.	Todos los valores de la solicitud de lector se incluyen en la solicitud de origen.	Todas las cadenas de consulta y cookies de la solicitud de lector y los encabezados especificados en la política de solicitud de origen se incluyen en la solicitud de origen.	Todas las cadenas de consulta y cookies de la solicitud de lector se incluyen en la solicitud de origen, incluso aquellos especificados en la lista de bloqueo de la política de solicitud de origen. La configuración de la política de caché invalida la lista de bloqueo de la política de solicitud de origen.

	Política de solicitud de origen			
	Ninguna	Todo	Lista de permitidos	Lista de bloqueos
Lista de permitidos	Solo los valores especificados de la solicitud de lector se incluyen en la solicitud de origen.	Todos los valores de la solicitud de lector se incluyen en la solicitud de origen.	Todos los valores especificados en la política de caché o la política de la solicitud de origen se incluyen en la solicitud de origen.	Los valores especificados en la política de caché se incluyen en la solicitud de origen, incluso si esos mismos valores se especifican en la lista de bloqueo de la política de solicitud de origen. La lista de permitidos de la política de caché invalida la lista de bloqueo de la política de solicitud de origen.

	Política de solicitud de origen			
	Ninguna	Todo	Lista de permitidos	Lista de bloqueos
Lista de bloqueos Nota: No puede especificar los encabezados de una lista de bloqueo de una política de caché.	Todas las cadenas de consulta y cookies de la solicitud de lector excepto aquellas especificadas se incluyen en la solicitud de origen.	Todos los valores de la solicitud de lector se incluyen en la solicitud de origen.	Los valores especificados en la política de solicitud de origen se incluyen en la solicitud de origen, aunque esos mismos valores se especifiquen en la lista de bloqueo de la política de caché. La lista de permitidos de la política de solicitud de origen invalida la lista de bloqueo de la política de caché.	Todos los valores de la solicitud de lector excepto aquellos especificados en la política de caché o la política de solicitud de origen se incluyen en la solicitud de origen.

Añadido o eliminación de encabezados HTTP en las respuestas de CloudFront con una política

Puede configurar CloudFront para modificar los encabezados HTTP en las respuestas que envía a los lectores (navegadores web y otros clientes). CloudFront puede eliminar los encabezados que recibió del origen o añadir encabezados en la respuesta antes de enviar la respuesta a los lectores. Realizar estos cambios no requiere escribir código ni cambiar el origen.

Por ejemplo, puede eliminar encabezados como `X-Powered-By` y `Vary` para que CloudFront no los incluya en las respuestas que envía a los lectores. O bien, puede añadir encabezados HTTP como los siguientes:

- Un encabezado `Cache-Control` para controlar el almacenamiento en caché del navegador.
- Un encabezado `Access-Control-Allow-Origin` para habilitar el intercambio de recursos entre orígenes (CORS). También puede agregar otros encabezados CORS.
- Un conjunto de encabezados de seguridad comunes, como `Strict-Transport-Security`, `Content-Security-Policy` y `X-Frame-Options`.
- Un encabezado `Server-Timing` para ver información relacionada con el rendimiento y el enrutamiento tanto de la solicitud como de la respuesta a través de CloudFront.

Para especificar los encabezados que CloudFront añade o elimina en las respuestas HTTP, utilice una política de encabezados de respuesta. Usted asocia una política de encabezado de respuesta a uno más comportamientos de caché y CloudFront modifica los encabezados en las respuestas que envía a las solicitudes que coinciden con el comportamiento de la caché. CloudFront modifica los encabezados en las respuestas que proporciona desde la caché y en las que reenvía desde el origen. Si la respuesta de origen incluye uno o más de los encabezados que se han añadido en una política de encabezados de respuesta, la política puede especificar si CloudFront utiliza el encabezado que recibió del origen o sobrescribe ese encabezado con el de la política de encabezados de respuesta.

> **Note**
>
> Si agrega encabezados que controlan el almacenamiento en caché del navegador a las políticas de encabezados de respuesta, como `Cache-Control`, CloudFront agrega estos

encabezados solo a la respuesta del lector. Estos encabezados no afectan a la forma en que CloudFront almacena en caché el objeto solicitado.

CloudFront proporciona algunas políticas de encabezados de respuesta predefinidas, conocidas como políticas administradas, para casos de uso comunes. Puede utilizar estas políticas administradas o crear sus propias políticas. Puede adjuntar una única política de encabezados de respuesta a varios comportamientos de la caché en varias distribuciones de su Cuenta de AWS.

Para obtener más información, consulte los siguientes temas:

Temas

- Descripción de las políticas de encabezados de respuesta
- Creación de políticas de encabezados de respuesta
- Uso de las políticas de encabezados de respuesta administradas

Descripción de las políticas de encabezados de respuesta

Puede utilizar una política de encabezados de respuesta para especificar los encabezados HTTP que Amazon CloudFront elimina o añade en las respuestas que envía a los lectores. Para obtener más información sobre las políticas de encabezados de respuesta y los motivos para usarlas, consulte Añadido o eliminación de encabezados de respuestas con una política.

En los siguientes temas, se explica la configuración de una política de encabezados de respuesta. La configuración se agrupa en categorías, que se representan en los siguientes temas.

Temas

- Detalles de la política (metadatos)
- Encabezados de CORS
- Encabezados de seguridad
- Encabezados personalizados
- Eliminar encabezados
- Encabezado Server-Timing

Detalles de la política (metadatos)

La configuración de detalles de la política contiene metadatos sobre una política de encabezados de respuesta.

- Nombre: un nombre para identificar la política de encabezados de respuesta. En la consola, se utiliza el nombre para adjuntar la política a un comportamiento de la caché.
- Descripción (opcional): un comentario para describir la política de encabezados de respuesta. Esto es opcional, pero puede ayudar a identificar el propósito de la política.

Encabezados de CORS

La configuración de uso compartido de recursos entre orígenes (CORS) permite agregar y configurar encabezados CORS en una política de encabezados de respuesta.

Esta lista se centra en cómo especificar la configuración y los valores válidos en una política de encabezados de respuesta. Para obtener más información sobre cada uno de estos encabezados y cómo se utilizan para solicitudes y respuestas de CORS reales, consulte el artículo sobre el uso compartido de recursos entre orígenes en MDN Web Docs y la especificación del protocolo CORS.

Access-Control-Allow-Credentials

Esta es una configuración booleana (`true` o `false`) que determina si CloudFront añade el encabezado `Access-Control-Allow-Credentials` en las respuestas a las solicitudes de CORS. Cuando esta configuración se configura como `true`, CloudFront agrega el encabezado `Access-Control-Allow-Credentials: true` en las respuestas a las solicitudes de CORS. De lo contrario, CloudFront no agrega este encabezado a las respuestas.

Access-Control-Allow-Headers

Especifica los nombres de encabezado que CloudFront utiliza como valores para el encabezado `Access-Control-Allow-Headers` en las respuestas a las solicitudes de comprobación previa de CORS. Los valores válidos para esta configuración incluyen los nombres de encabezado HTTP o el carácter comodín (`*`), lo que indica que se permiten todos los encabezados.

> **Note**
>
> El encabezado `Authorization` no puede usar un comodín y debe aparecer de forma explícita.

Ejemplos de usos válidos del carácter comodín

Ejemplo	Coincidirá	No coincidirá
`x-amz-*`	`x-amz-test` `x-amz-`	`x-amz`
`x-*-amz`	`x-test-amz` `x--amz`	
`*`	Todos los encabezados excepto `Authorization`	`Authorization`

Access-Control-Allow-Methods

Especifica los métodos HTTP que CloudFront utiliza como valores para el encabezado `Access-Control-Allow-Methods` en las respuestas a las solicitudes de comprobación previa de CORS. Los valores válidos son `GET`, `DELETE`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT` y `ALL`. `ALL` es un valor especial que incluye todos los métodos HTTP enumerados.

Access-Control-Allow-Origin

Especifica los valores que CloudFront puede utilizar en el encabezado de respuesta `Access-Control-Allow-Origin`. Los valores válidos para esta configuración incluyen un origen específico (como `http://www.example.com`) o el carácter comodín (`*`) que indica que se permiten todos los orígenes.

> **Notas**
>
> - Se permite el carácter comodín (`*`) como subdominio más a la izquierda (`*.example.org`).
> - El carácter comodín (`*`) no está permitido en las siguientes posiciones:
> - Dominios de nivel superior (`example.*`)
> - A la derecha de los subdominios (`test.*.example.org`) o en cualquier subdominio (`*test.example.org`)
> - Dentro de los términos (`exa*mple.org`)

Para ver ejemplos de formas de utilizar el carácter comodín, consulte la tabla siguiente.

Ejemplo	Coincidirá	No coincidirá

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

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

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

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

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

Ejemplo	Coincidirá	No coincidirá

`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

Especifica los nombres de encabezado que CloudFront utiliza como valores para el encabezado `Access-Control-Expose-Headers` en las respuestas a las solicitudes de CORS. Los valores válidos para esta configuración incluyen los nombres de encabezado HTTP o el carácter comodín (`*`).

Access-Control-Max-Age

Se trata de la cantidad de segundos que CloudFront utiliza como valor para el encabezado `Access-Control-Max-Age` en las respuestas a las solicitudes de comprobación previa de CORS.

Invalidación de origen

Configuración booleana que determina cómo se comporta CloudFront cuando la respuesta del origen contiene uno de los encabezados de CORS que también se encuentran en la política.

- Cuando se establece como `true` y la respuesta de origen contiene un encabezado de CORS que también está en la política, CloudFront agrega el encabezado de CORS en la política a la respuesta. A continuación, CloudFront envía esa respuesta al espectador. CloudFront ignora el encabezado que recibió del origen.
- Cuando es `false` y la respuesta de origen contiene un encabezado de CORS (independientemente de si el encabezado de CORS también está en la política), CloudFront incluye el encabezado de CORS que recibió del origen en la respuesta. CloudFront no agrega ningún encabezado de CORS de la política a la respuesta que se envía al lector.

Encabezados de seguridad

Puede usar la configuración de encabezados de seguridad permite agregar y configurar varios encabezados de respuesta HTTP relacionados con la seguridad en una política de encabezados de respuesta.

En esta lista se describe cómo se pueden especificar configuraciones y valores válidos en una política de encabezados de respuesta. Para obtener más información sobre cada uno de estos encabezados y cómo se utilizan en las respuestas HTTP reales, consulte los enlaces a MDN Web Docs.

Política de seguridad de contenido

Especifica las directivas de la política de seguridad del contenido que CloudFront utiliza como valores para el encabezado de respuesta `Content-Security-Policy`.

Para obtener más información sobre este encabezado y las directivas de políticas válidas, consulte Content-Security-Policy en MDN Web Docs.

> **Note**
>
> El valor de encabezado `Content-Security-Policy` está limitado a 1783 caracteres.

Política de referencia

Especifica la directiva de política de referencia que CloudFront utiliza como valor para el encabezado de respuesta `Referrer-Policy`. Los valores válidos para esta configuración son `no-referrer`, `no-referrer-when-downgrade`, `origin`, `origin-when-cross-origin`, `same-origin`, `strict-origin`, `strict-origin-when-cross-origin` y `unsafe-url`.

Para obtener más información acerca de este encabezado y estas directivas, consulte Referrer-Policy en MDN Web Docs.

Seguridad de transporte estricta

Especifica las directivas y la configuración que CloudFront utiliza como valor para el encabezado de respuesta `Strict-Transport-Security`. Para esta configuración, especifique por separado lo siguiente:

- la cantidad de segundos, que CloudFront utiliza como valor para la directiva `max-age` de este encabezado

- una configuración booleana (`true` o `false`) para `preload`, que determina si CloudFront incluye la directiva `preload` en el valor de este encabezado
- una configuración booleana (`true` o `false`) para `includeSubDomains`, que determina si CloudFront incluye la directiva `includeSubDomains` en el valor de este encabezado

Para obtener más información acerca de este encabezado y estas directivas, consulte Strict-Transport-Security en MDN Web Docs.

Opciones de tipo de contenido X

Es una configuración booleana (`true` o `false`) que determina si CloudFront añade el encabezado `X-Content-Type-Options` a las respuestas. Cuando esta configuración es `true`, CloudFront agrega el encabezado `X-Content-Type-Options: nosniff` a respuestas. De lo contrario, CloudFront no agrega este encabezado.

Para obtener más información sobre este encabezado, consulte X-Content-Type-Options en MDN Web Docs.

Opciones de marco X

Especifica la directiva que CloudFront utiliza como valor para el encabezado de respuesta `X-Frame-Options`. Los valores válidos para este ajuste son `DENY` o `SAMEORIGIN`.

Para obtener más información sobre este encabezado y estas directivas, consulte X-Frame-Options en MDN Web Docs.

Protección X-XSS

Especifica las directivas y la configuración que CloudFront utiliza como valor para el encabezado de respuesta `X-XSS-Protection`. Para esta configuración, especifique por separado lo siguiente:

- una configuración `X-XSS-Protection` de `0` (desactiva el filtrado XSS) o `1` (habilita el filtrado XSS)
- una configuración booleana (`true` o `false`) para `block`, que determina si CloudFront incluye la directiva `mode=block` en el valor de este encabezado
- un URI de informes, que determina si CloudFront incluye la directiva `report=`*`reporting URI`* en el valor de este encabezado

Puede especificar `true` para `block`, o puede especificar un URI de informes, pero no puede especificar ambos a la vez. Para obtener más información acerca de este encabezado y estas directivas, consulte X-XSS-Protection en MDN Web Docs.

Invalidación de origen

Cada una de estas configuraciones de encabezados de seguridad contiene una configuración booleana (`true` o `false`) que determina cómo se comporta CloudFront cuando la respuesta del origen contiene ese encabezado.

Cuando esta configuración se establece como `true` y la respuesta de origen contiene el encabezado, CloudFront agrega el encabezado a la política a la respuesta que envía al lector. Ignora el encabezado que recibió del origen.

Cuando esta configuración se establece como `false` y la respuesta del origen contiene el encabezado, CloudFront incluye el encabezado que recibió del origen en la respuesta que envía al lector.

Cuando la respuesta de origen no contiene el encabezado, CloudFront lo agrega a la política a la respuesta que envía al lector. CloudFront hace esto cuando esta configuración se establece en `true` o `false`.

Encabezados personalizados

Puede usar la configuración de encabezados personalizados para agregar y configurar encabezados HTTP personalizados en una política de encabezados de respuesta. CloudFront agrega estos encabezados a cada respuesta que devuelve a los lectores. Para cada encabezado personalizado, también se especifica el valor del encabezado, aunque especificar un valor es opcional. Esto se debe a que CloudFront puede agregar un encabezado de respuesta sin valor.

Cada encabezado personalizado también tiene su propia configuración de Invalidación de origen:

- Cuando esta configuración se establece como `true` y la respuesta de origen contiene el encabezado personalizado que está en la política, CloudFront agrega el encabezado de la política a la respuesta que envía al lector. Ignora el encabezado que recibió del origen.
- Cuando esta configuración es `false` y la respuesta del origen contiene el encabezado personalizado que está en la política, CloudFront incluye el encabezado personalizado que recibió del origen en la respuesta que envía al lector.
- Cuando la respuesta de origen no contiene el encabezado personalizado que está en la política, CloudFront agrega el encabezado de la política a la respuesta que envía al lector. CloudFront hace esto cuando esta configuración se establece en `true` o `false`.

Eliminar encabezados

Puede especificar los encabezados que desee que CloudFront elimine de las respuestas que recibe del origen para que no se incluyan en las respuestas que CloudFront envía a los lectores. CloudFront elimina los encabezados de todas las respuestas que envía a los lectores, independientemente de si los objetos se envían desde la memoria caché de CloudFront o desde el origen. Por ejemplo, puede eliminar los encabezados que no son útiles para los navegadores, como `X-Powered-By` o `Vary`, para que CloudFront los elimine de las respuestas que envía a los lectores.

Al especificar los encabezados que se van a eliminar mediante una política de encabezados de respuesta, CloudFront elimina primero los encabezados y, a continuación, añade los encabezados que se especifiquen en otras secciones de la política de encabezados de respuesta (encabezados de CORS, encabezados de seguridad, encabezados personalizados, etc.). Si especifica un encabezado para eliminarlo, pero también añade el mismo encabezado en otra sección de la política, CloudFront incluye el encabezado en las respuestas que envía a los lectores.

> **Note**
>
> Puede utilizar una política de encabezados de respuesta para eliminar los encabezados `Server` y `Date` que CloudFront ha recibido del origen, de modo que estos encabezados (tal como se recibieron del origen) no se incluyan en las respuestas que CloudFront envía a los lectores. Sin embargo, si lo hace, CloudFront añade su propia versión a las respuestas que envía a los lectores. El valor del encabezado `Server` que añade CloudFront es `CloudFront`.

Encabezados que no puede eliminar

No puede eliminar los siguientes encabezados mediante una política de encabezados de respuesta. Si especifica estos encabezados en la sección Remove headers (Eliminar encabezados) de una política de encabezados de respuesta (`ResponseHeadersPolicyRemoveHeadersConfig` en la API), recibirá un error.

- `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

Encabezado Server-Timing

Utilice la configuración de encabezado `Server-Timing` para habilitar el encabezado `Server-Timing` en las respuestas HTTP enviadas desde CloudFront. Puede utilizar este encabezado para ver las métricas que pueden ayudarle a obtener información sobre el comportamiento y el rendimiento de CloudFront y su origen. Por ejemplo, puede ver qué capa de caché sirvió un acierto de caché. O puede ver la latencia del primer byte desde el origen si hay un error de caché. Las métricas del encabezado `Server-Timing` pueden ayudarle a solucionar problemas o a probar la eficacia de su configuración de CloudFront o del origen.

Para obtener más información sobre las métricas de CloudFront en el encabezado `Server-Timing`, consulte los siguientes temas.

Para habilitar el encabezado `Server-Timing`, cree (o edite) una política de encabezados de respuesta.

Temas

- Frecuencia de muestreo y cabecera de solicitud de Pragma
- Encabezado Server-Timing del origen
- Métricas del encabezado Server-Timing
- Ejemplos del encabezado Sever-Timing

Frecuencia de muestreo y cabecera de solicitud de Pragma

Cuando se habilita el encabezado `Server-Timing` en una política de encabezados de respuesta, también se especifica la frecuencia de muestreo. La tasa de muestreo es un número de 0 a 100 (inclusive) que especifica el porcentaje de respuestas a las que desea que CloudFront agregue el encabezado `Server-Timing`. Cuando se establece la tasa de muestreo en 100, CloudFront agrega el encabezado `Server-Timing` a la respuesta HTTP para cada solicitud que coincida con el comportamiento de la caché a la que se adjunta la política de encabezados de respuesta. Si lo establece en 50, CloudFront agrega el encabezado al 50 % de las respuestas de las solicitudes que coinciden con el comportamiento de caché. Puede establecer la frecuencia de muestreo en cualquier número de 0 a 100 con un máximo de cuatro decimales.

Cuando la tasa de muestreo se establece en un número inferior a 100, no se puede controlar a qué respuestas agrega CloudFront el encabezado `Server-Timing`, solo el porcentaje. No obstante, puede agregar el encabezado `Pragma` con un valor establecido como `server-timing` en una

solicitud HTTP para recibir el encabezado `Server-Timing` en la respuesta a esa solicitud. Esto funciona independientemente de la frecuencia de muestreo. Incluso si la tasa de muestreo se establece en cero (0), CloudFront agrega el encabezado `Server-Timing` a la respuesta si la solicitud contiene el encabezado `Pragma: server-timing`.

Encabezado Server-Timing del origen

Si se produce un error de caché y CloudFront reenvía la solicitud al origen, el origen puede incluir un encabezado `Server-Timing` en su respuesta a CloudFront. En este caso, CloudFront agrega sus métricas al encabezado `Server-Timing` que recibió del origen. La respuesta que CloudFront envía al espectador contiene un único encabezado `Server-Timing` que incluye el valor que proviene del origen y las métricas que agregó CloudFront. El valor del encabezado del origen puede estar al final o entre dos conjuntos de métricas que CloudFront agrega al encabezado.

Cuando se produce un acierto de caché, la respuesta que CloudFront envía al espectador contiene un encabezado `Server-Timing` que incluye solo las métricas de CloudFront en el valor del encabezado (no se incluye el valor del origen).

Métricas del encabezado Server-Timing

Cuando CloudFront agrega el encabezado a una respuesta HTTP, el valor del encabezado `Server-Timing` contiene una o más métricas que pueden ayudarle a obtener información sobre el comportamiento y el rendimiento de CloudFront. La siguiente lista contiene todas las métricas y sus valores potenciales. Un encabezado `Server-Timing` contiene solo algunas de estas métricas, según la naturaleza de la solicitud y la respuesta a través de CloudFront.

Algunas de estas métricas se incluyen en el encabezado `Server-Timing` solo con un nombre (sin valor). Otras son un nombre y un valor. Cuando una métrica tiene un valor, el nombre y el valor están separados por un punto y coma (`;`). Cuando el encabezado contiene más de una métrica, estas se separan con una coma (`,`).

cdn-cache-hit

CloudFront proporcionó una respuesta desde la caché sin hacer una solicitud al origen.

cdn-cache-refresh

CloudFront proporcionó una respuesta desde la caché después de enviar una solicitud al origen para verificar que el objeto almacenado en la caché sigue siendo válido. En este caso, CloudFront no recuperó el objeto completo del origen.

cdn-cache-miss

CloudFront no proporcionó la respuesta desde la caché. En este caso, CloudFront solicitó el objeto completo al origen antes de devolver la respuesta.

cdn-pop

Contiene un valor que describe qué punto de presencia (POP) de CloudFront ha gestionado la solicitud.

cdn-rid

Contiene un valor con el identificador único de CloudFront para la solicitud. Puede utilizar este identificador de solicitud (RID) cuando solucione problemas con Soporte.

cdn-hit-layer

Esta métrica está presente cuando CloudFront proporciona una respuesta desde la caché sin realizar una solicitud al origen. Contiene uno de los siguientes valores:

- EDGE: CloudFront proporcionó la respuesta en caché desde una ubicación POP.
- REC: CloudFront proporcionó la respuesta en caché desde una ubicación de caché de borde regional (REC).
- Origin Shield: CloudFront proporcionó la respuesta en caché de REC que está actuando como Origin Shield.

cdn-upstream-layer

Cuando CloudFront solicita el objeto completo desde el origen, esta métrica está presente y contiene uno de los siguientes valores:

- EDGE: una ubicación POP envió la solicitud directamente al origen.
- REC: una ubicación REC envió la solicitud directamente al origen.
- Origin Shield: la REC que actúa de Origin Shield envió la solicitud directamente al origen.

cdn-upstream-dns

Contiene un valor con el número de milisegundos que se emplearon en recuperar el registro DNS para el origen. Un valor de cero (0) indica que CloudFront utilizó un resultado de DNS en caché o reutilizó una conexión existente.

cdn-upstream-connect

Contiene un valor con el número de milisegundos transcurridos desde que se completó la solicitud de DNS de origen hasta que se completó una conexión TCP (y TLS, si procede) con el origen. Un valor de cero (0) indica que CloudFront reutilizó una conexión existente.

cdn-upstream-fbl

Contiene un valor con el número de milisegundos que transcurren entre el momento en que se completa la solicitud HTTP de origen y el momento en que se recibe el primer byte en la respuesta del origen (latencia del primer byte).

cdn-upstream-fbl

Contiene un valor con el número de milisegundos que transcurren entre el momento en que la ubicación periférica terminó de recibir la solicitud y el momento en que se envió el primer byte de respuesta al lector.

Ejemplos del encabezado Sever-Timing

A continuación se muestran ejemplos de un encabezado `Server-Timing` que un lector podría recibir de CloudFront cuando la configuración del encabezado `Server-Timing` está habilitada.

Example: error de caché

En el siguiente ejemplo se muestra un encabezado `Server-Timing` que puede recibir un lector cuando el objeto solicitado no está en la caché de 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
```

Este encabezado `Server-Timing` indica lo siguiente:

- La solicitud de origen se envió desde una ubicación de punto de presencia (POP) de CloudFront (`cdn-upstream-layer;desc="EDGE"`).
- CloudFront usó un resultado de DNS en caché para el origen (`cdn-upstream-dns;dur=0`).
- CloudFront tardó 114 milisegundos en completar la conexión TCP (y TLS, si procede) con el origen (`cdn-upstream-connect;dur=114`).

- CloudFront tardó 177 milisegundos en recibir el primer byte de la respuesta del origen, tras completar la solicitud (`cdn-upstream-fbl;dur=177`).
- El objeto solicitado no estaba en la caché de CloudFront (`cdn-cache-miss`).
- La solicitud se recibió en la ubicación periférica identificada por el código `PHX50-C2` (`cdn-pop;desc="PHX50-C2"`).
- El ID único de CloudFront correspondiente a esta solicitud fue `yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg==` (`cdn-rid;desc="yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg==")`.
- CloudFront tardó 436 milisegundos en enviar el primer byte de la respuesta al espectador, tras recibir la solicitud del lector (`cdn-downstream-fbl;dur=436`).

Example: acierto de caché

En el siguiente ejemplo se muestra un encabezado `Server-Timing` que un lector podría recibir cuando el objeto solicitado está en la caché de 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
```

Este encabezado `Server-Timing` indica lo siguiente:

- El objeto solicitado estaba en la caché (`cdn-cache-hit`).
- La solicitud se recibió en la ubicación periférica identificada por el código `SEA19-C1` (`cdn-pop;desc="SEA19-C1"`).
- El ID único de CloudFront correspondiente a esta solicitud fue `nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g==` (`cdn-rid;desc="nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g==")`.
- El objeto solicitado se almacenó en una ubicación periférica regional (REC) (`cdn-hit-layer;desc="REC"`).
- CloudFront tardó 137 milisegundos en enviar el primer byte de la respuesta al espectador, tras recibir la solicitud del lector (`cdn-downstream-fbl;dur=137`).

Creación de políticas de encabezados de respuesta

Puede utiliza una política de encabezados de respuesta para especificar los encabezados HTTP que Amazon CloudFront añade o elimina de las respuestas HTTP. Para obtener más información sobre las políticas de encabezados de respuesta y los motivos para usarlas, consulte Añadido o eliminación de encabezados de respuestas con una política.

Puede crear una política de encabezados de respuesta en la consola de CloudFront. O bien, puede crear una mediante AWS CloudFormation, AWS Command Line Interface (AWS CLI) o la API de CloudFront. Después de crear una política de encabezados de respuesta, puede adjuntarla a uno o más comportamientos de la caché en una distribución de CloudFront.

Antes de crear una política de encabezados de respuesta personalizada, compruebe si una de las políticas de encabezados de respuesta administradas se ajusta a su caso de uso. Si lo hace, puede adjuntarla a su comportamiento de caché. De este modo, no tendrá que crear ni administrar su propia política de encabezados de respuesta.

Console

Para crear una política de encabezados de respuesta (consola)

1. Inicie sesión en la Consola de administración de AWS y, a continuación, vaya a la pestaña Response headers (Encabezados de respuesta) en la página Policies (Políticas) en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/policies/responseHeaders.
2. Elija Create response headers policy (Crear política de encabezados de respuesta).
3. En el formulario Create response headers policy (Crear política de encabezados de respuesta), haga lo siguiente:
   a. En el panel Details (Detalles), ingrese un Nombre para la política de encabezados de respuesta y (opcionalmente) una Descripción que explique para qué sirve la política.
   b. En el panel Cross-origin resource sharing (CORS) (Uso compartido de recursos entre orígenes [CORS]), elija alternar Configure CORS (Configurar CORS) y configure los encabezados CORS que desee agregar a la política. Si desea que los encabezados configurados invaliden los encabezados que CloudFront recibe del origen, seleccione la casilla de verificación Origin override (Invalidación de origen).

Para obtener más información sobre la configuración de encabezados CORS, consulte the section called “Encabezados de CORS”.

c. En el panel Security headers (Encabezados de seguridad), elija alternar y configure cada uno de los encabezados de seguridad que desee agregar a la política.

   Para obtener más información sobre la configuración de encabezados de seguridad, consulte the section called “Encabezados de seguridad”.

d. En el panel Custom headers (Encabezados personalizados), agregue los encabezados personalizados que desee incluir en la política.

   Para obtener más información sobre la configuración de encabezados personalizados, consulte the section called “Encabezados personalizados”.

e. En el panel Remove headers (Eliminar encabezados), añada los nombres de los encabezados que desee que CloudFront elimine de la respuesta del origen y no los incluya en la respuesta que CloudFront envía a los lectores.

   Para obtener más información sobre cómo eliminar encabezados, consulte the section called “Eliminar encabezados”.

f. En el panel Server-Timing header (Encabezado Server-Timing), elija el conmutador Enable (Habilitar) e introduzca una tasa de muestreo (un número entre 0 y 100, inclusive).

   Para obtener más información acerca del encabezado `Server-Timing`, consulte the section called “Encabezado Server-Timing”.

4. Elija Create (Crear) para crear la política.

Después de crear una política de encabezados de respuesta, puede adjuntarla a un comportamiento de la caché en una distribución de CloudFront.

Para adjuntar una política de encabezados de respuesta a una distribución existente (consola)

1. Abra la página Distributions (Distribuciones) en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Elija la distribución que se va a actualizar y, a continuación, elija la pestaña Behaviors (Comportamientos).

3. Elija el comportamiento de la caché que se va a actualizar y, a continuación, elija Edit (Editar).

   O bien, para crear un nuevo comportamiento de caché, elija Create behavior (Crear comportamiento).
4. Para Política de encabezados de respuesta, elija la política que desea agregar al comportamiento de la caché.
5. Elija Save changes (Guardar cambios) para actualizar el comportamiento de la caché. Si va a crear un nuevo comportamiento de la caché, elija Create behavior (Crear comportamiento).

Para adjuntar una política de encabezados de respuesta a una distribución nueva (consola)

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Crear distribución.
3. Para Política de encabezados de respuesta, elija la política que desea agregar al comportamiento de la caché.
4. Elija las demás configuraciones para la distribución. Para obtener más información, consulte the section called “Toda la configuración de distribución”.
5. Elija Create distribution (Crear distribución) para crear la distribución.

CloudFormation

Para crear una política de encabezados de respuesta con CloudFormation, utilice el tipo de recurso de `AWS::CloudFront::ResponseHeadersPolicy`. En el siguiente ejemplo se muestra la sintaxis de plantilla de CloudFormation, en formato YAML, para crear una política de encabezados de respuesta.

```
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
```

Para obtener más información, consulte AWS::CloudFront::ResponseHeadersPolicy en la Guía del usuario de AWS CloudFormation.

CLI

Para crear una política de encabezados de respuesta con la AWS Command Line Interface (AWS CLI), utilice el comando aws cloudfront create-response-headers-policy. Puede utilizar un archivo de entrada para proporcionar los parámetros de entrada del comando, en lugar de especificar cada parámetro individual como entrada de la línea de comandos.

Para crear una política de encabezados de respuesta (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo llamado `response-headers-policy.yaml`. Este archivo contiene todos los parámetros de entrada para el comando create-response-headers-policy.

   ```
   aws cloudfront create-response-headers-policy --generate-cli-skeleton yaml-input
    > response-headers-policy.yaml
   ```

2. Abra el archivo `response-headers-policy.yaml` que acaba de crear. Edite el archivo para especificar un nombre de política y la configuración de la política de encabezados de respuesta deseada y, a continuación, guarde el archivo.

   Para obtener más información sobre la configuración de política de encabezados de respuesta, consulte the section called “Descripción de las políticas de encabezados de respuesta”.

3. Utilice el siguiente comando para crear la política de encabezados de respuesta. La política que cree utiliza los parámetros de entrada del archivo `response-headers-policy.yaml`.

```
aws cloudfront create-response-headers-policy --cli-input-yaml file://response-
headers-policy.yaml
```

Anote el valor de `Id` en la salida del comando. Se trata del ID de la política de los encabezados de respuesta. Lo necesita para adjuntar la política al comportamiento de la caché de una distribución de CloudFront.

Para adjuntar una política de encabezados de respuesta a una distribución existente (CLI con archivo de entrada)

1. Utilice el comando siguiente para guardar la configuración de distribución de la distribución de CloudFront que desea actualizar. Reemplace *`distribution_ID`* por el ID de la distribución.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Abra el archivo llamado `dist-config.yaml` que acaba de crear. Edite el archivo y realice los siguientes cambios en el comportamiento de la caché para que utilice la política de encabezados de respuesta.

   - En el comportamiento de caché, agregue un campo que se denomina `ResponseHeadersPolicyId`. Para el valor del campo, utilice el ID de política de encabezados de respuesta que anotó después de crear la política.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución y utilizar la política de encabezados de respuesta. Reemplace *`distribution_ID`* por el ID de la distribución.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Para adjuntar una política de encabezados de respuesta a una distribución nueva (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo llamado `distribution.yaml`. Este archivo contiene todos los parámetros de entrada para el comando create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Abra el archivo `distribution.yaml` que acaba de crear. En el comportamiento de la caché predeterminado, en el campo `ResponseHeadersPolicyId`, ingrese el ID de política de encabezados de respuesta que anotó después de crear la política. Siga editando el archivo para especificar la configuración de distribución que desee y, a continuación, guarde el archivo cuando termine.

   Para obtener más información acerca de la configuración de distribución, consulte Referencia de toda la configuración de distribución.

3. Utilice el siguiente comando para crear la distribución mediante los parámetros de entrada del archivo de `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Para crear una política de encabezados de respuesta con la API de CloudFront, utilice CreateResponseHeadersPolicy. Para obtener más información sobre los campos que especifique en esta llamada a la API, consulte the section called “Descripción de las políticas de encabezados de respuesta” y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Después de crear una política de encabezados de respuesta, puede adjuntarla a un comportamiento de la caché, mediante una de las siguientes llamadas a la API:

- Para asociarla a un comportamiento de caché en una distribución existente, utilice UpdateDistribution.

- Para asociarlo con un comportamiento de caché en una nueva distribución, utilice CreateDistribution.

Para estas dos llamadas a la API, proporcione el ID de la política de los encabezados de respuesta en el campo `ResponseHeadersPolicyId`, dentro de un comportamiento de caché. Para obtener más información sobre los otros campos que especifique en estas llamadas a la API, consulte Referencia de toda la configuración de distribución y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Uso de las políticas de encabezados de respuesta administradas

Con una política de encabezados de respuesta de CloudFront, puede especificar los encabezados HTTP que Amazon CloudFront elimina o añade a las respuestas HTTP que envía a los lectores. Para obtener más información sobre las políticas de encabezados de respuesta y los motivos para usarlas, consulte Añadido o eliminación de encabezados de respuestas con una política.

CloudFront proporciona políticas de encabezados de respuesta administradas que puede adjuntar a los comportamientos de la caché en sus distribuciones de CloudFront. Con una política de encabezados de respuesta administrada, no necesita escribir ni mantener su propia política. Las políticas administradas contienen conjuntos de encabezados de respuesta HTTP para casos de uso comunes.

Para utilizar una política de encabezados de respuesta administrada, debe adjuntarla a un comportamiento de la caché en la distribución. El proceso es el mismo que cuando crea una política de encabezados de respuesta personalizada. No obstante, en lugar de crear una nueva política, se adjunta una de las políticas administradas. Adjunta la política por nombre (con la consola) o por ID (con CloudFormation, la AWS CLI o los AWS SDK). Los nombres e ID se muestran en la siguiente sección.

Para obtener más información, consulte the section called “Creación de políticas de encabezados de respuesta”.

En los temas siguientes, se describen las políticas de encabezados de respuesta administradas que puede utilizar.

Temas

- CORS-and-SecurityHeadersPolicy

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

CORS-and-SecurityHeadersPolicy

Consulte esta política en la consola de CloudFront

Utilice esta política administrada para permitir simple CORS requests de cualquier origen. Esta política también agrega un conjunto de encabezados de seguridad a todas las respuestas que CloudFront envía a los lectores. Esta política combina las políticas the section called “SimpleCORS” y the section called “SecurityHeadersPolicy” en una sola.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`e61eb60c-9c35-4d20-a928-2b84e02af89c`

Configuración de política

	Nombre del encabezado	Valor del encabezado	¿Invalidar el origen?
Encabezados CORS:	`Access-Control-Allow-Origin`	`*`	No
Encabezados de seguridad:	`Referrer-Policy`	`strict-origin-when-cross-origin`	No
	`Strict-Transport-Security`	`max-age=31536000`	No
	`X-Content-Type-Options`	`nosniff`	Sí
	`X-Frame-Options`	`SAMEORIGIN`	No
	`X-XSS-Protection`	`1; mode=block`	No

CORS-With-Preflight

Consulte esta política en la consola de CloudFront

Utilice esta política administrada para permitir solicitudes de CORS de cualquier origen, incluidas las solicitudes de comprobación previa. Para solicitudes de comprobación previa (mediante el método `OPTIONS` HHTP), CloudFront agrega los tres encabezados siguientes a la respuesta. Para solicitudes de CORS sencillas, CloudFront agrega solo el encabezado `Access-Control-Allow-Origin`.

Si la respuesta que CloudFront recibe del origen incluye cualquiera de estos encabezados, CloudFront utiliza el encabezado recibido (y su valor) en su respuesta al lector. CloudFront no utiliza el encabezado de esta política.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`5cc3b908-e619-4b99-88e5-2cf7f45965bd`

Configuración de política

	Nombre del encabezado	Valor del encabezado	¿Invalidar el origen?
Encabezados 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

Consulte esta política en la consola de CloudFront

Utilice esta política administrada para permitir las solicitudes CORS de cualquier origen. Esto incluye las solicitudes previas. Esta política también agrega un conjunto de encabezados de seguridad a

todas las respuestas que CloudFront envía a los lectores. Esta política combina las políticas the section called “CORS-With-Preflight” y the section called “SecurityHeadersPolicy” en una sola.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`eaab4381-ed33-4a86-88ca-d9558dc6cd63`

Configuración de política

	Nombre del encabezado	Valor del encabezado	¿Invalidar el origen?
Encabezados CORS:	`Access-Control-Allow-Methods`	`DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT`	No
	`Access-Control-Allow-Origin`	`*`	
	`Access-Control-Expose-Headers`	`*`	
Encabezados de seguridad:	`Referrer-Policy`	`strict-origin-when-cross-origin`	No
	`Strict-Transport-Security`	`max-age=31536000`	No
	`X-Content-Type-Options`	`nosniff`	Sí
	`X-Frame-Options`	`SAMEORIGIN`	No
	`X-XSS-Protection`	`1; mode=block`	No

SecurityHeadersPolicy

Consulte esta política en la consola de CloudFront

Utilice esta política administrada para agregar un conjunto de encabezados de seguridad a todas las respuestas que CloudFront envía a los lectores. Para obtener más información sobre estos encabezados de seguridad, consulte Mozilla's web security guidelines (Directrices de seguridad web de Mozilla).

Con esta política de encabezados de respuesta, CloudFront agrega `X-Content-Type-Options: nosniff` a todas las respuestas. Esto sucede cuando la respuesta que CloudFront recibió del origen incluyó este encabezado y cuando no lo hizo. Para todos los demás encabezados en esta política, si la respuesta que CloudFront recibe del origen incluye el encabezado, CloudFront utiliza el encabezado que recibió (y su valor) en su respuesta al lector. No utiliza el encabezado de esta política.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`67f7725c-6f97-4210-82d7-5512b31e9d03`

Configuración de política

	Nombre del encabezado	Valor del encabezado	¿Invalidar el origen?
Encabezados de seguridad:	`Referrer-Policy`	`strict-origin-when-cross-origin`	No
	`Strict-Transport-Security`	`max-age=31536000`	No
	`X-Content-Type-Options`	`nosniff`	Sí
	`X-Frame-Options`	`SAMEORIGIN`	No
	`X-XSS-Protection`	`1; mode=block`	No

SimpleCORS

Consulte esta política en la consola de CloudFront

Utilice esta política administrada para permitir simple CORS requests de cualquier origen. Con esta política, CloudFront agrega el encabezado `Access-Control-Allow-Origin: *` a todas las respuestas para solicitudes de CORS sencillas.

Si la respuesta que CloudFront recibe del origen incluye el encabezado `Access-Control-Allow-Origin`, CloudFront utiliza ese encabezado (y su valor) en su respuesta al lector. CloudFront no utiliza el encabezado de esta política.

Al utilizar CloudFormation, la AWS CLI o la API de CloudFront, el identificador de esta política es:

`60669652-455b-4ae9-85a4-c4c02393f86c`

Configuración de política

	Nombre del encabezado	Valor del encabezado	¿Invalidar el origen?
Encabezados CORS:	`Access-Control-Allow-Origin`	`*`	No

Comportamiento de solicitudes y respuestas

En los siguientes temas se describe cómo CloudFront gestiona las solicitudes y las respuestas.

Puede obtener información sobre cómo CloudFront interactúa con Amazon S3 u orígenes personalizados, gestiona diversos métodos y encabezados HTTP, procesa códigos de estado y administra el almacenamiento en caché y las respuestas de error.

Temas

- Cómo procesa CloudFront las solicitudes HTTP y HTTPS
- Comportamiento de solicitudes y respuestas para orígenes de Amazon S3
- Comportamiento de solicitudes y respuestas para orígenes personalizados
- Comportamiento de solicitudes y respuestas para grupos de origen
- Añadido de encabezados personalizados a solicitudes de origen
- Cómo CloudFront procesa las solicitudes parciales de un objeto (rango GET)
- Cómo CloudFront procesa los códigos de estado HTTP 3xx desde el origen
- Procesamiento de CloudFront de los códigos de estado HTTP 4xx y 5xx desde el origen
- Generación de respuestas de error personalizadas

Cómo procesa CloudFront las solicitudes HTTP y HTTPS

Para los orígenes de Amazon S3, CloudFront acepta de forma predeterminada solicitudes en protocolos HTTP y HTTPS para objetos de una distribución de CloudFront. A continuación, CloudFront reenvía las solicitudes al bucket de Amazon S3 utilizando el mismo protocolo en el que se hicieron las solicitudes.

En el caso de orígenes personalizados, al crear su distribución, puede especificar cómo CloudFront obtiene acceso a su origen: solo HTTP o con el mismo protocolo utilizado por el lector. Para obtener más información acerca de cómo CloudFront gestiona las solicitudes HTTP y HTTPS para orígenes personalizados, consulte Protocolos.

Para obtener información acerca de cómo restringir la distribución para que los usuarios finales solo puedan obtener acceso a los objetos a través de HTTPS, consulte Uso de HTTPS con CloudFront.

> **Note**
>
> El cargo por solicitudes HTTPS es superior al de solicitudes HTTP. Para obtener más información acerca de tarifas de facturación, consulte los precios de CloudFront.

Comportamiento de solicitudes y respuestas para orígenes de Amazon S3

Para entender cómo CloudFront procesa solicitudes y respuestas cuando se está utilizando Amazon S3 como origen, consulte las secciones siguientes:

Temas

- Cómo CloudFront procesa y reenvía solicitudes a su origen de Amazon S3
- Cómo procesa CloudFront las respuestas de su origen de Amazon S3

Cómo CloudFront procesa y reenvía solicitudes a su origen de Amazon S3

Obtenga información sobre cómo CloudFront procesa solicitudes de lectores y las reenvía a su origen de Amazon S3.

Contenido

- Duración de almacenamiento en caché y TTL mínimo
- Direcciones IP de clientes
- Solicitudes GET condicionales
- Cookies
- Compartir recursos entre orígenes (CORS)
- Solicitudes GET que incluyen un cuerpo
- Métodos HTTP
- Encabezados de solicitud HTTP que CloudFront elimina o actualiza
- Longitud máxima de una solicitud y de una URL
- Asociación de OCSP
- Protocolos

- Cadenas de consulta
- Tiempo de espera e intentos de conexión de origen
- Tiempo de espera de respuesta de origen
- Solicitudes simultáneas del mismo objeto (contracción de solicitudes)

Duración de almacenamiento en caché y TTL mínimo

Para controlar durante cuánto tiempo se mantienen los objetos en una caché de CloudFront antes de que CloudFront reenvíe otra solicitud al origen, puede:

- Configure su origen para añadir un `Cache-Control` o un encabezado `Expires` para cada objeto.
- Especificar un valor de TTL mínimo en comportamientos de la caché de CloudFront.
- Utilice el valor de predeterminado de 24 horas.

Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Direcciones IP de clientes

Si un lector envía una solicitud a CloudFront y no incluye un encabezado de solicitud `X-Forwarded-For`, CloudFront obtiene la dirección IP del lector de la conexión TCP, agrega un encabezado `X-Forwarded-For` que incluya la dirección IP y reenvía la solicitud al origen. Por ejemplo, si CloudFront obtiene la dirección IP `192.0.2.2` de la conexión TCP, reenvía el siguiente encabezado al origen:

```
X-Forwarded-For: 192.0.2.2
```

Si un lector envía una solicitud a CloudFront e incluye un encabezado de solicitud `X-Forwarded-For`, CloudFront obtiene la dirección IP del lector de la conexión TCP, la agrega al final del encabezado `X-Forwarded-For` que incluya la dirección IP y reenvía la solicitud al origen.
Por ejemplo, si la solicitud del lector incluye `X-Forwarded-For: 192.0.2.4,192.0.2.3` y CloudFront obtiene la dirección IP `192.0.2.2` de la conexión TCP, reenvía el siguiente encabezado al origen:

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

> **Note**
>
> El encabezado `X-Forwarded-For` contiene direcciones IPv4 (como 192.0.2.44) e IPv6 (como 2001:0db8:85a3::8a2e:0370:7334).

Solicitudes GET condicionales

Cuando CloudFront recibe una solicitud de un objeto que ha caducado en una caché perimetral, reenvía la solicitud al origen de Amazon S3 para obtener la última versión del objeto o para obtener la confirmación de Amazon S3 de que la caché perimetral de CloudFront ya dispone de la última versión. Cuando Amazon S3 envió el objeto originalmente a CloudFront, incluyó un valor `ETag` y un valor `LastModified` en la respuesta. En la nueva solicitud que CloudFront reenvía a Amazon S3, CloudFront agrega uno o ambos de los siguientes encabezados:

- Un encabezado `If-Match` o `If-None-Match` que contenga el valor `ETag` para la versión caducada del objeto.
- Un encabezado `If-Modified-Since` que contenga el valor `LastModified` para la versión caducada del objeto.

Amazon S3 utiliza esta información para determinar si el objeto se ha actualizado y, en consecuencia, si debe devolver todo el objeto a CloudFront o devolver solo un código de estado HTTP 304 (no modificado).

Cookies

Amazon S3 no procesa cookies. Si configura un comportamiento de caché para reenviar las cookies a un origen de Amazon S3, CloudFront reenvía las cookies, pero Amazon S3 las ignora. Todas las solicitudes futuras del mismo objeto, independientemente si varía la cookie, se atienden desde el objeto existente en la caché.

Compartir recursos entre orígenes (CORS)

Si desea que CloudFront respete la configuración de intercambio de recursos entre orígenes de Amazon S3, configure CloudFront para que reenvíe los encabezados seleccionados a Amazon S3. Para obtener más información, consulte Almacenamiento en caché de contenido en función de encabezados de solicitud.

Solicitudes GET que incluyen un cuerpo

Si una solicitud `GET` del lector incluye un cuerpo, CloudFront devuelve un código de estado HTTP 403 (prohibido) al lector.

Métodos HTTP

Si configura CloudFront para procesar todos los métodos de HTTP que admite, CloudFront acepta las siguientes solicitudes de los lectores y los reenvía al origen de Amazon S3:

- `DELETE`
- `GET`
- `HEAD`
- `OPTIONS`
- `PATCH`
- `POST`
- `PUT`

CloudFront siempre almacena en caché las respuestas a las solicitudes `GET` y `HEAD`. También puede configurar CloudFront para almacenar en caché las respuestas a solicitudes `OPTIONS`. CloudFront no almacena en caché las respuestas a las solicitudes que utilizan los otros métodos.

Si desea utilizar cargas de multipartes para agregar objetos a un bucket de Amazon S3, debe agregar un control de acceso de origen (OAC) de CloudFront a su distribución y conceder al OAC los permisos necesarios. Para obtener más información, consulte the section called “Restricción del acceso a un origen de Amazon S3”.

> **Important**
>
> Si configura CloudFront para que acepte y reenvíe a Amazon S3 todos los métodos HTTP que CloudFront admite, debe crear un OAC de CloudFront para restringir el acceso a su contenido de Amazon S3 y conceder al OAC los permisos necesarios. Por ejemplo, si configura CloudFront para que acepte y reenvíe estos métodos porque desea utilizar el método `PUT`, debe configurar las políticas de buckets de Amazon S3 para que se ocupen de las solicitudes de `DELETE` de forma adecuada, de modo que los lectores no puedan eliminar recursos que usted no desea. Para obtener más información, consulte the section called “Restricción del acceso a un origen de Amazon S3”.

Para obtener más información acerca de las operaciones admitidas por Amazon S3, consulte la documentación de Amazon S3.

Encabezados de solicitud HTTP que CloudFront elimina o actualiza

CloudFront elimina o actualiza algunos encabezado antes de reenviar solicitudes a su origen de Amazon S3. Para la mayoría de encabezados este comportamiento es el mismo que para orígenes personalizados. Para obtener una lista completa de encabezados de solicitudes HTTP y cómo los procesa CloudFront, consulte Encabezados de solicitudes HTTP y comportamiento de CloudFront (personalizado y orígenes de Amazon S3).

Longitud máxima de una solicitud y de una URL

La longitud máxima de una solicitud, incluida la ruta, la cadena de consulta (si procede) y los encabezados, es 20 480 bytes.

CloudFront crea una URL a partir de la solicitud. La longitud máxima de esta URL es de 8 192 bytes.

Si una solicitud o una URL supera la longitud máxima, CloudFront devuelve el código de estado HTTP 413 (entidad de solicitud demasiado grande), al lector y, a continuación, interrumpe la conexión TCP con el lector.

Asociación de OCSP

Cuando un lector envía una solicitud de un objeto HTTPS, CloudFront o el lector deben confirmar con la autoridad de certificación (CA) que el certificado SSL del dominio no se ha revocado. La asociación de OCSP agiliza la validación de certificados al permitir a CloudFront validar el certificado y almacenar en caché la respuesta de la CA, por lo que el cliente no tiene por qué validar el certificado directamente con la CA.

La mejora en el rendimiento de la asociación de OCSP es más notoria cuando CloudFront recibe una gran cantidad de solicitudes de HTTPS de objetos en el mismo dominio. Cada servidor en una ubicación periférica de CloudFront debe enviar una solicitud de validación independiente. Cuando CloudFront recibe una gran cantidad de solicitudes HTTPS para el mismo dominio, cada servidor de la ubicación periférica obtiene pronto una respuesta de la CA que puede asociar a un paquete en el protocolo de enlace de SSL. Cuando el lector confirme que el certificado es válido, CloudFront puede entregar el objeto solicitado. Si la distribución no recibe mucho tráfico en una ubicación periférica de CloudFront, es más probable que las nuevas solicitudes se dirijan a un servidor que todavía no haya validado el certificado con la CA. En ese caso, el lector realiza el paso de validación por

separado y el servidor de CloudFront ofrece el objeto. Este servidor de CloudFront también envía una solicitud de validación a la CA, por lo que la próxima vez que recibe una solicitud que incluye el mismo nombre de dominio, cuenta con una respuesta de validación de la CA.

Protocolos

CloudFront reenvía las solicitudes de HTTP o HTTPS al servidor de origen en función del protocolo de la solicitud del lector, ya sea HTTP o HTTPS.

> **Important**
>
> Si su bucket de Amazon S3 se configura como un punto de enlace de sitio web, no puede configurar CloudFront para usar HTTPS para comunicarse con su origen porque Amazon S3 no admite conexiones HTTPS en dicha configuración.

Cadenas de consulta

Puede configurar si CloudFront reenvía parámetros de cadenas de consulta a su origen Amazon S3. Para obtener más información, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta.

Tiempo de espera e intentos de conexión de origen

Origin connection timeout (Tiempo de espera de conexión de origen) es el número de segundos que CloudFront espera al intentar establecer una conexión con el origen.

Origin connection attempts (Intentos de conexión de origen) es el número de veces que CloudFront intenta conectarse al origen.

Juntos, estos parámetros determinan cuánto tiempo intenta CloudFront conectarse al origen antes de realizar una conmutación al origen secundario (en el caso de un grupo de orígenes) o devolver una respuesta de error al lector. De forma predeterminada, CloudFront espera hasta 30 segundos (3 intentos de 10 segundos cada uno) antes de intentar conectarse al origen secundario o devolver una respuesta de error. Puede reducir este tiempo si especifica menos intentos, un tiempo de espera de conexión más corto o ambas opciones.

Para obtener más información, consulte Control de tiempos de espera e intentos de origen.

Tiempo de espera de respuesta de origen

El tiempo de espera de respuesta del origen, también conocido como tiempo de espera de lectura del origen y tiempo de espera de solicitud al origen, se aplica a los dos siguientes:

- El periodo de tiempo, en segundos, que CloudFront espera una respuesta después de enviar una solicitud al origen.
- El periodo de tiempo, en segundos, que CloudFront espera después de recibir un paquete de una respuesta del origen y antes de recibir el paquete siguiente.

El comportamiento de CloudFront depende del método HTTP en la solicitud del lector:

- Solicitudes `GET` y `HEAD`: si el origen no responde en un plazo de 30 segundos o deja de responder durante 30 segundos, CloudFront interrumpe la conexión. Si el número especificado de intentos de conexión de origen es superior a 1, CloudFront intenta obtener de nuevo una respuesta completa. CloudFront lo intenta hasta tres veces, según lo determinado por el valor de la opciónOrigin connection attempts (Intentos de conexión de origen). Si el origen no responde en el último intento, CloudFront no vuelve a intentarlo hasta que recibe una nueva solicitud de contenido en el mismo origen.
- Solicitudes `DELETE`, `OPTIONS`, `PATCH`, `PUT` y `POST`: si el origen no responde en 30 segundos, CloudFront interrumpe la conexión y no vuelve a intentar ponerse en contacto con el origen. El cliente puede volver a enviar la solicitud en caso de que sea necesario.

No puede cambiar el tiempo de espera de respuesta para un origen de Amazon S3 (un bucket de S3 que no está configurado con alojamiento de sitio web estático).

Solicitudes simultáneas del mismo objeto (contracción de solicitudes)

Cuando una ubicación periférica de CloudFront recibe una solicitud de un objeto y este no se encuentra en la caché o el objeto ha caducado, CloudFront envía inmediatamente la solicitud al origen. Sin embargo, si hay solicitudes simultáneas del mismo objeto, es decir, si llegan solicitudes adicionales del mismo objeto (con la misma clave de caché) a la ubicación periférica antes de que CloudFront reciba la respuesta a la primera solicitud, CloudFront se pone en pausa antes de reenviar las solicitudes adicionales al origen. Esta breve pausa ayuda a reducir la carga en el origen. CloudFront envía la respuesta de la solicitud original a todas las solicitudes que recibió mientras estaba en pausa. Esto se llama contracción de solicitudes. En los registros de CloudFront, la primera solicitud se identifica como `Miss` en el campo `x-edge-result-type`, y las solicitudes contraídas

se identifican como `Hit`. Para obtener más información sobre los registros de CloudFront, consulte the section called “Registro de funciones de CloudFront y perimetrales”.

CloudFront solo contrae las solicitudes que comparten clave de caché. Si las solicitudes adicionales no son idénticas, porque, por ejemplo, ha configurado CloudFront para almacenar en caché en función de los encabezados de solicitudes o las cadenas de consulta, CloudFront reenvía todas las solicitudes únicas a su origen.

Si quiere evitar la contracción de todas las solicitudes, puede utilizar la política de caché administrada `CachingDisabled`, que también impide el almacenamiento en caché. Para obtener más información, consulte Uso de políticas de caché administradas.

Si quiere evitar la contracción de la solicitud para objetos específicos, puede establecer el TTL mínimo para el comportamiento de la caché en 0 y configurar el origen para enviar `Cache-Control: private`, `Cache-Control: no-store`, `Cache-Control: no-cache`, `Cache-Control: max-age=0` o `Cache-Control: s-maxage=0`. Estas configuraciones aumentarán la carga en el origen e introducirán latencia adicional para las solicitudes simultáneas que se detienen mientras CloudFront espera la respuesta a la primera solicitud.

> **Important**
>
> Actualmente, CloudFront no admite la contracción de solicitudes si se habilita el reenvío de cookies en la política de caché, la política de solicitudes de origen o la configuración de caché antigua.

Cómo procesa CloudFront las respuestas de su origen de Amazon S3

Obtenga información sobre cómo procesa CloudFront las respuestas de su origen de Amazon S3

Contenido

- Solicitudes canceladas
- Encabezados de respuesta HTTP que CloudFront elimina o actualiza
- Tamaño máximo de archivo que se puede almacenar en caché
- Redireccionamientos

Solicitudes canceladas

Si un objeto no está en la caché perimetral y un lector termina una sesión (por ejemplo, cierra un navegador) después de que CloudFront obtiene el objeto solicitado del origen, pero antes de que pueda entregarlo, CloudFront no almacena el objeto en la caché de la ubicación periférica.

Encabezados de respuesta HTTP que CloudFront elimina o actualiza

CloudFront elimina o actualiza los siguientes campos de encabezado antes de reenviar la respuesta desde su origen de Amazon S3 al lector:

- `X-Amz-Id-2`
- `X-Amz-Request-Id`
- `Set-Cookie`: si configura CloudFront para reenviar cookies, reenviará el campo del encabezado `Set-Cookie` a los clientes. Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.
- `Trailer`
- `Transfer-Encoding`: si el origen de Amazon S3 devuelve este campo de encabezado CloudFront establece el valor en `chunked` antes de devolver la respuesta al lector.
- `Upgrade`
- `Via`: CloudFront establece el valor en lo siguiente en la respuesta al lector:

  `Via: versión-http cadena-alfanumérica.cloudfront.net (CloudFront)`

  Por ejemplo, el valor será similar a lo siguiente:

  `Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)`

Tamaño máximo de archivo que se puede almacenar en caché

El tamaño máximo de un cuerpo de respuesta que CloudFront guarda en su caché es de 50 GB. Eso incluye respuestas transferidas en fragmentos que no especifican el valor de encabezado `Content-Length`.

Puede utilizar CloudFront para almacenar en caché un objeto superior a este tamaño mediante solicitudes de rango para solicitar los objetos en partes de 50 GB o menos cada una. CloudFront almacena en caché estas partes porque cada una de ellas es de 50 GB o menos. Una vez que el lector recupera todas las partes del objeto, puede reconstruir el objeto original de mayor tamaño.

Para obtener más información, consulte Uso de solicitudes de rango para almacenar en caché objetos grandes.

Redireccionamientos

Puede configurar un bucket de Amazon S3 para redirigir todas las solicitudes a otro nombre de host; este puede ser otro bucket de Amazon S3 o un servidor HTTP. Si configura un bucket para redirigir todas las solicitudes y es el origen de una distribución de CloudFront, le recomendamos configurarlo para redirigirlas a una distribución de CloudFront utilizando el nombre de dominio para la distribución (por ejemplo, d111111abcdef8.cloudfront.net) o un nombre alternativo de dominio (un CNAME) asociado a una distribución (por ejemplo, ejemplo.com). De lo contrario, las solicitudes de los lectores eluden CloudFront y los objetos se sirven directamente desde el nuevo origen.

> **Note**
>
> Si redirige solicitudes a un nombre de dominio alternativo, también debe actualizar el servicio de DNS del dominio mediante la adición de un registro CNAME. Para obtener más información, consulte Uso de URL personalizadas añadiendo nombres de dominio alternativos (CNAME).

Esto es lo que ocurre cuando configura un bucket para redirigir todas las solicitudes:

1. Un lector (por ejemplo, un navegador) solicita un objeto de CloudFront.
2. CloudFront reenvía la solicitud al bucket de Amazon S3 que es el origen de la distribución.
3. Amazon S3 devuelve un código de estado HTTP 301 (movido permanentemente) y la nueva ubicación.
4. CloudFront almacena en caché el código de estado de la redirección y la nueva ubicación, y devuelve los valores al lector. CloudFront no sigue la redirección para obtener el objeto de la nueva ubicación.
5. El lector envía otra solicitud del objeto, pero esta vez el lector especifica la nueva ubicación que obtuvo de CloudFront:

   - Si el bucket de Amazon S3 está redirigiendo todas las solicitudes a una distribución de CloudFront usando el nombre de dominio para la distribución o un nombre de dominio alternativo, CloudFront solicita el objeto del bucket de Amazon S3 o del servidor HTTP en la nueva ubicación. Cuando la nueva ubicación devuelve el objeto, CloudFront lo devuelve al lector y lo almacena en caché en una ubicación periférica.

- Si el bucket de Amazon S3 está redirigiendo las solicitudes a otra ubicación, la segunda solicitud elude CloudFront. El bucket de Amazon S3 o el servidor HTTP de la nueva ubicación devuelven el objeto directamente al lector, por lo que el objeto nunca se almacena en una caché perimetral de CloudFront.

Comportamiento de solicitudes y respuestas para orígenes personalizados

Para entender cómo CloudFront procesa solicitudes y respuestas cuando se está utilizando orígenes personalizados, consulte las secciones siguientes:

Temas

- Cómo procesa y reenvía CloudFront solicitudes a su origen personalizado
- Cómo procesa CloudFront las respuestas de su origen personalizado

Cómo procesa y reenvía CloudFront solicitudes a su origen personalizado

Obtenga información sobre cómo CloudFront procesa solicitudes de lectores y las reenvía a su origen personalizado.

Contenido

- Autenticación
- Duración de almacenamiento en caché y TTL mínimo
- Direcciones IP de clientes
- Autenticación SSL en el cliente
- Compresión
- Solicitudes condicionales
- Cookies
- Compartir recursos entre orígenes (CORS)
- Cifrado
- Solicitudes GET que incluyen un cuerpo
- Métodos HTTP

- Encabezados de solicitudes HTTP y comportamiento de CloudFront (personalizado y orígenes de Amazon S3)
- Versión de HTTP
- Longitud máxima de una solicitud y de una URL
- Asociación de OCSP
- Conexiones persistentes
- Protocolos
- Cadenas de consulta
- Tiempo de espera e intentos de conexión de origen
- Tiempo de espera de respuesta de origen
- Solicitudes simultáneas del mismo objeto (contracción de solicitudes)
- User-AgentEncabezado

Autenticación

Si reenvía el encabezado `Authorization` a su origen, puede configurar el servidor de origen a fin de solicitar autenticación del cliente para los siguientes tipos de solicitudes:

- `DELETE`
- `GET`
- `HEAD`
- `PATCH`
- `PUT`
- `POST`

Para las solicitudes `OPTIONS`, la autenticación del cliente solo se puede configurar si utiliza las siguientes opciones de CloudFront:

- CloudFront se ha configurado para reenviar el encabezado `Authorization` al origen.
- CloudFront se ha configurado para que no almacene en caché la respuesta a solicitudes `OPTIONS`.

Para obtener más información, consulte Configuración de CloudFront para reenviar el encabezado de `Authorization`.

Puede utilizar HTTP o HTTPS para reenviar las solicitudes al servidor de origen. Para obtener más información, consulte Uso de HTTPS con CloudFront.

Duración de almacenamiento en caché y TTL mínimo

Para controlar durante cuánto tiempo se mantienen los objetos en una caché de CloudFront antes de que CloudFront reenvíe otra solicitud al origen, puede:

- Configure su origen para añadir un `Cache-Control` o un encabezado `Expires` para cada objeto.
- Especificar un valor de TTL mínimo en comportamientos de la caché de CloudFront.
- Utilice el valor de predeterminado de 24 horas.

Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Direcciones IP de clientes

Si un lector envía una solicitud a CloudFront y no incluye un encabezado de solicitud `X-Forwarded-For`, CloudFront obtiene la dirección IP del lector de la conexión TCP, agrega un encabezado `X-Forwarded-For` que incluya la dirección IP y reenvía la solicitud al origen. Por ejemplo, si CloudFront obtiene la dirección IP `192.0.2.2` de la conexión TCP, reenvía el siguiente encabezado al origen:

```
X-Forwarded-For: 192.0.2.2
```

Si un lector envía una solicitud a CloudFront e incluye un encabezado de solicitud `X-Forwarded-For`, CloudFront obtiene la dirección IP del lector de la conexión TCP, la agrega al final del encabezado `X-Forwarded-For` que incluya la dirección IP y reenvía la solicitud al origen. Por ejemplo, si la solicitud del lector incluye `X-Forwarded-For: 192.0.2.4,192.0.2.3` y CloudFront obtiene la dirección IP `192.0.2.2` de la conexión TCP, reenvía el siguiente encabezado al origen:

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

Algunas aplicaciones, como, por ejemplo, equilibradores de carga (incluido Elastic Load Balancing), firewalls de aplicaciones web, proxis inversos, sistemas de prevención de intrusos y API Gateway, agregan la dirección IP del servidor de borde de CloudFront que reenvía la solicitud al extremo del encabezado `X-Forwarded-For`. Por ejemplo, si CloudFront incluye `X-Forwarded-For: 192.0.2.2` en una solicitud que reenvía a ELB y si la dirección IP del servidor periférico

de CloudFront es 192.0.2.199, la solicitud que recibe su instancia EC2 contiene el siguiente encabezado:

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

> **Note**
>
> El encabezado `X-Forwarded-For` contiene direcciones IPv4 (como 192.0.2.44) e IPv6 (como 2001:0db8:85a3::8a2e:0370:7334).
> Tenga en cuenta también que todos los nodos de la ruta al servidor actual (CloudFront) pueden modificar el encabezado `X-Forwarded-For`. Para obtener más información, consulte la sección 8.1 de RFC 7239. También puede modificar el encabezado mediante las funciones de computación en la periferia de CloudFront.

Autenticación SSL en el cliente

CloudFront admite la autenticación TLS mutua (mTLS), en la que tanto el cliente como el servidor se autentican entre sí mediante certificados. Con mTLS configurado, CloudFront puede validar los certificados de los clientes durante el establecimiento de comunicación de TLS y, de forma opcional, ejecutar CloudFront Functions para implementar una lógica de validación personalizada.

Para orígenes que solicitan certificados del cliente cuando mTLS no está configurado, CloudFront interrumpe la solicitud.

Para obtener más información sobre la configuración de mTLS, consulte ???.

CloudFront no admite la autenticación del cliente con certificados SSL del lado del cliente. Si un origen solicita un certificado de cliente, CloudFront interrumpe la solicitud.

Compresión

Para obtener más información, consulte Ofrecimiento de archivos comprimidos.

Solicitudes condicionales

Cuando CloudFront recibe una solicitud de un objeto que ha caducado en una caché perimetral, reenvía la solicitud al origen para obtener la última versión del objeto o para obtener la confirmación del origen de que la caché perimetral de CloudFront ya dispone de la última versión. Por lo general, la última vez que el origen envía el objeto a CloudFront, incluye un valor `ETag`, un valor

`LastModified` o ambos en la respuesta. En la nueva solicitud que CloudFront reenvía al origen, CloudFront agrega uno o ambos de los siguientes elementos:

- Un encabezado `If-Match` o `If-None-Match` que contenga el valor `ETag` para la versión caducada del objeto.
- Un encabezado `If-Modified-Since` que contenga el valor `LastModified` para la versión caducada del objeto.

El origen utiliza esta información para determinar si el objeto se ha actualizado y, en consecuencia, devolver todo el objeto a CloudFront o devolver solo un código de estado HTTP 304 (no modificado).

> **Note**
>
> Las solicitudes condicionales `If-Modified-Since` y `If-None-Match` no son compatibles cuando CloudFront se configura para reenviar cookies (todas o un subconjunto).
> Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.

Cookies

Puede configurar CloudFront para que reenvíe cookies al origen. Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.

Compartir recursos entre orígenes (CORS)

Si desea que CloudFront respete la configuración de intercambio de recursos entre orígenes, configure `Origin` para que reenvíe el encabezado al origen. Para obtener más información, consulte Almacenamiento en caché de contenido en función de encabezados de solicitud.

Cifrado

Puede requerir que los lectores utilicen HTTPS para enviar solicitudes a CloudFront y exigir a CloudFront que reenvíe las solicitudes a su origen personalizado mediante el protocolo que utiliza el lector. Para obtener más información, consulte la siguiente configuración de distribución:

- Política de protocolo para lectores
- Protocolo (solo orígenes personalizados)

CloudFront reenvía las solicitudes HTTPS al servidor de origen mediante los protocolos SSLv3, TLSv1.0, TLSv1.1, TLSv1.2 y TLSv1.3. En el caso de orígenes personalizados, puede elegir los protocolos SSL que desea que CloudFront utilice al comunicarse con su origen:

- Si utiliza la consola de CloudFront, elija los protocolos en las casillas Origin SSL Protocols (Protocolos SSL de origen). Para obtener más información, consulte Creación de una distribución.
- Si utiliza la API de CloudFront, especifique los protocolos mediante el elemento `OriginSslProtocols`. Para obtener más información, consulte OriginSslProtocols y DistributionConfig en la Referencia de la API de Amazon CloudFront.

Si el origen es un bucket de Amazon S3, CloudFront utilizará de forma predeterminada TLSv1.3.

> **Important**
>
> Otras versiones de SSL y TLS no son compatibles.

Para obtener más información acerca del uso de HTTPS con CloudFront, consulte Uso de HTTPS con CloudFront. Para obtener listas de los algoritmos criptográficos que CloudFront admite para la comunicación HTTPS entre lectores y CloudFront, y entre CloudFront y su origen, consulte Protocolos y cifrados admitidos entre lectores y CloudFront.

Solicitudes GET que incluyen un cuerpo

Si una solicitud `GET` del lector incluye un cuerpo, CloudFront devuelve un código de estado HTTP 403 (prohibido) al lector.

Métodos HTTP

Si configura CloudFront para procesar todos los métodos de HTTP que admite, CloudFront acepta las siguientes solicitudes de los lectores y las reenvía al origen personalizado:

- `DELETE`
- `GET`
- `HEAD`
- `OPTIONS`
- `PATCH`

- `POST`
- `PUT`

CloudFront siempre almacena en caché las respuestas a las solicitudes `GET` y `HEAD`. También puede configurar CloudFront para almacenar en caché las respuestas a solicitudes `OPTIONS`. CloudFront no almacena en caché las respuestas a las solicitudes que utilizan los otros métodos.

Para obtener más información acerca de la configuración para que su origen personalizado procese estos métodos, consulte la documentación de su origen.

> **Important**
>
> Si configura CloudFront para aceptar y reenviar al origen todos los métodos HTTP que admite CloudFront, configure su servidor de origen para administrar todos los métodos. Por ejemplo, si configura CloudFront para aceptar y reenviar estos métodos porque desea utilizar `POST`, debe configurar también su servidor de origen para administrar las solicitudes `DELETE` adecuadamente, de forma que los lectores no puedan eliminar los recursos que no desee que eliminen. Para obtener más información, consulte la documentación de su servidor HTTP.

Encabezados de solicitudes HTTP y comportamiento de CloudFront (personalizado y orígenes de Amazon S3)

En la siguiente tabla se indican los encabezados de solicitudes HTTP que puede reenviar a orígenes personalizados y de Amazon S3 (con las excepciones que se indican). Para cada encabezado, la tabla incluye información acerca de lo siguiente:

- El comportamiento de CloudFront si no configura CloudFront para reenviar el encabezado a su origen, lo que hace que CloudFront almacene en caché los objetos en función de los valores de encabezado.
- Si puede configurar CloudFront para almacenar en caché los objetos en función de los valores de ese encabezado.

  Puede configurar CloudFront para almacenar en caché los objetos en función de los valores de los encabezados `Date` y `User-Agent`, pero no lo recomendamos. Estos encabezados tienen muchos valores posibles y el almacenamiento en caché en función de sus valores podría hacer que CloudFront reenvíe una cantidad de solicitudes significativamente mayor a su origen.

Para obtener más información acerca del almacenamiento en caché en función de valores de encabezado, consulte Almacenamiento en caché de contenido en función de encabezados de solicitud.

Encabezado	Comportamiento si no configura CloudFront para almacenar en caché en función de los valores de encabezados	Se admite el almacenamiento en caché admite en función de valores de encabezados
Encabezados definidos por otros	Configuración de caché heredada: CloudFront reenvía los encabezados al origen.	Sí
`Accept`	CloudFront elimina el encabezado.	Sí
`Accept-Charset`	CloudFront elimina el encabezado.	Sí
`Accept-Encoding`	Si el valor contiene `gzip` o `br`, CloudFront reenvía un encabezado `Accept-Encoding` normalizado a su origen. Para obtener más información, consulte Compatibilidad con la compresión y Ofrecimiento de archivos comprimidos.	Sí
`Accept-Language`	CloudFront elimina el encabezado.	Sí
`Authorization`	• Solicitudes `GET` y `HEAD`: CloudFront elimina el campo del encabezado `Authorization` antes de reenviar la solicitud al origen.	Sí

Encabezado	Comportamiento si no configura CloudFront para almacenar en caché en función de los valores de encabezados	Se admite el almacenamiento en caché admite en función de valores de encabezados
	• Solicitudes `OPTIONS`: CloudFront elimina el campo de encabezado `Authorization` antes de enviar la solicitud al origen si configura CloudFront para almacenar en caché las respuestas a las solicitudes `OPTIONS`. CloudFront reenvía el campo de encabezado `Authorization` al origen si no configura CloudFront para almacenar en caché las respuestas a solicitudes OPTIONS. • Solicitudes `DELETE`, `PATCH`, `POST` y `PUT`: CloudFront no elimina el campo del encabezado antes de reenviar la solicitud al origen.	
`Cache-Control`	CloudFront reenvía los encabezados al origen.	No
`CloudFront-Forwarded-Proto`	CloudFront no agrega el encabezado antes de reenviar la solicitud al origen. Para obtener más información, consulte Configuración del almacenamiento en caché en función del protocolo de la solicitud.	Sí

Encabezado	Comportamiento si no configura CloudFront para almacenar en caché en función de los valores de encabezados	Se admite el almacenamiento en caché admite en función de valores de encabezados
`CloudFront-Is-Desktop-Viewer`	CloudFront no agrega el encabezado antes de reenviar la solicitud al origen. Para obtener más información, consulte Configuración del almacenamiento en caché en función del tipo de dispositivo.	Sí
`CloudFront-Is-Mobile-Viewer`	CloudFront no agrega el encabezado antes de reenviar la solicitud al origen. Para obtener más información, consulte Configuración del almacenamiento en caché en función del tipo de dispositivo.	Sí
`CloudFront-Is-Tablet-Viewer`	CloudFront no agrega el encabezado antes de reenviar la solicitud al origen. Para obtener más información, consulte Configuración del almacenamiento en caché en función del tipo de dispositivo.	Sí
`CloudFront-Viewer-Country`	CloudFront no agrega el encabezado antes de reenviar la solicitud al origen.	Sí

Encabezado	Comportamiento si no configura CloudFront para almacenar en caché en función de los valores de encabezados	Se admite el almacenamiento en caché admite en función de valores de encabezados
`Connection`	CloudFront sustituye este encabezado por `Connection: Keep-Alive` antes de enviar la solicitud a su origen.	No
`Content-Length`	CloudFront reenvía los encabezados al origen.	No
`Content-MD5`	CloudFront reenvía los encabezados al origen.	Sí
`Content-Type`	CloudFront reenvía los encabezados al origen.	Sí
`Cookie`	Si configura CloudFront para reenviar cookies, reenviará el campo del encabezado `Cookie` a su origen. En caso contrario, CloudFront elimina el campo de encabezado `Cookie`. Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.	No
`Date`	CloudFront reenvía los encabezados al origen.	Sí, pero no se recomienda
`Expect`	CloudFront elimina el encabezado.	Sí

Encabezado	Comportamiento si no configura CloudFront para almacenar en caché en función de los valores de encabezados	Se admite el almacenamiento en caché admite en función de valores de encabezados
`From`	CloudFront reenvía los encabezados al origen.	Sí
`Host`	CloudFront establece el valor en el nombre de dominio del origen que se asocia al objeto solicitado. No puede almacenar en caché en función del encabezado Host para los orígenes de Amazon S3 o MediaStore.	Sí (personalizado) No (S3 y MediaStore)
`If-Match`	CloudFront reenvía los encabezados al origen.	Sí
`If-Modified-Since`	CloudFront reenvía los encabezados al origen.	Sí
`If-None-Match`	CloudFront reenvía los encabezados al origen.	Sí
`If-Range`	CloudFront reenvía los encabezados al origen.	Sí
`If-Unmodified-Since`	CloudFront reenvía los encabezados al origen.	Sí
`Max-Forwards`	CloudFront reenvía los encabezados al origen.	No

Encabezado	Comportamiento si no configura CloudFront para almacenar en caché en función de los valores de encabezados	Se admite el almacenamiento en caché admite en función de valores de encabezados
`Origin`	CloudFront reenvía los encabezados al origen.	Sí
`Pragma`	CloudFront reenvía los encabezados al origen.	No
`Proxy-Authenticate`	CloudFront elimina el encabezado.	No
`Proxy-Authorization`	CloudFront elimina el encabezado.	No
`Proxy-Connection`	CloudFront elimina el encabezado.	No
`Range`	CloudFront reenvía los encabezados al origen. Para obtener más información, consulte Cómo CloudFront procesa las solicitudes parciales de un objeto (rango GET).	Sí de forma predeterminada
`Referer`	CloudFront elimina el encabezado.	Sí
`Request-Range`	CloudFront reenvía los encabezados al origen.	No
`TE`	CloudFront elimina el encabezado.	No

Encabezado	Comportamiento si no configura CloudFront para almacenar en caché en función de los valores de encabezados	Se admite el almacenamiento en caché admite en función de valores de encabezados
`Trailer`	CloudFront elimina el encabezado.	No
`Transfer-Encoding`	CloudFront reenvía los encabezados al origen.	No
`Upgrade`	CloudFront elimina el encabezado, a menos que haya establecido una conexión WebSocket.	No (excepto para las conexiones WebSocket)
`User-Agent`	CloudFront sustituye el valor de este campo de encabezado por `Amazon CloudFront` . Si desea que CloudFront almacene en caché el contenido en función del dispositivo del usuario, consulte Configuración del almacenamiento en caché en función del tipo de dispositivo.	Sí, pero no se recomienda
`Via`	CloudFront reenvía los encabezados al origen.	Sí
`Warning`	CloudFront reenvía los encabezados al origen.	Sí

Encabezado	Comportamiento si no configura CloudFront para almacenar en caché en función de los valores de encabezados	Se admite el almacenamiento en caché admite en función de valores de encabezados
`X-Amz-Cf-Id`	CloudFront agrega el encabezado a la solicitud del lector antes de reenviar la solicitud al origen. El valor de encabezado contiene una cadena cifrada que identifica la solicitud de forma única.	No
`X-Edge-*`	CloudFront elimina todos los encabezados `X-Edge-*`.	No
`X-Forwarded-For`	CloudFront reenvía los encabezados al origen. Para obtener más información, consulte Direcciones IP de clientes.	Sí
`X-Forwarded-Proto`	CloudFront elimina el encabezado.	No
`X-HTTP-Method-Override`	CloudFront elimina el encabezado.	Sí
`X-Real-IP`	CloudFront elimina el encabezado.	No

Versión de HTTP

CloudFront reenvía las solicitudes a su origen personalizado mediante HTTP/1.1.

Longitud máxima de una solicitud y de una URL

La longitud máxima de una solicitud, incluida la ruta, la cadena de consulta (si procede) y los encabezados, es 20 480 bytes.

CloudFront crea una URL a partir de la solicitud. La longitud máxima de esta URL es de 8 192 bytes.

Si una solicitud o una URL supera estos máximos, CloudFront devuelve el código de estado HTTP 413 (entidad de solicitud demasiado grande), al lector y, a continuación, interrumpe la conexión TCP con el lector.

Asociación de OCSP

Cuando un lector envía una solicitud de un objeto HTTPS, CloudFront o el lector deben confirmar con la autoridad de certificación (CA) que el certificado SSL del dominio no se ha revocado. La asociación de OCSP agiliza la validación de certificados al permitir a CloudFront validar el certificado y almacenar en caché la respuesta de la CA, por lo que el cliente no tiene por qué validar el certificado directamente con la CA.

La mejora en el rendimiento de la asociación de OCSP es más notoria cuando CloudFront recibe numerosas solicitudes HTTPS de objetos en el mismo dominio. Cada servidor en una ubicación periférica de CloudFront debe enviar una solicitud de validación independiente. Cuando CloudFront recibe una gran cantidad de solicitudes HTTPS para el mismo dominio, cada servidor de la ubicación periférica obtiene pronto una respuesta de la CA que puede asociar a un paquete en el protocolo de enlace de SSL; cuando el lector considera que el certificado es válido, CloudFront puede ofrecer el objeto solicitado. Si la distribución no recibe mucho tráfico en una ubicación periférica de CloudFront, es más probable que las nuevas solicitudes se dirijan a un servidor que todavía no haya validado el certificado con la CA. En ese caso, el lector realiza el paso de validación por separado y el servidor de CloudFront ofrece el objeto. Este servidor de CloudFront también envía una solicitud de validación a la CA, por lo que la próxima vez que recibe una solicitud que incluye el mismo nombre de dominio, cuenta con una respuesta de validación de la CA.

Conexiones persistentes

Cuando CloudFront obtiene una respuesta de su origen, intenta mantener la conexión durante varios segundos en caso de que otra solicitud llegue durante ese periodo. Garantizar una conexión persistente ahorra el tiempo necesario para restablecer la conexión TCP y realizar otro protocolo de enlace TLS para solicitudes posteriores.

Para obtener más información, incluido el modo de configurar la duración de las conexiones persistentes, consulte Tiempo de espera de keep-alive (solo orígenes personalizados y de VPC) en la sección Referencia de toda la configuración de distribución.

Protocolos

CloudFront reenvía solicitudes HTTP o HTTPS al servidor de origen en función de lo siguiente:

- El protocolo de la solicitud que el lector envía a CloudFront, ya sea HTTP o HTTPS.
- El valor del campo Origin Protocol Policy (Política de protocolo de origen) en la consola de CloudFront o, si está utilizando la API de CloudFront, el elemento `OriginProtocolPolicy` del tipo complejo `DistributionConfig`. En la consola de CloudFront, las opciones son HTTP Only (Solo HTTP), HTTPS Only (Solo HTTPS) y Match Viewer (Coincidir con lector).

Si especifica HTTP Only (Solo HTTP) o HTTPS Only (Solo HTTPS), CloudFront reenvía las solicitudes al servidor de origen mediante el protocolo especificado, independientemente del protocolo de la solicitud del lector.

Si especifica Match Viewer (Coincidir con lector), CloudFront reenvía las solicitudes al servidor de origen mediante el protocolo especificado en la solicitud del lector. Tenga en cuenta que CloudFront almacena en caché el objeto solo una vez, incluso si los lectores realizan solicitudes a través de los protocolos HTTP y HTTPS.

> **Important**
>
> Si CloudFront reenvía una solicitud al origen mediante el protocolo HTTPS, y si el servidor de origen devuelve un certificado no válido o autofirmado, CloudFront interrumpe la conexión TCP.

Para obtener más información acerca de cómo actualizar una distribución desde la consola de CloudFront, consulte Actualizar una distribución. Para obtener información acerca de cómo actualizar una distribución mediante la API de CloudFront, consulte UpdateDistribution en la Referencia de la API de Amazon CloudFront.

Cadenas de consulta

Puede configurar si CloudFront reenvía parámetros de cadenas de consulta a su origen. Para obtener más información, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta.

Tiempo de espera e intentos de conexión de origen

Origin connection timeout (Tiempo de espera de conexión de origen) es el número de segundos que CloudFront espera al intentar establecer una conexión con el origen.

Origin connection attempts (Intentos de conexión de origen) es el número de veces que CloudFront intenta conectarse al origen.

Juntos, estos parámetros determinan cuánto tiempo intenta CloudFront conectarse al origen antes de realizar una conmutación al origen secundario (en el caso de un grupo de orígenes) o devolver una respuesta de error al lector. De forma predeterminada, CloudFront espera hasta 30 segundos (3 intentos de 10 segundos cada uno) antes de intentar conectarse al origen secundario o devolver una respuesta de error. Puede reducir este tiempo si especifica menos intentos, un tiempo de espera de conexión más corto o ambas opciones.

Para obtener más información, consulte Control de tiempos de espera e intentos de origen.

Tiempo de espera de respuesta de origen

El tiempo de espera de respuesta del origen, también conocido como tiempo de espera de lectura del origen y tiempo de espera de solicitud al origen, se aplica a los dos siguientes:

- El periodo de tiempo, en segundos, que CloudFront espera una respuesta después de enviar una solicitud al origen.
- El periodo de tiempo, en segundos, que CloudFront espera después de recibir un paquete de una respuesta del origen y antes de recibir el paquete siguiente.

El comportamiento de CloudFront depende del método HTTP en la solicitud del lector:

- Solicitudes `GET` y `HEAD`: si el origen no responde o deja de responder durante el tiempo de espera de la respuesta, CloudFront interrumpe la conexión. Si el número especificado de intentos de conexión de origen es superior a 1, CloudFront intenta obtener de nuevo una respuesta completa. CloudFront lo intenta hasta tres veces, según lo determinado por el valor de la opciónOrigin

connection attempts (Intentos de conexión de origen). Si el origen no responde en el último intento, CloudFront no vuelve a intentarlo hasta que recibe una nueva solicitud de contenido en el mismo origen.

- Solicitudes `DELETE`, `OPTIONS`, `PATCH`, `PUT` y `POST`: si el origen no responde mientras dura el tiempo de espera de lectura, CloudFront interrumpe la conexión y no vuelve a intentar ponerse en contacto con el origen. El cliente puede volver a enviar la solicitud en caso de que sea necesario.

Para obtener más información, incluido el modo de configurar el tiempo de espera de la respuesta del origen, consulte Tiempo de espera de respuesta.

Solicitudes simultáneas del mismo objeto (contracción de solicitudes)

Cuando una ubicación periférica de CloudFront recibe una solicitud de un objeto y este no se encuentra en la caché o el objeto ha caducado, CloudFront envía inmediatamente la solicitud al origen. Sin embargo, si hay solicitudes simultáneas del mismo objeto, es decir, si llegan solicitudes adicionales del mismo objeto (con la misma clave de caché) a la ubicación periférica antes de que CloudFront reciba la respuesta a la primera solicitud, CloudFront se pone en pausa antes de reenviar las solicitudes adicionales al origen. Esta breve pausa ayuda a reducir la carga en el origen. CloudFront envía la respuesta de la solicitud original a todas las solicitudes que recibió mientras estaba en pausa. Esto se llama contracción de solicitudes. En los registros de CloudFront, la primera solicitud se identifica como `Miss` en el campo `x-edge-result-type`, y las solicitudes contraídas se identifican como `Hit`. Para obtener más información sobre los registros de CloudFront, consulte the section called “Registro de funciones de CloudFront y perimetrales”.

CloudFront solo contrae las solicitudes que comparten clave de caché. Si las solicitudes adicionales no son idénticas, porque, por ejemplo, ha configurado CloudFront para almacenar en caché en función de los encabezados de solicitudes o las cadenas de consulta, CloudFront reenvía todas las solicitudes únicas a su origen.

Si quiere evitar la contracción de todas las solicitudes, puede utilizar la política de caché administrada `CachingDisabled`, que también impide el almacenamiento en caché. Para obtener más información, consulte Uso de políticas de caché administradas.

Si quiere evitar la contracción de la solicitud para objetos específicos, puede establecer el TTL mínimo para el comportamiento de la caché en 0 y configurar el origen para enviar `Cache-Control: private`, `Cache-Control: no-store`, `Cache-Control: no-cache`, `Cache-Control: max-age=0` o `Cache-Control: s-maxage=0`. Estas configuraciones aumentarán la

carga en el origen e introducirán latencia adicional para las solicitudes simultáneas que se detienen mientras CloudFront espera la respuesta a la primera solicitud.

> **Important**
>
> Actualmente, CloudFront no admite la contracción de solicitudes si se habilita el reenvío de cookies en la política de caché, la política de solicitudes de origen o la configuración de caché antigua.

`User-Agent` Encabezado

Si desea que CloudFront almacene en caché diversas versiones de sus objetos según el dispositivo que el usuario utilice para ver su contenido, le recomendamos que configure CloudFront para que reenvíe uno o varios de los siguientes encabezados a su origen personalizado:

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

En función del valor del encabezado `User-Agent`, CloudFront establece el valor de estos encabezados en `true` o `false` antes de reenviar la solicitud al origen. Si un dispositivo entra en más de una categoría, más de un valor podría ser `true`. Por ejemplo, en el caso de algunas tabletas, CloudFront podría establecer tanto `CloudFront-Is-Mobile-Viewer` como `CloudFront-Is-Tablet-Viewer` en `true`. Para obtener más información acerca de la configuración de CloudFront para almacenar en caché en función de los encabezados de solicitud, consulte Almacenamiento en caché de contenido en función de encabezados de solicitud.

Puede configurar CloudFront para almacenar en caché los objetos en función de los valores del encabezado `User-Agent`, pero no lo recomendamos. El encabezado `User-Agent` tiene muchos valores posibles y el almacenamiento en caché en función de esos valores podría hacer que CloudFront reenvíe una cantidad de solicitudes significativamente mayor a su origen.

Si no configura CloudFront para almacenar en caché los objetos en función de los valores del encabezado `User-Agent`, CloudFront agrega un encabezado `User-Agent` con el siguiente valor antes de reenviar una solicitud al origen:

```
User-Agent = Amazon CloudFront
```

CloudFront agrega este encabezado independientemente de si la solicitud del lector incluye un encabezado `User-Agent`. Si la solicitud del lector incluye un encabezado `User-Agent`, CloudFront lo elimina.

Cómo procesa CloudFront las respuestas de su origen personalizado

Obtenga información sobre cómo procesa CloudFront las respuestas de su origen personalizado.

Contenido

- 100 Continue respuestas
- Almacenamiento en caché
- Solicitudes canceladas
- Negociación de contenido
- Cookies
- Conexiones TCP interrumpidas
- Encabezados de respuesta HTTP que CloudFront elimina o reemplaza
- Tamaño máximo de archivo que se puede almacenar en caché
- Origen no disponible
- Redireccionamientos
- Transfer-EncodingEncabezado

`100 Continue` respuestas

Su origen no puede enviar más de una respuesta 100-Continue a CloudFront. Después de la primera respuesta 100-Continue, CloudFront espera una respuesta HTTP 200 OK. Si el origen envía otra respuesta 100-Continue después de la primera, CloudFront devolverá un error.

Almacenamiento en caché

- Asegúrese de que el servidor de origen establece valores válidos y precisos para los campos de encabezado `Date` y `Last-Modified`.
- CloudFront normalmente respeta un encabezado `Cache-Control: no-cache` en la respuesta del origen. Para ver una excepción, consulte Solicitudes simultáneas del mismo objeto (contracción de solicitudes).

Solicitudes canceladas

Si un objeto no está en la caché perimetral y un lector termina una sesión (por ejemplo, cierra un navegador) después de que CloudFront obtiene el objeto solicitado del origen, pero antes de que pueda entregarlo, CloudFront no almacena el objeto en la caché de la ubicación periférica.

Negociación de contenido

Si el origen devuelve `Vary:*` en la respuesta y si el valor de Minimum TTL (TTL mínimo) para el comportamiento de la caché correspondiente es 0, CloudFront almacena en caché el objeto, pero igualmente reenvía cada solicitud posterior del objeto al origen para confirmar que la caché contiene la última versión de dicho objeto. CloudFront no incluye encabezados condicionales, como `If-None-Match` o `If-Modified-Since`. Por tanto, el origen devuelve el objeto a CloudFront como respuesta a cada solicitud.

Si el origen devuelve `Vary:*` en la respuesta y si el valor de TTL mínimo para el comportamiento de la caché correspondiente es cualquier otro valor, CloudFront procesa el encabezado `Vary` tal y como se describe en Encabezados de respuesta HTTP que CloudFront elimina o reemplaza.

Cookies

Si habilita cookies para un comportamiento de la caché y si el origen devuelve las cookies con un objeto, CloudFront almacena en la caché tanto el objeto como las cookies. Tenga en cuenta que este reduce la capacidad de almacenamiento en caché para un objeto. Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.

Conexiones TCP interrumpidas

Si la conexión TCP entre CloudFront y el origen se interrumpe al mismo tiempo que el origen devuelve un objeto a CloudFront, el comportamiento de CloudFront depende de si el origen incluye un encabezado `Content-Length` en la respuesta:

- Encabezado Content-Length: CloudFront devuelve el objeto al lector mientras lo obtiene del origen. Sin embargo, si el valor del encabezado `Content-Length` no coincide con el tamaño del objeto, CloudFront no lo almacena en caché.
- Transfer-Encoding: Chunked: CloudFront devuelve el objeto al lector mientras lo obtiene del origen. Sin embargo, si la respuesta fragmentada no está completa, CloudFront no almacena el objeto en la caché.

- Encabezado No Content-Length: CloudFront devuelve el objeto al lector y lo almacena en la caché, pero el objeto puede no estar completo. Sin un encabezado `Content-Length`, CloudFront no puede determinar si la conexión TCP se interrumpió de forma accidental o intencionadamente.

Le recomendamos que configure su servidor HTTP para agregar un encabezado `Content-Length` y así evitar que CloudFront almacene en caché objetos parciales.

Encabezados de respuesta HTTP que CloudFront elimina o reemplaza

CloudFront elimina o actualiza los siguientes campos de encabezado antes de reenviar la respuesta desde su origen al lector:

- `Set-Cookie`: si configura CloudFront para reenviar cookies, reenviará el campo del encabezado `Set-Cookie` a los clientes. Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.
- `Trailer`
- `Transfer-Encoding`: si el origen devuelve este campo de encabezado, CloudFront establece el valor en `chunked` antes de devolver la respuesta al lector.
- `Upgrade`
- `Vary`: tenga en cuenta lo siguiente:
  - Si configura CloudFront para reenviar cualquiera de los encabezados específicos del dispositivo al origen (`CloudFront-Is-Desktop-Viewer`, `CloudFront-Is-Mobile-Viewer`, `CloudFront-Is-SmartTV-Viewer`, `CloudFront-Is-Tablet-Viewer`) y configura su origen para devolver `Vary:User-Agent` a CloudFront, CloudFront devuelve `Vary:User-Agent` al lector. Para obtener más información, consulte Configuración del almacenamiento en caché en función del tipo de dispositivo.
  - Si configura su origen para incluir bien `Accept-Encoding` o `Cookie` en el encabezado `Vary`, CloudFront incluye los valores en la respuesta al lector.
  - Si configura CloudFront para que reenvíe una lista blanca de encabezados al origen y, además, configura el origen para devolver los nombres de encabezado a CloudFront en el encabezado `Vary` (por ejemplo, `Vary:Accept-Charset,Accept-Language`), CloudFront devuelve el encabezado `Vary` con ese valor al lector.
  - Para obtener más información acerca de cómo CloudFront procesa un valor de `*` en el encabezado `Vary`, consulte Negociación de contenido.

- Si configura su origen para incluir cualquier otro valor en el encabezado `Vary`, CloudFront eliminará dichos valores antes de devolver la respuesta al lector.

- `Via`: CloudFront establece el valor en lo siguiente en la respuesta al lector:

  ```
  Via: versión-http cadena-alfanumérica.cloudfront.net (CloudFront)
  ```

  Por ejemplo, el valor será similar a lo siguiente:

  ```
  Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)
  ```

Tamaño máximo de archivo que se puede almacenar en caché

El tamaño máximo de un cuerpo de respuesta que CloudFront guarda en su caché es de 50 GB. Eso incluye respuestas transferidas en fragmentos que no especifican el valor de encabezado `Content-Length`.

Puede utilizar CloudFront para almacenar en caché un objeto superior a este tamaño mediante solicitudes de rango para solicitar los objetos en partes de 50 GB o menos cada una. CloudFront almacena en caché estas partes porque cada una de ellas es de 50 GB o menos. Una vez que el lector recupera todas las partes del objeto, puede reconstruir el objeto original de mayor tamaño. Para obtener más información, consulte Uso de solicitudes de rango para almacenar en caché objetos grandes.

Origen no disponible

Si el servidor de origen no está disponible y CloudFront obtiene una solicitud de un objeto que se encuentra en la caché perimetral, pero que ha caducado (por ejemplo, porque el periodo especificado en la política `Cache-Control max-age` ya ha transcurrido), CloudFront ofrece esa versión caducada del objeto o una página de error personalizada. Para obtener más información sobre el comportamiento de CloudFront cuando se han configurado páginas de error personalizadas, consulte Cómo CloudFront procesa los errores cuando las páginas de error personalizadas están configuradas.

En algunos casos, un objeto poco solicitado es desalojado y deja de estar disponible en la caché perimetral. CloudFront no puede servir un objeto que haya sido desalojado.

Redireccionamientos

Si cambia la ubicación de un objeto en el servidor de origen, puede configurar su servidor web para redirigir las solicitudes a la nueva ubicación. Después de configurar el redireccionamiento, la primera vez que un lector envía una solicitud del objeto, CloudFront envía la solicitud al origen y el origen responde con un redireccionamiento (por ejemplo, `302 Moved Temporarily`). CloudFront almacena en caché el redireccionamiento y lo devuelve al lector. CloudFront no sigue el redireccionamiento.

Puede configurar su servidor web para redirigir las solicitudes a una de las siguientes ubicaciones:

- La nueva URL del objeto en el servidor de origen. Cuando el lector sigue el redireccionamiento a la nueva URL, el lector elude CloudFront y va directamente al origen. Por tal motivo, le recomendamos que no redirija las solicitudes a la nueva URL del objeto en el origen.
- La nueva URL de CloudFront para el objeto. Cuando el lector envía la solicitud que contiene la nueva URL de CloudFront, CloudFront obtiene el objeto de la nueva ubicación de su origen, lo almacena en la caché de la ubicación periférica y lo devuelve al lector. Las solicitudes posteriores del objeto serán atendidas por la ubicación periférica. Esto evita la latencia y carga asociadas a la solicitud del objeto al origen por parte de los espectadores. Sin embargo, cada nueva solicitud del objeto implicará cargos por concepto de dos solicitudes a CloudFront.

`Transfer-Encoding`Encabezado

CloudFront admite únicamente el valor `chunked` del encabezado `Transfer-Encoding`. Si el origen devuelve `Transfer-Encoding: chunked`, CloudFront devuelve el objeto al cliente tan pronto como lo recibe la ubicación periférica y lo almacena en caché en formato fragmentado para solicitudes posteriores.

Si un lector envía una solicitud `Range GET` y el origen devuelve `Transfer-Encoding: chunked`, CloudFront devuelve el objeto entero al lector en lugar del intervalo solicitado.

Le recomendamos utilizar codificación fragmentada si la longitud de su respuesta no puede ser predeterminada. Para obtener más información, consulte Conexiones TCP interrumpidas.

Comportamiento de solicitudes y respuestas para grupos de origen

Las solicitudes a un grupo de orígenes funcionan igual que las solicitudes a un origen que no está configurado como un grupo de orígenes, excepto cuando hay una conmutación por error de origen.

Al igual que con cualquier otro origen, cuando CloudFront recibe una solicitud y el contenido ya está almacenado en caché en una ubicación periférica, el contenido se sirve a los lectores desde la caché. Cuando hay un error de caché, las solicitudes de lector se reenvían al origen principal en el grupo de orígenes.

El comportamiento de solicitud y respuesta para el origen principal es igual que un origen que no es un grupo de orígenes. Para obtener más información, consulte Comportamiento de solicitudes y respuestas para orígenes de Amazon S3 y Comportamiento de solicitudes y respuestas para orígenes personalizados.

A continuación se describe el comportamiento de conmutación por error de origen cuando el origen principal devuelve códigos de estado HTTP específicos:

- Código de estado HTTP 2xx (éxito): CloudFront almacena en caché el archivo y lo devuelve al lector.
- Código de estado HTTP 3xx (redirección): CloudFront devuelve el código de estado al lector.
- Código de estado HTTP 4xx o 5xx (error de cliente/servidor): si el código de estado devuelto se ha configurado para la conmutación por error, CloudFront envía la misma solicitud al origen secundario del grupo de orígenes.
- Código de estado HTTP 4xx o 5xx (error de cliente/servidor): si el código de estado devuelto no se ha configurado para conmutación por error, CloudFront devuelve el error al lector.

CloudFront conmuta por error al origen secundario solo cuando el método HTTP de la solicitud del lector es `GET`, `HEAD` u `OPTIONS`. CloudFront no realiza una conmutación por error cuando el lector envía un método HTTP diferente (por ejemplo `POST`, `PUT`, etc.).

Cuando CloudFront envía una solicitud a un origen secundario, el comportamiento de respuesta es el mismo que para un origen de CloudFront que no está en un grupo de orígenes.

Para obtener más información acerca de los grupos de orígenes, consulte Optimización de alta disponibilidad con conmutación por error de origen de CloudFront.

Añadido de encabezados personalizados a solicitudes de origen

Puede configurar CloudFront para agregar encabezados personalizados a las solicitudes que envía a su origen. Puede usar encabezados personalizados para enviar y recopilar información de su origen que no obtenga con las solicitudes típicas del lector. Puede incluso personalizar estos

encabezados para cada origen. CloudFront admite encabezados personalizados tanto para orígenes personalizados como para orígenes Amazon S3.

Contenido

- Casos de uso
- Configuración de CloudFront para agregar encabezados personalizados a solicitudes de origen
- Encabezados personalizados que CloudFront no puede agregar a solicitudes de origen
- Configuración de CloudFront para reenviar el encabezado de Authorization

Casos de uso

Puede utilizar encabezados personalizados, como los siguientes ejemplos:

Identificación de solicitudes de CloudFront

Puede identificar las solicitudes que su origen recibe de CloudFront. Esto resulta útil si desea saber si los usuarios están eludiendo CloudFront o si está utilizando más de una CDN y desea obtener información acerca de qué solicitudes provienen de cada CDN.

> **Note**
>
> Si utiliza un origen de Amazon S3 y habilita el registro de acceso del servidor de Amazon S3, los registros no incluyen información del encabezado.

Determinar qué solicitudes provienen de una distribución en concreto

Si configura más de una distribución de CloudFront para que utilice el mismo origen, puede agregar distintos encabezados personalizados a cada distribución. A continuación, puede utilizar los registros de su origen para determinar qué solicitudes provenían de cada distribución de CloudFront.

Habilitar el uso compartido de recursos entre orígenes (CORS)

Si algunos de sus lectores no admite el uso compartido de recursos entre orígenes (CORS), puede configurar CloudFront para que agregue siempre el encabezado `Origin` a las solicitudes que envía al origen. A continuación, puede configurar su origen para que devuelva el encabezado `Access-Control-Allow-Origin` de cada solicitud. También debe configurar CloudFront para que respete la configuración de CORS.

Controlar el acceso al contenido

Puede utilizar encabezados personalizados para controlar el acceso al contenido. Al configurar el origen para que responda a las solicitudes solo cuando incluyan un encabezado personalizado que haya agregado CloudFront, evita que los usuarios eludan CloudFront y obtengan acceso al contenido directamente en el origen. Para obtener más información, consulte Restricción del acceso a archivos en orígenes personalizados.

Configuración de CloudFront para agregar encabezados personalizados a solicitudes de origen

Para configurar una distribución para agregar encabezados personalizados a las solicitudes que envía al origen, actualice la configuración de origen mediante uno de los métodos siguientes:

- Consola de CloudFront: al crear o actualizar una distribución, especifique los nombres y los valores de encabezado en la opción Origin Custom Headers. Para obtener más información, consulte Agregar encabezado personalizado.
- API de CloudFront: para cada origen al que desee agregar encabezados personalizados, especifique los nombres y valores del encabezado en el campo `CustomHeaders` dentro de `Origin`. Para obtener más información, consulte CreateDistribution o UpdateDistribution en la Amazon CloudFront API Reference.

Si los nombres y valores del encabezado que especifica ya no están presentes en la solicitud del lector, CloudFront los agrega a la solicitud de origen. Si hay un encabezado, CloudFront sobrescribe el valor de encabezado antes de reenviar la solicitud al origen.

Para ver las cuotas que se aplican a los encabezados personalizados de origen, consulte Cuotas en encabezados.

Encabezados personalizados que CloudFront no puede agregar a solicitudes de origen

No puede configurar CloudFront para que agregue ninguno de los encabezados siguientes a las solicitudes que envía a su origen:

- `Cache-Control`
- `Connection`

- `Content-Length`
- `Cookie`
- `Host`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Range`
- `If-Unmodified-Since`
- `Max-Forwards`
- `Pragma`
- `Proxy-Authenticate`
- `Proxy-Authorization`
- `Proxy-Connection`
- `Range`
- `Request-Range`
- `TE`
- `Trailer`
- `Transfer-Encoding`
- `Upgrade`
- `Via`
- Encabezados que comiencen por `X-Amz-`
- Encabezados que comiencen por `X-Edge-`
- `X-Real-Ip`

Configuración de CloudFront para reenviar el encabezado de **`Authorization`**

Cuando CloudFront reenvía una solicitud del lector a su origen, CloudFront elimina algunos encabezados de lector de forma predeterminada, incluido el encabezado `Authorization`. Para asegurarse de que su origen siempre recibe el encabezado `Authorization` en las solicitudes de origen, tiene las siguientes opciones:

- Agregue el encabezado `Authorization` a la clave de caché mediante una política de caché. Todos los encabezados de la clave de caché se incluyen automáticamente en las solicitudes de origen. Para obtener más información, consulte Control de la clave de caché con una política.
- Utilice una política de solicitud de origen que reenvíe todos los encabezados del lector al origen. No puede reenviar el encabezado `Authorization` individualmente en una política de solicitud de origen, pero cuando reenvíe todos los encabezados del lector CloudFront incluye el encabezado `Authorization` en las solicitudes de lector. CloudFront proporciona una política de solicitud de origen administrada para este caso de uso, denominada Managed-AllViewer. Para obtener más información, consulte Uso de políticas de solicitudes de origen administradas.

Cómo CloudFront procesa las solicitudes parciales de un objeto (rango GET)

Para objetos grandes, es posible que los lectores (navegadores web u otros clientes) realicen varias solicitudes `GET` y utilicen el encabezado de solicitud `Range` para descargar el objeto en partes más pequeñas. Estas solicitudes de rangos de bytes, a veces conocidas como solicitudes `Range GET`, mejoran la eficacia de las descargas parciales y la recuperación de transferencias que hayan fallado parcialmente.

Cuando CloudFront recibe una solicitud `Range GET`, revisa la caché de la ubicación periférica que recibe la solicitud. Si la caché de dicha ubicación periférica ya contiene todo el objeto o la parte solicitada del objeto, CloudFront envía inmediatamente el rango solicitado desde la caché.

Si la caché no contiene el rango solicitado, CloudFront reenvía la solicitud al origen. (Para optimizar el rendimiento, CloudFront puede solicitar un intervalo superior al solicitado en `Range GET`.) Lo que ocurre a continuación depende de si el origen admite solicitudes `Range GET`:

- Si el origen admite solicitudes **`Range GET`**: devuelve el intervalo solicitado. CloudFront sirve el intervalo solicitado y lo almacena en la caché para futuras solicitudes. (Amazon S3 admite solicitudes `Range GET`, al igual que muchos servidores HTTP).
- Si el origen no admite solicitudes **`Range GET`**: devuelve todo el objeto. CloudFront sirve la solicitud actual enviando todo el objeto almacenándolo también en caché para futuras solicitudes. Después de que CloudFront almacene en caché todo el objeto en una caché perimetral, responde a las nuevas solicitudes `Range GET` enviando el intervalo solicitado.

En cualquier caso, CloudFront comienza a enviar el intervalo o el objeto solicitado al usuario final en cuanto llega el primer byte del origen.

> **Note**
>
> Si un lector envía una solicitud `Range GET` y el origen devuelve `Transfer-Encoding: chunked`, CloudFront devuelve el objeto entero al lector en lugar del intervalo solicitado.

Por lo general, CloudFront sigue la especificación RFC en el encabezado `Range`. Sin embargo, si sus encabezados `Range` no cumplen con los siguientes requisitos, CloudFront devuelve el código de estado HTTP `200` con el objeto entero en lugar del código de estado `206` con los intervalos especificados:

- Los rangos deben publicarse en orden ascendente. Por ejemplo, `100-200,300-400` es válido; `300-400,100-200` no es válido.
- Los rangos no deben superponerse. Por ejemplo, `100-200,150-250` no es válido.
- Todas las especificaciones de los rangos deben ser válidas. Por ejemplo, no puede especificar valores negativos como parte de un rango.

Para obtener más información sobre el encabezado de solicitud `Range`, consulteRange Requests en RFC 7233, o Range en MDN Web Docs.

Uso de solicitudes de rango para almacenar en caché objetos grandes

Cuando el almacenamiento en caché está habilitado, CloudFront no recupera ni almacena en caché un objeto de más de 50 GB. Cuando un origen indica que el objeto es mayor que este tamaño (en el encabezado de respuesta `Content-Length`), CloudFront cierra la conexión con el origen y devuelve un error al lector. (Con el almacenamiento en caché desactivado, CloudFront puede recuperar un objeto mayor que este tamaño del origen y pasarlo al lector. Sin embargo, CloudFront no almacena en caché el objeto).

Sin embargo, con las solicitudes de rango, puede utilizar CloudFront para almacenar en caché un objeto mayor que el tamaño máximo de archivo almacenable en caché.

Example Ejemplo

1. Considere un origen con un objeto de 100 GB. Cuando el almacenamiento en caché está habilitado, CloudFront no recupera ni almacena en caché un objeto de este tamaño. Sin embargo, el lector puede enviar varias solicitudes de rango para recuperar este objeto en partes, con cada parte menor que 50 GB.
2. El lector puede solicitar el objeto en partes de 20 GB mediante el envío de una solicitud con el encabezado `Range: bytes=0-21474836480` para recuperar la primera parte, otra solicitud con el encabezado `Range: bytes=21474836481-42949672960` para recuperar la siguiente parte, y así sucesivamente.
3. Cuando el lector ha recibido todas las partes, puede combinarlas para construir el objeto original de 100 GB.
4. En este caso, CloudFront almacena en caché cada una de las partes de 20 GB del objeto y puede responder a las solicitudes posteriores de la misma parte desde la caché.

Para una solicitud de rango para un objeto comprimido, la solicitud de rango de bytes se basa en el tamaño comprimido y no en el tamaño original del objeto. Para obtener más información acerca de la compresión de archivos, consulte Ofrecimiento de archivos comprimidos.

Cómo CloudFront procesa los códigos de estado HTTP 3xx desde el origen

Cuando CloudFront solicita un objeto desde su bucket de Amazon S3 o el servidor de origen personalizado, su origen a veces devuelve un código de estado HTTP 3xx. Esto suele indicar una de las siguientes posibilidades:

- La dirección URL del objeto ha cambiado (por ejemplo, códigos de estado 301, 302, 307 o 308)
- El objeto no ha cambiado desde la última vez que CloudFront lo solicitó (código de estado 304)

CloudFront almacena en caché las respuestas 3xx de acuerdo con la configuración de su distribución de CloudFront y los encabezados de la respuesta. CloudFront almacena en caché las respuestas 307 y 308 solo cuando incluye el encabezado `Cache-Control` en las respuestas del origen. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Si su origen devuelve un código de estado de redireccionamiento (por ejemplo, 301 o 307), CloudFront no sigue el redireccionamiento. CloudFront pasa la respuesta 301 o 307 al lector, que puede seguir el redireccionamiento enviando una nueva solicitud.

Procesamiento de CloudFront de los códigos de estado HTTP 4xx y 5xx desde el origen

Cuando CloudFront solicita un objeto desde su bucket de Amazon S3 o un servidor de origen personalizado, el origen a veces devuelve un código de estado HTTP 4xx o 5xx, que indica que se ha producido un error. El comportamiento de CloudFront depende de:

- Si ha configurado páginas de error personalizadas
- Si ha configurado el tiempo durante el que desea que CloudFront almacene en caché las respuestas de error de su origen (TTL mínimo de almacenamiento de errores en la caché)
- El código del estado
- En el caso de códigos de estado 5xx, si el objeto solicitado se encuentra en la caché perimetral de CloudFront
- Para algunos códigos de estado 4xx, si el origen devuelve un encabezado `Cache-Control max-age` o `Cache-Control s-maxage`

CloudFront siempre almacena en caché las respuestas a las solicitudes `GET` y `HEAD`. También puede configurar CloudFront para almacenar en caché las respuestas a solicitudes `OPTIONS`. CloudFront no almacena en caché las respuestas a las solicitudes que utilizan los otros métodos.

Si el origen no responde, la solicitud de CloudFront al origen agota el tiempo de espera, lo que se considera un error HTTP 5xx del origen, aunque el origen no haya respondido con ese error. En ese caso, CloudFront sigue ofreciendo contenido almacenado en caché. Para obtener más información, consulte Origen no disponible.

Si ha activado el registro, CloudFront escribe los resultados en registros independientemente del código de estado HTTP.

Para obtener más información acerca de las características y las opciones relacionadas con el mensaje de error devuelto por CloudFront, consulte lo siguiente:

- Para obtener más información acerca de la configuración de páginas de error personalizadas desde la consola de CloudFront, consulte Páginas de error personalizadas y almacenamiento de errores en caché.
- Para obtener información acerca del TTL mínimo de almacenamiento de errores en la caché desde la consola de CloudFront, consulte TTL mínimo de almacenamiento de errores en caché (segundos).
- Para obtener una lista de los códigos de estado HTTP que CloudFront almacena en caché, consulte Códigos de estado HTTP 4xx y 5xx que CloudFront almacena en caché.

Temas

- Cómo CloudFront procesa los errores cuando las páginas de error personalizadas están configuradas
- Cómo CloudFront procesa los errores si no ha configurado las páginas de error personalizadas
- Códigos de estado HTTP 4xx y 5xx que CloudFront almacena en caché

Cómo CloudFront procesa los errores cuando las páginas de error personalizadas están configuradas

Si ha configurado páginas de error personalizadas, el comportamiento de CloudFront dependerá de si el objeto solicitado está o no en la caché perimetral.

El objeto solicitado no está en la caché perimetral

CloudFront continúa intentando obtener el objeto solicitado de su origen si se cumplen todas las condiciones que se indican a continuación:

- Un espectador solicita un objeto.
- El objeto no está en la caché perimetral.
- Su origen devuelve un código de estado HTTP 4xx o 5xx y se cumple alguna de las condiciones siguientes:
  - Su origen devuelve un código de estado HTTP 5xx en lugar de devolver un código 304 (No modificado) o una versión actualizada del objeto.
  - Su origen devuelve un código de estado HTTP 4xx que no está restringido por un encabezado de control de la caché y está incluido en la siguiente lista de códigos de estado: Códigos de estado HTTP 4xx y 5xx que CloudFront almacena en caché.

- El origen devuelve un código de estado HTTP 4xx con un encabezado `Cache-Control max-age` o un encabezado `Cache-Control s-maxage` y el código de estado está incluido en la siguiente lista de códigos de estado: Control Códigos de estado HTTP 4xx que CloudFront almacena en caché en función de los encabezados `Cache-Control`.

CloudFront hace lo siguiente:

1. En la caché perimetral de CloudFront que recibió la solicitud del lector, CloudFront comprueba la configuración de la distribución y obtiene la ruta de la página de error personalizada que corresponde al código de estado devuelto por su origen.
2. CloudFront comprueba el primer comportamiento de la caché de la distribución que tenga un patrón de ruta que coincida con la ruta de la página de error personalizada.
3. La ubicación periférica de CloudFront envía una solicitud de la página de error personalizada al origen especificado en el comportamiento de la caché.
4. El origen devuelve la página de error personalizada a la ubicación periférica.
5. CloudFront devuelve la página de error personalizada al lector que ha realizado la solicitud y almacena en caché dicha página durante el tiempo máximo siguiente:
   - La cantidad de tiempo especificado por el TTL mínimo de almacenamiento en caché de errores (10 segundos de forma predeterminada)
   - El periodo de tiempo especificado por un encabezado `Cache-Control max-age` o un encabezado `Cache-Control s-maxage` que devuelve el origen cuando la primera solicitud generó el error
6. Una vez transcurrido el tiempo de almacenamiento en caché (determinado en el paso 5), CloudFront intenta de nuevo obtener el objeto solicitado reenviando otra solicitud a su origen. CloudFront continúa intentándolo a intervalos especificados por el TTL mínimo de almacenamiento de errores en caché.

> **Note**
>
> Si también configuró un comportamiento de caché para la misma página de error personalizada, CloudFront utiliza el TTL del comportamiento de caché en su lugar. En este caso, CloudFront hará lo siguiente en los pasos 5 y 6:
>
> - Después de que CloudFront devuelva la página de error personalizada al espectador que realizó la solicitud, CloudFront verifica el TTL del comportamiento de caché (por ejemplo, si

configuró el TTL predeterminado en 5 segundos). A continuación, CloudFront almacena en caché la página de error personalizada hasta ese máximo.

- Después de transcurrir 5 segundos, CloudFront recupera la página de error personalizada del origen nuevamente. CloudFront continuará intentándolo a intervalos especificados por el TTL de comportamiento de almacenamiento en caché.

Para obtener más información, consulte la configuración de TTL de comportamiento de la caché.

El objeto solicitado está en la caché perimetral

CloudFront continúa sirviendo el objeto que se encuentra en ese momento en la caché perimetral si se cumplen todas las condiciones que se indican a continuación:

- Un espectador solicita un objeto.
- El objeto se encuentra en la memoria caché de borde, pero ha caducado
- Su origen devuelve un código de estado HTTP 5xx en lugar de devolver un código 304 (No modificado) o una versión actualizada del objeto.

CloudFront hace lo siguiente:

1. Si el origen devuelve un código de estado 5xx, CloudFront sirve el objeto a pesar de que haya caducado. Durante el TTL mínimo de almacenamiento de errores en caché, CloudFront continúa respondiendo a las solicitudes de los lectores ofreciendo el objeto de la caché perimetral.

   Si el origen devuelve un código de estado 4xx, CloudFront devuelve el código de estado al lector en lugar del objeto solicitado.
2. Una vez finalizado el TTL mínimo de almacenamiento de errores en caché, CloudFront intenta obtener el objeto solicitado una vez más reenviando otra solicitud al origen. Tenga en cuenta que si el objeto no se solicita con frecuencia, CloudFront podría desalojarlo de la caché perimetral mientras el servidor de origen sigue devolviendo respuestas 5xx. Para obtener más información acerca de por cuánto tiempo pueden permanecer los objetos en las cachés perimetrales de CloudFront, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

Cómo CloudFront procesa los errores si no ha configurado las páginas de error personalizadas

Si no ha configurado páginas de error personalizadas, el comportamiento de CloudFront dependerá de si el objeto solicitado está o no en la caché perimetral.

Temas

- El objeto solicitado no está en la caché perimetral
- El objeto solicitado está en la caché perimetral

El objeto solicitado no está en la caché perimetral

CloudFront continúa intentando obtener el objeto solicitado de su origen si se cumplen todas las condiciones que se indican a continuación:

- Un espectador solicita un objeto.
- El objeto no está en la caché perimetral.
- Su origen devuelve un código de estado HTTP 4xx o 5xx y se cumple alguna de las condiciones siguientes:
  - Su origen devuelve un código de estado HTTP 5xx en lugar de devolver un código 304 (No modificado) o una versión actualizada del objeto.
  - Su origen devuelve un código de estado HTTP 4xx que no está restringido por un encabezado de control de la caché y está incluido en la siguiente lista de códigos de estado: Códigos de estado HTTP 4xx y 5xx que CloudFront almacena en caché
  - El origen devuelve un código de estado HTTP 4xx con un encabezado `Cache-Control max-age` o un encabezado `Cache-Control s-maxage` y el código de estado está incluido en la siguiente lista de códigos de estado: Control Códigos de estado HTTP 4xx que CloudFront almacena en caché en función de los encabezados `Cache-Control`.

CloudFront hace lo siguiente:

1. CloudFront devuelve un código de estado 4xx o 5xx al lector y también almacena el código de estado en la caché perimetral que recibió la solicitud durante el tiempo máximo siguiente:
   - La cantidad de tiempo especificado por el TTL mínimo de almacenamiento en caché de errores (10 segundos de forma predeterminada)

- El periodo de tiempo especificado por un encabezado `Cache-Control max-age` o un encabezado `Cache-Control s-maxage` que devuelve el origen cuando la primera solicitud generó el error

2. Para la duración del tiempo de almacenamiento en caché (determinado en el paso 1), CloudFront responde a las solicitudes de los lectores posteriores del mismo objeto con el código de estado almacenado en caché 4xx o 5xx.
3. Una vez transcurrido el tiempo de almacenamiento en caché (determinado en el paso 1), CloudFront intenta de nuevo obtener el objeto solicitado reenviando otra solicitud a su origen. CloudFront continúa intentándolo a intervalos especificados por el TTL mínimo de almacenamiento de errores en caché.

El objeto solicitado está en la caché perimetral

CloudFront continúa sirviendo el objeto que se encuentra en ese momento en la caché perimetral si se cumplen todas las condiciones que se indican a continuación:

- Un espectador solicita un objeto.
- El objeto se encuentra en la memoria caché de borde, pero ha caducado Esto significa que el objeto está obsoleto.
- Su origen devuelve un código de estado HTTP 5xx en lugar de devolver un código 304 (No modificado) o una versión actualizada del objeto.

CloudFront hace lo siguiente:

1. Si el origen devuelve un código de error 5xx, CloudFront sirve el objeto a pesar de que haya caducado. Durante la vigencia del TTL mínimo de almacenamiento en caché de errores (10 segundos de forma predeterminada), CloudFront continúa respondiendo a las solicitudes de los lectores sirviendo el objeto de la caché perimetral.

   Si el origen devuelve un código de estado 4xx, CloudFront devuelve el código de estado al lector en lugar del objeto solicitado.
2. Una vez finalizado el TTL mínimo de almacenamiento de errores en caché, CloudFront intenta obtener el objeto solicitado una vez más reenviando otra solicitud al origen. Si el objeto no se solicita con frecuencia, CloudFront podría desalojarlo de la caché perimetral mientras el servidor de origen sigue devolviendo respuestas 5xx. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

> **Tip**
>
> - Si configura la directiva `stale-if-error` o `Stale-While-Revalidate`, puede especificar durante cuánto tiempo estarán disponibles los objetos obsoletos en la caché perimetral. Esto le permite seguir ofreciendo contenido a los lectores incluso cuando su origen no esté disponible. Para obtener más información, consulte Distribución de contenido obsoleto (caducado).
> - CloudFront solo servirá un objeto que esté obsoleto hasta el valor TTL máximo especificado. Después de este tiempo, el objeto no estará disponible desde la caché perimetral.

Códigos de estado HTTP 4xx y 5xx que CloudFront almacena en caché

CloudFront almacena en caché códigos de estado HTTP 4xx y 5xx devueltos por su origen, en función del código de estado específico que se devuelve y de si el origen devuelve encabezados específicos en la respuesta.

CloudFront almacena en caché los siguientes códigos de estado HTTP 4xx y 5xx devueltos por el origen. Si ha configurado una página de error personalizada para un código de estado HTTP, CloudFront la almacena en caché.

> **Note**
>
> Si utiliza la política de caché administrada por CachingDisabled, CloudFront no almacenará en caché estos códigos de estado ni las páginas de error personalizadas.

404	no encontrado
414	URI de solicitud demasiado grande
500	Internal Server Error

501	No implementado
502	Puerta de enlace incorrecta
503	Servicio no disponible
504	Tiempo de espera de puerta de enlace agotado

Códigos de estado HTTP 4xx que CloudFront almacena en caché en función de los encabezados **`Cache-Control`**

CloudFront solo almacena en caché los siguientes códigos de estado HTTP 4xx devueltos por el origen si el origen devuelve un encabezado `Cache-Control max-age` o `Cache-Control s-maxage`. Si ha configurado una página de error personalizada para uno de estos códigos de estado HTTP, y el origen devuelve uno de los encabezados de control de la caché, CloudFront la almacena en caché.

400	solicitud errónea
403	Prohibido
405	método no permitido
412[1]	Condición previa con error
415[1]	Tipo de medio incompatible

[1] CloudFront no admite la creación de páginas de error personalizadas para estos códigos de estado HTTP.

Generación de respuestas de error personalizadas

Si un objetos que ofrece a través de CloudFront no está disponible por algún motivo, el servidor web suele devolver un código de estado HTTP a CloudFront. Por ejemplo, si un lector especifica una URL no válida, el servidor web devuelve un código de estado HTTP 404 (no encontrado) a CloudFront y CloudFront se lo devuelve al lector. En lugar de utilizar esta respuesta de error predeterminada, puede crear una respuesta personalizada que CloudFront devuelva al lector.

Si configura CloudFront para devolver una página de error personalizada para un código de estado HTTP pero la página de error personalizada no está disponible, CloudFront devuelve al lector el código de estado que CloudFront recibió del origen que contiene las páginas de error personalizadas. Por ejemplo, supongamos que el origen personalizado devuelve un código de estado 500 y que haya configurado CloudFront para obtener de un bucket de Amazon S3 una página de error personalizada para un código de estado 500. Sin embargo, alguien ha eliminado accidentalmente la página de error personalizada del bucket de Amazon S3. CloudFront devolverá un código de estado HTTP 404 (no encontrado) al lector que solicitó el objeto.

Cuando CloudFront devuelve una página de error personalizada a un lector, paga los cargos estándar de CloudFront por la página de error personalizada, no paga cargos por el objeto solicitado. Para obtener más información acerca de los cargos de CloudFront, consulte Precios de Amazon CloudFront.

Temas

- Configuración del comportamiento de respuestas de error
- Creación de una página de error personalizada para códigos de estado HTTP específicos
- Almacenamiento de objetos y páginas de error personalizadas en diferentes lugares
- Cambio de códigos de respuesta devueltos por CloudFront
- Control de cuánto tiempo CloudFront almacena los errores en caché

Configuración del comportamiento de respuestas de error

Tiene varias opciones para administrar cómo responde CloudFront cuando hay un error. Para configurar respuestas de errores personalizadas, puede utilizar la consola o la API de CloudFront o CloudFormation. Independientemente de cómo elija actualizar la configuración, tenga en cuenta las siguientes sugerencias y recomendaciones:

- Guarde las páginas de error personalizadas en una ubicación accesible para CloudFront. Le recomendamos que las almacene en un bucket de Amazon S3 y que no las almacene en el mismo lugar que el resto del contenido de su sitio web o aplicación. Si almacena las páginas de error personalizadas en el mismo origen que su sitio web o aplicación y el origen comienza a devolver errores 5xx, CloudFront no puede obtener las páginas de error personalizadas porque el servidor de origen no está disponible. Para obtener más información, consulte Almacenamiento de objetos y páginas de error personalizadas en diferentes lugares.
- Asegúrese de que CloudFront tenga permiso para obtener sus páginas de error personalizadas. Si las páginas de error personalizadas se almacenan en Amazon S3, deben ser accesibles públicamente o debe configurar un control de acceso de origen (OAC) de CloudFront. Si las páginas de error personalizadas se almacenan en un origen personalizado, deben ser accesibles públicamente.
- (Opcional) Configure su origen para agregar un encabezado `Cache-Control` o `Expires` junto con las páginas de error personalizadas, si lo desea. También puede utilizar la configuración TTL mínimo de almacenamiento de errores en caché para controlar cuánto tiempo CloudFront almacena en caché las páginas de error personalizadas. Para obtener más información, consulte Control de cuánto tiempo CloudFront almacena los errores en caché.

Configuración de respuestas de error personalizadas

Para configurar respuestas de error personalizadas en la consola de CloudFront, debe tener una distribución de CloudFront. En la consola, la configuración de las respuestas de error personalizadas solo está disponible para distribuciones existentes. Para obtener información sobre cómo crear una distribución, consulte Introducción a una distribución estándar de CloudFront.

Console

Para configurar respuestas de error personalizadas (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la página Distributions (Distribuciones) en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#distributions.
2. En la lista de distribuciones, elija la distribución que desea actualizar.
3. Elija la pestaña Error Pages (Páginas de error) y, a continuación, elija Create Custom Error Response (Crear respuesta de error personalizada).

4. Ingrese los valores aplicables. Para obtener más información, consulte Páginas de error personalizadas y almacenamiento de errores en caché.
5. Después de introducir los valores deseados, elija Create (Crear).

CloudFront API or CloudFormation

Para configurar respuestas de error personalizadas con la API de CloudFront o la CloudFormation, utilice el tipo `CustomErrorResponse` en una distribución. Para obtener más información, consulte los siguientes temas:

- AWS::CloudFront::Distribution CustomErrorResponse en la Guía del usuario de AWS CloudFormation
- CustomErrorResponse en la Referencia de la API de Amazon CloudFront

Creación de una página de error personalizada para códigos de estado HTTP específicos

Si prefiere mostrar un mensaje de error personalizado en lugar del mensaje predeterminado (por ejemplo, una página que utiliza el mismo formato que el resto del sitio web), puede hacer que CloudFront devuelva al lector un objeto (por ejemplo, un archivo HTML) que contenga el mensaje de error personalizado.

Para especificar el archivo que desea devolver y los errores por los que se debe devolver este archivo, debe actualizar la distribución de CloudFront y especificar esos valores. Para obtener más información, consulte Configuración del comportamiento de respuestas de error.

Por ejemplo, la siguiente es una página de error personalizada:

Puede especificar un objeto diferente por código de estado HTTP admitido o el mismo objeto para todos los códigos de estado admitidos. Puede elegir especificar páginas de error personalizadas para algunos códigos de estado y no para otros.

Los objetos que ofrece a través de CloudFront pueden no estar disponibles por diversas razones. Estas se dividen en dos amplias categorías:

- Errores de cliente, que indican un problema con la solicitud. Por ejemplo, un objeto con el nombre especificado no está disponible o el usuario no tiene los permisos necesarios para obtener un objeto en el bucket de Amazon S3. Cuando se produce un error de cliente, el origen devuelve a CloudFront un código de estado HTTP en el intervalo de los 4xx.
- Errores de servidor, que indican un problema con el servidor de origen. Por ejemplo, el servidor HTTP está ocupado o no disponible. Cuando se produce un error de servidor, el servidor de origen devuelve a CloudFront un código de estado HTTP en el intervalo de los 5xx o CloudFront no obtiene respuesta del servidor de origen durante un periodo determinado y supone un código de estado 504 (tiempo de espera de gateway agotado).

Los códigos de estado HTTP para los que CloudFront puede devolver una página de error personalizada son:

- 400, 403, 404, 405, 414, 416
- 500, 501, 502, 503, 504

> **Notas**
>
> - Si CloudFront detecta que la solicitud puede no ser segura, devuelve un error 400 (Solicitud incorrecta) en lugar de una página de error personalizada.
> - Puede crear una página de error personalizada para el código de estado HTTP 416 (Intervalo solicitado no puede ser satisfecho) y puede cambiar el código de estado HTTP que CloudFront proporciona a los lectores cuando el origen devuelve un código de estado 416 a CloudFront. Para obtener más información, consulte Cambio de códigos de respuesta devueltos por CloudFront. Sin embargo, CloudFront no almacena en caché las respuestas de los códigos de estado 416, así que, aunque especifique un valor para Error Caching Minimum TTL (TTL mínimo de almacenamiento de errores en caché) para el código de estado 416, CloudFront no lo utiliza.
> - En algunos casos, CloudFront no devuelve una página de error personalizada para el código de estado HTTP 503, incluso si configura CloudFront para hacerlo. Si el código de error de CloudFront es `Capacity Exceeded` o `Limit Exceeded`, CloudFront devuelve un código de estado 503 al lector sin utilizar la página de error personalizada.
> - Si ha creado una página de error personalizada, CloudFront devolverá `Connection: close` o `Connection: keep-alive` para los siguientes códigos de respuesta:
> - CloudFront devuelve `Connection: close` para los códigos de estado: 400, 405, 414, 416, 500 y 501
> - CloudFront devuelve `Connection: keep-alive` para los códigos de estado 403, 404, 502, 503 y 504

Para obtener una explicación detallada acerca de cómo CloudFront gestiona las respuestas de error del origen, consulte Procesamiento de CloudFront de los códigos de estado HTTP 4xx y 5xx desde el origen.

Almacenamiento de objetos y páginas de error personalizadas en diferentes lugares

Si desea almacenar los objetos y las páginas de error personalizadas en diferentes ubicaciones, la distribución debe incluir un comportamiento de la caché que cumpla con las siguientes condiciones:

- El valor de Path Pattern (Patrón de ruta) debe coincidir con la ruta de los mensajes de error personalizados. Por ejemplo, supongamos que ha guardado páginas para errores 4xx personalizadas en un bucket de Amazon S3 en un directorio llamado `/4xx-errors`. La distribución debe incluir un comportamiento de la caché cuyo patrón de ruta dirija las solicitudes de las páginas de error personalizadas a esa ubicación, por ejemplo, `/4xx-errors/*`.
- El valor de Origin (Origen) especifica el valor de Origin ID (ID de origen) del origen que contiene las páginas de error personalizadas.

Para obtener más información, consulte Configuración del comportamiento de la caché.

Cambio de códigos de respuesta devueltos por CloudFront

Puede configurar CloudFront para que devuelva al lector un código de estado HTTP diferente al que CloudFront recibió del origen. Por ejemplo, si el origen devuelve un código de estado 500 a CloudFront, es posible que desee que CloudFront devuelva una página de error personalizada y un código de estado 200 (OK) al lector. Existen diversas razones por las que puede querer que CloudFront devuelva al lector un código de estado diferente del que el origen ha devuelto a CloudFront:

- Algunos dispositivos de Internet (algunos firewalls y proxis corporativos, por ejemplo) interceptan los códigos de estado HTTP 4xx y 5xx y evitan que la respuesta se devuelva al lector. En este escenario, si sustituye `200`, la respuesta no se intercepta.
- Si no le resulta especialmente importante distinguir entre diferentes errores de servidor y de cliente, puede especificar `400` o `500` como el valor que CloudFront devuelve para todos los códigos de estado 4xx o 5xx.
- Quizá desee devolver un código de estado `200` (OK) y un sitio web estático para que sus clientes no sepan que su sitio web está caído.

Si habilita los registros estándar de CloudFront y configura CloudFront para cambiar el código de estado HTTP en la respuesta, el valor de la columna `sc-status` de los registros contiene el código de estado que se especifique. Sin embargo, el valor de la columna `x-edge-result-type` no se ve afectado. Contiene el tipo de resultado de la respuesta del origen. Por ejemplo: supongamos que configura CloudFront para devolver un código de estado de `200` al espectador cuando el origen devuelve `404` (No encontrado) a CloudFront. Cuando el origen responda a una solicitud con un código de estado `404`, el valor de la columna `sc-status` en el registro será `200`, pero el valor de la columna `x-edge-result-type` será `Error`.

Puede configurar CloudFront para devolver cualquiera de los siguientes códigos de estado HTTP junto con una página de error personalizada:

- 200
- 400, 403, 404, 405, 414, 416
- 500, 501, 502, 503, 504

Control de cuánto tiempo CloudFront almacena los errores en caché

CloudFront almacena en caché las respuestas de error durante una duración predeterminada de 10 segundos. A continuación, CloudFront envía la siguiente solicitud para el objeto al origen para ver si el problema que causó el error se ha resuelto y el objeto solicitado está disponible.

Puede especificar la duración de almacenamiento en caché de errores (Error Caching Minimum TTL [TTL mínimo de almacenamiento de errores en caché]) para cada código de estado 4xx y 5xx que CloudFront almacena en las caché. (Para obtener más información, consulte). Códigos de estado HTTP 4xx y 5xx que CloudFront almacena en caché.) Al especificar una duración, tenga en cuenta lo siguiente:

- Si se especifica una duración breve de almacenamiento de errores en caché, CloudFront reenvía más solicitudes al origen que si se especifica una mayor duración. En el caso de errores 5xx, esto podría agravar el problema que causó el origen para devolver un error.
- Cuando el origen devuelve un error por un objeto, CloudFront responde a las solicitudes de dicho objeto con la respuesta de error o con la página de error personalizada hasta que finaliza la duración de almacenamiento de errores en caché. Si especifica una duración de almacenamiento de errores en caché mayor, es posible que CloudFront continúe respondiendo a las solicitudes con una respuesta de error o la página de error personalizada durante mucho tiempo después de que el objeto vuelva a estar disponible.

> **Note**
>
> Puede crear una página de error personalizada para el código de estado HTTP 416 (Intervalo solicitado no puede ser satisfecho) y puede cambiar el código de estado HTTP que CloudFront proporciona a los lectores cuando el origen devuelve un código de estado 416 a CloudFront. (Para obtener más información, consulte Cambio de códigos de respuesta devueltos por CloudFront.) Sin embargo, CloudFront no almacena en caché las respuestas de los códigos de estado 416, así que, aunque especifique un valor para Error Caching

Minimum TTL (TTL mínimo de almacenamiento de errores en caché) para el código de estado 416, CloudFront no lo utiliza.

Si desea controlar el tiempo durante el cual CloudFront almacena errores para objetos individuales en la caché, puede configurar el servidor de origen para añadir el encabezado aplicable a la respuesta de error para dicho objeto.

Si el origen añade una directiva `Cache-Control: max-age` o `Cache-Control: s-maxage`, o un encabezado `Expires`, CloudFront almacena en caché respuestas de error para el valor mayor en el encabezado o el valor de Error Caching Minimum TTL (TTL mínimo de almacenamiento de errores en caché).

> **Note**
>
> Los valores `Cache-Control: max-age` y `Cache-Control: s-maxage` no pueden ser mayores que el valor de Maximum TTL (TTL máximo) definido para el comportamiento de la caché para el que se está obteniendo la página de error.

Si el origen agrega una directiva `Cache-Control: no-store`, `Cache-Control: no-cache` o `Cache-Control: private` para los códigos de error 404, 410, 414 o 501, CloudFront no almacena en caché la respuesta de error. Para todos los demás códigos de error, CloudFront ignora las directivas `no-store`, `no-cache` y `private`, y almacena en caché la respuesta de error con el valor del TTL mínimo de almacenamiento en caché de errores.

Si el origen añade otras directivas `Cache-Control` o no añade encabezados, CloudFront almacena en caché respuestas de error para el valor de Error Caching Minimum TTL (TTL mínimo de almacenamiento de errores en caché).

Si la fecha de vencimiento de un código de estado 4xx o 5xx de un objeto es más lejana de lo que desea y el objeto está disponible nuevamente, puede invalidar el código de error almacenado en caché utilizando la URL del objeto solicitado. Si el origen devuelve una respuesta de error para varios objetos, es necesario invalidar cada uno de los objetos por separado. Para obtener más información acerca de las invalidaciones de objetos, consulte Invalidación de archivos para eliminar el contenido.

Si tiene habilitado el almacenamiento en caché para un origen de bucket de S3 y configura un error que almacena en caché el TTL mínimo de 0 segundos en su distribución de CloudFront, seguirá apareciendo un error al almacenar en caché el TTL mínimo de 1 segundo en los errores de origen de

S3. CloudFront lo hace para proteger su origen de los ataques DDoS. Esto no se aplica a otros tipos de orígenes.

Agregación, eliminación o sustitución de contenido que distribuye CloudFront

En esta sección se explica cómo asegurarse de que CloudFront pueda acceder al contenido que desea distribuir a los lectores, cómo especificar los objetos en su sitio web o en su aplicación y cómo quitar o reemplazar contenido.

Temas

- Agregación de contenido que distribuye CloudFront y acceso al mismo
- Uso del control de versiones de los archivos para actualizar o eliminar contenido con una distribución de CloudFront
- Personalización del formato de URL para archivos en CloudFront
- Especificación de un objeto raíz predeterminado
- Invalidación de archivos para eliminar el contenido
- Ofrecimiento de archivos comprimidos

Agregación de contenido que distribuye CloudFront y acceso al mismo

Si desea que CloudFront distribuya contenido (objetos), agregue archivos a uno de los orígenes que haya especificado para la distribución y exponga un enlace de CloudFront a los archivos. Una ubicación periférica de CloudFront no recupera los nuevos archivos desde un origen hasta que la ubicación periférica recibe solicitudes de lectores para ellos. Para obtener más información, consulte Cómo CloudFront entrega el contenido.

Cuando agrega un archivo que desee que CloudFront distribuya, asegúrese de agregarlo a uno de los buckets de Amazon S3 especificados en la distribución o, en el caso de un origen personalizado, a un directorio en el dominio especificado. Confirme también que el patrón de ruta en el comportamiento de la caché aplicable envía solicitudes al origen correcto.

Por ejemplo, suponga que el patrón de una ruta de comportamiento de la caché es `*.html`. Si no dispone de ningún otro comportamiento de caché configurado para reenviar solicitudes a dicho origen, CloudFront solo reenviará archivos `*.html`. En este caso, por ejemplo, CloudFront nunca

distribuirá archivos .jpg que carga al origen, ya que no ha creado un comportamiento de caché que incluya archivos .jpg.

Los servidores de CloudFront no determinan el tipo MIME de los objetos que distribuyen. Al cargar un archivo en su origen, le recomendamos que establezca el campo de encabezado `Content-Type` del mismo.

Uso del control de versiones de los archivos para actualizar o eliminar contenido con una distribución de CloudFront

Para actualizar el contenido existente que CloudFront tiene configurado para distribuir por usted, le recomendamos que utilice un identificador de versión en los nombres de archivos o en los nombres de carpetas. Esto le permite controlar la administración del contenido que entrega CloudFront.

Actualización de archivos existentes con versiones de nombres de archivos

Al actualizar los archivos existentes en una distribución de CloudFront, le recomendamos incluir algún identificador de versión en sus nombres de archivo o de directorios para tener un mejor control de su contenido. Este identificador puede ser una marca temporal fecha-hora, un número en secuencia o algún otro método que permita distinguir dos versiones del mismo objeto.

Por ejemplo, en lugar de denominar un archivo de imagen image.jpg, puede llamarlo image_1.jpg. Cuando desee comenzar a ofrecer una nueva versión del archivo, deberá llamarlo image_2.jpg y actualizar los enlaces en su sitio o aplicación web para que apunten a image_2.jpg. De forma alternativa, puede colocar todos los gráficos en un directorio images_v1 y, cuando desee comenzar a distribuir nuevas versiones de uno o varios gráficos, crear un nuevo directorio images_v2 y actualizar los enlaces para apuntar a dicho directorio. Con el control de versiones, no es necesario esperar a que un objeto caduque antes de que CloudFront comience a ofrecer una nueva versión del mismo ni pagar por la invalidación de objetos.

Incluso si crea versiones de sus archivos, recomendamos que defina una fecha de vencimiento. Para obtener más información, consulte Administración de cuánto tiempo se mantiene el contenido en una caché (vencimiento).

> **Note**
>
> Especificar nombres de archivo o de directorios con versiones no está relacionado con el control de versiones de objetos de Amazon S3.

Eliminación de contenido para que CloudFront no lo distribuya

Puede quitar archivos de su origen que ya no desee incluir en su distribución de CloudFront. Sin embargo, CloudFront seguirá mostrando a los lectores contenido desde la caché de borde hasta que los archivos caduquen.

Si desea quitar un archivo de forma inmediata, debe realizar una de estas acciones:

- Utilizar el control de versiones de archivos. Cuando se utiliza el control de versiones, las distintas versiones de un archivo tienen diferentes nombres que puede usar en su distribución de CloudFront, para cambiar el archivo que se devuelve a los lectores. Para obtener más información, consulte Actualización de archivos existentes con versiones de nombres de archivos.
- Invalidar el archivo. Para obtener más información, consulte Invalidación de archivos para eliminar el contenido.

Personalización del formato de URL para archivos en CloudFront

Después de configurar el origen con los objetos (contenido) que desee que CloudFront distribuya a los lectores, debe utilizar las URL correctas para hacer referencia a dichos objetos en su sitio web o código de aplicación para que CloudFront puede distribuirlo.

El nombre de dominio que utiliza en las URL de los objetos en sus páginas web o en su aplicación web puede ser uno de los siguientes:

- El nombre de dominio, como `d111111abcdef8.cloudfront.net`, que CloudFront asigna automáticamente al crear una distribución
- Su propio nombre de dominio, como `example.com`

Por ejemplo, puede utilizar una de las siguientes URL para devolver el archivo `image.jpg`:

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

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

Puede utilizar el mismo formato de URL si almacena el contenido en buckets de Amazon S3 o en un origen personalizado, como uno de sus servidores web.

> **Note**
>
> El formato de URL depende en parte del valor que especifique para Origin Path (Ruta de origen) en su distribución. Este valor ofrece a CloudFront una ruta de directorio de nivel superior para sus objetos. Para obtener más información sobre la configuración de la ruta de origen al crear una distribución, consulte Ruta de origen.

Para obtener más información sobre los formatos de URL, consulte las siguientes secciones.

Uso de su propio nombre de dominio (example.com)

En lugar de utilizar el nombre de dominio predeterminado que CloudFront le asigna al crear una distribución, puede agregar un nombre de dominio alternativo con el que sea más fácil trabajar, como `example.com`. Al configurar su propio nombre de dominio con CloudFront, puede utilizar una URL como esta para los objetos de su distribución:

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

Si tiene previsto utilizar HTTPS entre los lectores y CloudFront, consulte Uso de nombres de dominio alternativos y HTTPS.

Uso de un delimitador final (/) en las URL

Cuando especifique direcciones URL para los directorios de la distribución de CloudFront, elija si utilizará siempre una barra final o si nunca la utilizará. Por ejemplo, elija solo uno de los siguientes formatos para todas las direcciones URL:

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

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

¿Por qué importa?

Ambos formatos son válidos para el enlace a objetos de CloudFront, pero el hecho de ser coherente puede ayudar a prevenir problemas cuando desea invalidar un directorio más tarde. CloudFront almacena las URL exactamente como se definen, incluidas las barras finales. Por tanto, si el formato es incoherente, tendrá que invalidar las URL de directorio con y sin la barra, para garantizar que CloudFront quite el directorio.

Resulta incómodo tener que invalidar ambos formatos de URL y puede suponer costos adicionales. Esto se debe a que si hay que duplicar las invalidaciones para cubrir ambos tipos de URL, se podría exceder el número máximo de invalidaciones gratuitas permitidas durante el mes. Y si esto ocurre, tendrá que pagar por todas las invalidaciones, aunque solo exista en CloudFront un formato para cada URL de directorio.

Creación de URL firmadas para contenido restringido

Si tiene contenido al que desea restringir el acceso, puede crear URL firmadas. Por ejemplo, si desea distribuir su contenido únicamente a los usuarios que se hayan autenticado, puede crear unas URL que solo sean válidas durante un periodo de tiempo indicado o que solo estén disponibles desde una dirección IP especificada. Para obtener más información, consulte Distribución de contenido privado con URL firmadas y cookies firmadas.

Especificación de un objeto raíz predeterminado

Puede configurar CloudFront para devolver un objeto específico (el objeto raíz predeterminado) cuando un usuario (espectador) solicita la URL raíz de su distribución en lugar de solicitar un objeto de su distribución. Puede usar un objeto raíz predeterminado para evitar la exposición del contenido de su distribución.

Contenido

- Cómo especificar un objeto raíz predeterminado
- Cómo funciona el objeto raíz predeterminado
- Cómo funciona CloudFront si no define un objeto raíz

Cómo especificar un objeto raíz predeterminado

Para evitar exponer el contenido de la distribución o devolver un error, especifique un objeto raíz predeterminado para la distribución. Puede especificar el nombre exacto del archivo o la ruta al archivo. Por ejemplo, si el objeto raíz es un archivo `index.html`, puede especificar el nombre de ese archivo. Si el archivo `index.html` está en otra carpeta, especifique la ruta en su lugar; por ejemplo, *`exampleFolderName`*`/index.html`. Si establece una ruta al objeto raíz predeterminado, las solicitudes de los espectadores a la URL raíz de la distribución devolverán el archivo especificado desde esa ruta. Puede usar una ruta de archivo para tener más flexibilidad a la hora de organizar el contenido en el origen, ya que el objeto raíz predeterminado puede estar en una carpeta en lugar de en el nivel raíz.

Especificar un objeto raíz predeterminado para su distribución

1. Cargue el objeto raíz predeterminado al origen al que apunta su distribución.

   El archivo puede ser cualquier tipo admitido por CloudFront. Para obtener una lista de las limitaciones de los nombres de archivo, consulte el elemento `DefaultRootObject` en DistributionConfig de la Referencia de la API de Amazon CloudFront.

   > **Note**
   >
   > Si el nombre de archivo del objeto raíz predeterminado es demasiado largo o contiene caracteres no válidos, CloudFront devuelve el error `HTTP 400 Bad Request - InvalidDefaultRootObject`. Además, CloudFront almacena en caché el código durante 10 segundos (de forma predeterminada) y escribe los resultados en los registros de acceso.

2. Confirme que los permisos del objeto conceden a CloudFront al menos acceso de lectura.

   Para obtener más información acerca de los permisos de Amazon S3, consulte Administración de la identidad y el acceso en Amazon S3 en la Guía para usuarios de Amazon Simple Storage Service.

3. Actualice la distribución para referirse al objeto raíz predeterminado mediante la consola de CloudFront o la API de CloudFront.

   Para especificar un objeto raíz predeterminado mediante la consola de CloudFront:

   a. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
   b. En la lista de distribuciones que se encuentra en el panel superior, seleccione la distribución a actualizar.
   c. En el panel Settings (Configuración), en la pestaña General, elija Edit (Editar).
   d. En el cuadro de diálogo Editar configuración, en el campo Objeto raíz predeterminado, escriba el nombre de archivo del objeto raíz predeterminado.

      > **Tip**
      >
      > La cadena no puede comenzar con una barra diagonal (`/`). Especifique únicamente el nombre del objeto o la ruta al objeto. Por ejemplo, utilice `index.html` o

> *exampleFolderName*/index.html. Si se especifica **/***exampleFolderName***/**index.html o **/**index.html, se puede producir un error 403 Acceso denegado.

e. Seleccione Save changes (Guardar cambios).

Para actualizar la configuración mediante la API de CloudFront, especifique un valor en el elemento `DefaultRootObject` de su distribución. Para obtener información sobre el uso de la API de CloudFront para especificar un objeto raíz predeterminado, consulte UpdateDistribution en la Referencia de la API de Amazon CloudFront.

4. Realice una solicitud de su URL raíz para confirmar si el objeto raíz predeterminado está habilitado. Si el navegador no muestra el objeto raíz predeterminado, siga los pasos siguientes:

   a. Consulte el estado de su distribución en la consola de CloudFront para confirmar que está implementada por completo.

   b. Repita los pasos 2 y 3 para verificar que ha concedido los permisos pertinentes y que ha actualizado correctamente la configuración de la distribución para especificar el objeto raíz predeterminado.

Cómo funciona el objeto raíz predeterminado

Suponga que la siguiente solicitud apunta al objeto `image.jpg`:

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

Por el contrario, la siguiente solicitud apunta a la URL raíz de la misma distribución en lugar de a un objeto específico, como en el primer ejemplo:

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

Si define un objeto raíz predeterminado, cualquier solicitud de un usuario final que realice una llamada a la raíz de su distribución devolverá el objeto raíz predeterminado. Por ejemplo, si designa el archivo `index.html` como su objeto raíz predeterminado, una solicitud de:

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

Devuelve:

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

> **Note**
>
> CloudFront no determina si una URL con varias barras diagonales al final (`https://d111111abcdef8.cloudfront.net///`) es equivalente a `https://d111111abcdef8.cloudfront.net/`. Su servidor de origen hace esa comparación.

Si define un objeto raíz predeterminado, una solicitud de un usuario final que realice una llamada a un subdirectorio de su distribución no devolverá el objeto raíz predeterminado. Supongamos que `index.html` es su objeto raíz predeterminado y que CloudFront recibe una solicitud de parte de un usuario final, del directorio `install` que se encuentra en su distribución de CloudFront:

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

CloudFront no devuelve el objeto raíz predeterminado incluso si hay una copia de `index.html` en el directorio `install`. Sin embargo, si especificó una ruta al objeto raíz predeterminado, (`install/index.html`) CloudFront devolverá el objeto raíz predeterminado para las solicitudes de los usuarios finales al directorio `install`.

Si configura su distribución para permitir todos los métodos de HTTP que admite CloudFront, el objeto raíz predeterminado se aplicará a todos ellos. Por ejemplo, si su objeto raíz predeterminado es index.php y escribe su aplicación para enviar una solicitud `POST` a la raíz de su dominio (https://example.com), CloudFront envía la solicitud a https://example.com/index.php.

El comportamiento de los objetos raíz predeterminados de CloudFront es diferente del comportamiento de los documentos del índice de Amazon S3. Al configurar un bucket de Amazon S3 como un sitio web y especificar el documento de índice, Amazon S3 devuelve dicho documento incluso si un usuario solicita un subdirectorio del bucket. (Deberá aparecer una copia del documento de índice en cada subdirectorio). Para obtener más información sobre la configuración de buckets de Amazon S3 como sitios web y sobre documentos de índice, consulte el capítulo Hosting de sitios web en Amazon S3 de la Guía del usuario de Amazon Simple Storage Service.

> **Important**
>
> Recuerde que un objeto raíz predeterminado es aplicable únicamente a su distribución de CloudFront. Aún tendrá que administrar la seguridad de su origen. Por ejemplo, si utiliza un origen de Amazon S3, deberá configurar las ACL de su bucket de Amazon S3 de forma tal que se asegure el nivel de acceso que desea en dicho bucket.

Cómo funciona CloudFront si no define un objeto raíz

Si no define un objeto raíz predeterminado, las solicitudes de la raíz de su distribución pasarán a su servidor de origen. Si utiliza un origen de Amazon S3, es posible que se devuelva cualquiera de los siguientes elementos:

- Una lista del contenido de su bucket de Amazon S3: cualquier persona que utilice CloudFront para obtener acceso a su distribución podrá ver el contenido de su origen si se cumple cualquiera de estas condiciones:
  - Si su bucket no está configurado correctamente.
  - Si los permisos de Amazon S3 del bucket asociado a su distribución y de los objetos del bucket conceden acceso a todo el mundo.
  - Si un usuario final obtiene acceso a su origen mediante la URL raíz del origen.
- Una lista del contenido privado de su origen: si configura el origen como una distribución privada (solo usted y CloudFront tienen acceso), cualquiera que tenga las credenciales para obtener acceso a la distribución a través de CloudFront podrá ver el contenido del bucket de Amazon S3 asociado a su distribución. En este caso, los usuarios no podrán obtener acceso a su contenido a través de la URL raíz del origen. Para obtener más información acerca de la distribución de contenido privado, consulte the section called “Restricción de contenido con URL firmadas y cookies firmadas”.
- `Error 403 Forbidden`: CloudFront devuelve este error si los permisos del bucket de Amazon S3 asociado a la distribución o los permisos de los objetos de dicho bucket deniegan el acceso a CloudFront y a los demás usuarios.

Invalidación de archivos para eliminar el contenido

Si necesita quitar un archivo de cachés de borde de CloudFront antes de que caduquen, puede elegir una de las siguientes alternativas:

- Invalide el archivo de las cachés perimetrales. La vez siguiente que un lector solicita el archivo, CloudFront vuelve al origen para recuperar la última versión.
- Utilice el control de versiones de archivos para ofrecer una versión diferente del archivo con un nombre distinto. Para obtener más información, consulte Actualización de archivos existentes con versiones de nombres de archivos.

Temas

- Elección entre invalidar archivos y utilizar nombres de archivo con versiones
- Determinación de qué archivos invalidar
- Qué se debe saber al invalidar archivos
- Invalidación de archivos
- Máximo de solicitud de invalidación simultánea
- Cargos por invalidación de archivo

Elección entre invalidar archivos y utilizar nombres de archivo con versiones

Para controlar las versiones de los archivos que se distribuyen desde su distribución, puede invalidar archivos o asignarles nombres de archivo con versiones. Si desea actualizar sus archivos con frecuencia, le recomendamos utilizar principalmente el control de versiones de archivos por las siguientes razones:

- El control de versiones le permite controlar qué archivo devuelve una solicitud incluso cuando el usuario tiene una versión almacenada en caché, ya sea localmente o tras un proxy de almacenamiento en caché de empresa. Si invalida el archivo, el usuario podría seguir viendo la versión antigua hasta que caduque en esas cachés.
- Los registros de acceso de CloudFront incluyen los nombres de los archivos, así que el control de versiones facilita el análisis de los resultados de los cambios de archivos.
- El control de versiones es una forma de ofrecer distintas versiones de archivos a diferentes usuarios.
- El control de versiones simplifica la progresión y restauración de archivos entre revisiones.
- El control de versiones es más económico. Todavía tendrá que pagar la transferencia que hace CloudFront de las nuevas versiones de los archivos a ubicaciones periférica, pero no tendrá que pagar por la invalidación de archivos.

Para obtener más información acerca del control de versiones, consulte Actualización de archivos existentes con versiones de nombres de archivos.

Determinación de qué archivos invalidar

Si desea invalidar varios archivos como, por ejemplo, todos los archivos de un directorio o todos los archivos que comienzan por los mismos caracteres, puede incluir el comodín `*` al final de la ruta de invalidación. Para obtener más información acerca de cómo utilizar el comodín `*`, consulte Invalidation paths.

Para invalidar archivos, puede especificar la ruta de archivos individuales o una ruta que termine en el comodín `*`, que puede ser aplicable a un archivo o a muchos, tal y como se muestra en los siguientes ejemplos:

- `/images/image1.jpg`
- `/images/image*`
- `/images/*`

Si desea invalidar archivos seleccionados, pero los usuarios no necesariamente obtienen acceso a todos los del origen, puede determinar qué archivos de CloudFront han sido solicitados por lectores e invalidar solo esos. Para determinar qué archivos han solicitado los lectores, habilite el registro de acceso de CloudFront. Para obtener más información acerca de los registros de acceso, consulte Registros de acceso (registros estándar).

Qué se debe saber al invalidar archivos

Al especificar los archivos para invalidarlos, consulte la siguiente información:

Sensibilidad de mayúsculas y minúsculas

En las rutas de invalidación se distingue entre mayúsculas y minúsculas. Por ejemplo, `/images/image.jpg` y `/images/Image.jpg` especifican dos archivos diferentes.

Cambio del URI mediante una función de Lambda

Si su distribución de CloudFront activa una función de Lambda en eventos de solicitud del lector, y si la función cambia el URI del archivo solicitado, recomendamos que invalide ambos URI para quitar el archivo de las cachés de borde de CloudFront:

- El URI de la solicitud del espectador
- El URI después de que la función lo cambiara

Example Ejemplo

Suponga que su función de Lambda cambia el URI de un archivo de la siguiente manera:

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

Por un URI que incluye un directorio de idioma:

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

Para invalidar el archivo, debe especificar las siguientes rutas:

- `/index.html`
- `/en/index.html`

Para obtener más información, consulte Invalidation paths.

Objeto raíz predeterminado

Para invalidar el objeto raíz predeterminado (archivo), especifique la ruta del mismo modo que especifica la de cualquier otro archivo. Para obtener más información, consulte Cómo funciona el objeto raíz predeterminado.

Reenvío de cookies

Si configura CloudFront para reenviar cookies a su origen, las cachés de borde de CloudFront pueden contener varias versiones del archivo. Al invalidar un archivo, CloudFront invalida todas las versiones del archivo almacenado en caché independientemente de sus cookies asociadas. No se puede invalidar de manera selectiva algunas versiones y otras no en función de las cookies asociadas. Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.

Reenvío de encabezados

Si configuró CloudFront para reenviar una lista de encabezados a su origen y para almacenar en caché en función de los valores de los encabezados, las cachés de borde de CloudFront podrían contener varias versiones del archivo. Al invalidar un archivo, CloudFront invalida todas las versiones del archivo almacenado en caché independientemente de los valores de los encabezados. No se puede invalidar de manera selectiva algunas versiones y otras no en función de los valores de los encabezados. (Si configura CloudFront para reenviar todos los encabezados a su origen, CloudFront no almacenará en caché los archivos). Para obtener más información, consulte Almacenamiento en caché de contenido en función de encabezados de solicitud.

Reenvío de cadenas de consulta

Si configura CloudFront para que reenvíe cadenas de consultas a su origen, deberá incluir las cadenas de consulta a la hora de invalidar archivos, tal y como se muestra en los siguientes ejemplos:

- `/images/image.jpg?parameter1=a`
- `/images/image.jpg?parameter1=b`

Si los clientes incluyen cinco cadenas de consulta diferentes para el mismo archivo, puede invalidar el archivo cinco veces, una vez por cadena de consulta, o utilizar el comodín * en la ruta, tal y como se muestra en el ejemplo siguiente:

```
/images/image.jpg*
```

Para obtener más información acerca del uso de comodines en la ruta de invalidación, consulte Invalidation paths.

Para obtener más información acerca de cadenas de consulta, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta.

Para determinar qué cadenas de consulta están en uso, puede habilitar el registro de CloudFront. Para obtener más información, consulte Registros de acceso (registros estándar).

Máximo permitido

Para obtener más información sobre el número máximo de invalidaciones permitidas, consulte Máximo de solicitud de invalidación simultánea.

Microsoft Smooth Streaming files

No es posible invalidar archivos multimedia en el formato de Microsoft Smooth Streaming si se ha activado Smooth Streaming para el comportamiento de la caché correspondiente.

Caracteres no ASCII o no seguros en la ruta

Si la ruta incluye caracteres no ASCII o no seguros, tal y como se define en RFC 1738, codifique los caracteres como URL. No codifique como URL otros caracteres de la ruta, o CloudFront no invalidará la versión antigua del archivo actualizado.

> **Important**
>
> No utilice el carácter ~ en la ruta. CloudFront no admite este carácter para las invalidaciones, ya sea codificado mediante URL o no.

Rutas de invalidación

La ruta es relativa a la distribución. Por ejemplo, para invalidar el archivo en `https://d111111abcdef8.cloudfront.net/images/image2.jpg`, especifique `/images/image2.jpg`.

> **Note**
>
> En la consola de CloudFront, puede omitir la barra diagonal inicial en la ruta, así: `images/image2.jpg`. Cuando se utiliza la API de CloudFront directamente, las rutas de invalidación deben comenzar con una barra diagonal a la izquierda.

También puede invalidar varios archivos simultáneamente mediante el comodín `*`. El `*`, que sustituye a 0 o más caracteres, debe ser el último carácter de la ruta de invalidación.

> **Important**
>
> Para utilizar comodines (*) en la invalidación, debe poner el comodín al final de la ruta. Los asteriscos (*) insertados en cualquier otro lugar se tratan como una coincidencia literal de caracteres en lugar de una invalidación de comodines.

Si utiliza la AWS Command Line Interface (AWS CLI) para la invalidación de archivos y especifica una ruta que incluya el comodín `*`, debe utilizar comillas (`"`) para delimitar la ruta de la siguiente manera: `"/*"`.

La longitud máxima de una ruta es 4 000 caracteres.

Example Ejemplo: Rutas de invalidación

- Para invalidar todos los archivos de un directorio:

  ```
  /ruta-directorio/*
  ```

- Para invalidar un directorio, todos sus subdirectorios y todos los archivos en el directorio y subdirectorios:

  `/ruta-directorio*`

- Para invalidar todos los archivos que tienen el mismo nombre, pero diferentes extensiones, como logo.jpg, logo.png y logo.gif:

  `/ruta-directorio/nombre-archivo.*`

- Para invalidar todos los archivos de un directorio cuyos nombres comienzan por los mismos caracteres (como, por ejemplo, todos los archivos de video en formato HLS), independientemente de la extensión del nombre del archivo:

  `/ruta-directorio/primeros-caracteres-nombre-archivo*`

- Si ha configurado CloudFront para almacenar en caché en función de los parámetros de cadenas de consulta y desea invalidar todas las versiones de un archivo:

  `/ruta-directorio/nombre-archivo.extensión-nombre-archivo*`

- Para invalidar todos los archivos de una distribución:

  `/*`

Para obtener información sobre la invalidación de archivos si utiliza una función de Lambda para cambiar el URI, consulte Changing the URI Using a Lambda Function.

Si la ruta de invalidación es un directorio y no ha estandarizado un método para especificar directorios (con o sin barra inclinada, /, al final), le recomendamos invalidar el directorio con y sin barra inclinada al final, por ejemplo, `/images` y `/images/`.

URL firmadas

Si utiliza URL firmadas, invalide un archivo incluyendo solo la parte de la URL anterior al signo de interrogación (?).

Invalidación de archivos

Puede utilizar la consola de CloudFront para crear y ejecutar una invalidación, mostrar una lista de las invalidaciones que ha enviado anteriormente y mostrar información detallada acerca de invalidaciones individuales. También puede copiar una invalidación existente, editar la lista de las rutas de archivos y ejecutar la invalidación editada. No puede eliminar las invalidaciones de la lista.

Contenido

- Invalidación de archivos
- Copia, edición y nueva ejecución de una invalidación existente
- Cancelación de invalidaciones
- Enumeración de invalidaciones
- Visualización de información acerca de una invalidación

Invalidación de archivos

Para invalidar archivos mediante la consola de CloudFront, haga lo siguiente.

Console

Invalidación de archivos (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la distribución cuyos archivos desea invalidar.
3. Elija la pestaña Invalidations (Invalidaciones).
4. Elija Crear invalidación.
5. Escriba una ruta de invalidación de cada archivo que desea invalidar por línea. Para obtener más información acerca de cómo especificar rutas de invalidación, consulte Qué se debe saber al invalidar archivos.

   > **Important**
   >
   > Especifique las rutas de archivos cuidadosamente. Las solicitudes de invalidación no se pueden cancelar una vez comenzadas.

6. Elija Crear invalidación.

CloudFront API

Para obtener más información acerca de la invalidación de objetos y mostrar información acerca de invalidaciones, consulte los siguientes temas en la Referencia de la API de Amazon CloudFront:

- CreateInvalidation
- ListInvalidations
- GetInvalidation

> **Note**
>
> Si utiliza la AWS Command Line Interface (AWS CLI) para la invalidación de archivos y especifica una ruta que incluya el comodín *, debe utilizar comillas (") para delimitar la ruta, como en el siguiente ejemplo:
>
> ```
> aws cloudfront create-invalidation --distribution-id distribution_ID --paths
> "/*"
> ```

Copia, edición y nueva ejecución de una invalidación existente

Puede copiar invalidaciones que haya creado anteriormente, actualizar la lista de rutas de invalidación y ejecutar las invalidaciones actualizadas. No es posible copiar invalidaciones existentes, actualizar rutas de invalidación ni guardar invalidaciones actualizadas a continuación sin ejecutarlas.

> **Important**
>
> Si copia una invalidación que sigue en curso, actualiza la lista de rutas de anulación y, a continuación, ejecuta la invalidación actualizada, CloudFront no detiene ni elimina la invalidación que ha copiado. Si aparece cualquier ruta de invalidación en el original y en la copia, CloudFront intentará invalidar los archivos dos veces, y ambas invalidaciones se contabilizarán como parte de la cantidad máxima de invalidaciones gratuitas del mes. Si ya se ha alcanzado la cantidad máxima de invalidaciones gratuitas, se le facturarán las invalidaciones de ambos archivos. Para obtener más información, consulte Máximo de solicitud de invalidación simultánea.

Para copiar, editar y volver a ejecutar una invalidación existente

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.

2. Elija la distribución que contiene la invalidación que desea copiar.
3. Elija la pestaña Invalidaciones.
4. Elija la invalidación que desea copiar.

   Si no está seguro de qué invalidación desea copiar, puede elegir una invalidación y elegir Ver detalles para mostrar información detallada sobre ella.
5. Seleccione Copiar en uno nuevo.
6. Actualice la lista de rutas de invalidación si procede.
7. Elija Crear invalidación.

Cancelación de invalidaciones

Al enviar una solicitud de invalidación a CloudFront, CloudFront reenvía la solicitud a todas las ubicaciones periférica al cabo de unos segundos, y cada ubicación periférica comienza a procesar la invalidación de forma inmediata. Por consiguiente, no puede cancelar una invalidación después de enviarla.

Enumeración de invalidaciones

Puede mostrar una lista de las 100 últimas invalidaciones que ha creado y ejecutado para una distribución utilizando la consola de CloudFront. Si desea obtener una lista de más de 100 invalidaciones, utilice la operación de la API `ListInvalidations`. Para obtener más información, consulte ListInvalidations en la Referencia de la API de Amazon CloudFront.

Para mostrar una lista de invalidaciones

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la distribución cuyas invalidaciones desee mostrar en una lista.
3. Elija la pestaña Invalidations (Invalidaciones).

> **Note**
>
> No puede eliminar las invalidaciones de la lista.

Visualización de información acerca de una invalidación

Visualice información detallada sobre cualquier invalidación, incluidos ID de distribución y de invalidación, estado de la invalidación, la fecha y la hora de creación de la invalidación y una lista completa de las rutas de invalidación.

Para mostrar información acerca de una invalidación

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la distribución que contenga la invalidación de la que desea mostrar información detallada.
3. Elija la pestaña Invalidaciones.
4. Elija el ID de invalidación correspondiente o seleccione el ID de invalidación y, a continuación, seleccione Ver detalles.

Máximo de solicitud de invalidación simultánea

Si está invalidando archivos uno a uno, podría haber solicitudes de invalidación de hasta 3000 archivos por distribución en ejecución simultáneamente. Podría tratarse de una sola solicitud de invalidación para hasta 3000 archivos, hasta 3000 solicitudes de un archivo cada una o cualquier otra combinación que no supere 3000 archivos. Por ejemplo, puede enviar 30 solicitudes de invalidación para 100 archivos cada una. Mientras las 30 solicitudes de invalidación estén realizándose, no se pueden enviar más solicitudes de invalidación. Si supera el máximo, CloudFront devuelve un mensaje de error.

Si está utilizando el comodín *, puede tener solicitudes de hasta 15 patrones de invalidación ejecutándose simultáneamente. También puede tener solicitudes de invalidación de hasta 3000 archivos individuales por distribución ejecutándose simultáneamente; el máximo permitido de solicitudes de invalidación con comodines es independiente del máximo de invalidación de archivos individuales.

Cargos por invalidación de archivo

Las primeras 1 000 rutas de invalidación que envíe al mes son gratis; cada ruta de invalidación adicional a las 1 000 mensuales genera cargos. Una ruta de invalidación puede ser aplicable a un único archivo (por ejemplo, `/images/logo.jpg`) o a varios archivos (como, por ejemplo, `/images/*`). Cualquier ruta que incluya el comodín `*` cuenta como una ruta incluso si hace que CloudFront invalide miles de archivos.

Este máximo de 1000 rutas de invalidación gratuitas al mes se aplica al número total de rutas de invalidación de todas las distribuciones que haya creado con una Cuenta de AWS. Por ejemplo, si utiliza la Cuenta de AWS `john@example.com` para crear tres distribuciones y envía 600 rutas de invalidación para cada distribución en un mes determinado (para un total de 1800 rutas de invalidación), AWS le cobrará la diferencia entre el total de rutas de invalidación y el límite gratuito de 1000. En este ejemplo, AWS le cobraría 800 rutas de invalidación en ese mes.

El cargo por enviar una ruta de invalidación es la misma independientemente de la cantidad de archivos que invalide: un único archivo (`/images/logo.jpg`) o todos los archivos asociados a una distribución (`/*`). Dado que se le cobra por ruta en la solicitud de invalidación, incluso si agrupa varias rutas en una sola solicitud, cada ruta se sigue contando de forma individual a efectos de facturación.

Para obtener más información acerca de los precios de invalidación, consulte Precios de Amazon CloudFront. Para obtener más información acerca de rutas de invalidación, consulte Invalidation paths.

Ofrecimiento de archivos comprimidos

Al comprimir los objetos solicitados, las descargas son más rápidas, ya que los objetos son más pequeños: en algunos casos, menos de una cuarta parte del original. Las descargas más rápidas pueden resultar en páginas web que se muestran más rápido a los lectores, especialmente para archivos de JavaScript y CSS. Además, el costo de transferencia de datos de CloudFront se basa en la cantidad total de datos ofrecidos. Ofrecer objetos comprimidos puede resultar menos costoso que ofrecerlos sin comprimir.

Temas

- Configuración de CloudFront para comprimir objetos
- Cómo funciona la compresión de CloudFront
- Condiciones para la compresión
- Tipos de archivos que CloudFront comprime
- ETagConversión de encabezado

Configuración de CloudFront para comprimir objetos

Si quiere configurar CloudFront para comprimir objetos, actualice el comportamiento de la caché al que desea ofrecer objetos comprimidos.

Configuración de CloudFront para comprimir objetos (consola)

1. Inicie sesión en la consola de CloudFront.
2. Elija la distribución y, a continuación, elija el Comportamiento que desee editar.
3. En la configuración de Comprimir objetos automáticamente, elija Sí.
4. Utilice una política de caché para especificar la configuración de almacenamiento en caché y habilite los formatos de compresión Gzip y Brotli.

> **Notas**
>
> - Debe usar políticas de caché para usar la compresión Brotli. Brotli no admite la configuración de caché heredada.
> - Para habilitar la compresión mediante CloudFormation o la API de CloudFront, establezca los parámetros `Compress`, `EnableAcceptEncodingGzip`, `EnableAcceptEncodingBrotli` en `true`.

Para entender cómo CloudFront comprime los objetos, consulte la siguiente sección.

Cómo funciona la compresión de CloudFront

1. Un espectador solicita un objeto. El lector incluye el encabezado HTTP `Accept-Encoding` en la solicitud, y los valores de encabezado incluyen `gzip`, `br` o ambos. Esto indica que el lector admite objetos comprimidos. Cuando el lector admite Gzip y Brotli, CloudFront usa Brotli.

   > **Note**
   >
   > Los navegadores web Chrome y Firefox admiten compresión Brotli solo cuando la solicitud se envía mediante HTTPS. No admiten Brotli con solicitudes HTTP.

2. En la ubicación de borde, CloudFront verifica la caché en busca de una versión comprimida del objeto solicitado.
3. En función de si el objeto comprimido está en la caché o no, CloudFront realiza una de las siguientes acciones:
   - Si el objeto comprimido ya está en la caché, CloudFront envía el objeto al lector y omite los demás pasos.

- Si el objeto comprimido no se encuentra en la caché, CloudFront reenvía la solicitud al origen.

> **Note**
>
> Si una copia sin comprimir del objeto ya está en la caché, CloudFront podría enviarla al lector sin reenviar la solicitud al origen. Por ejemplo, esto puede ocurrir cuando CloudFront omitió previamente la compresión. Cuando esto sucede, CloudFront almacena en caché el objeto sin comprimir y continúa atendiéndolo hasta que el objeto se vence, desaloja o invalida.

4. Si el origen devuelve un objeto comprimido (como indica la presencia del lector de `Content-Encoding` en la respuesta HTTP), CloudFront envía el objeto comprimido al lector, lo agrega a la caché y omite los demás pasos. CloudFront no comprime de nuevo el objeto.
5. Si el origen devuelve un objeto sin comprimir a CloudFront sin el encabezado `Content-Encoding` en la respuesta HTTP, CloudFront determina si el objeto se puede comprimir. Para obtener más información, consulte Condiciones para la compresión.
6. Si el objeto se puede comprimir, CloudFront lo comprime, lo envía al lector y lo agrega a la caché.
7. Si hay solicitudes de lector posteriores para el mismo objeto, CloudFront devuelve la primera versión almacenada en caché. Por ejemplo, si un lector solicita un objeto en caché específico que utiliza la compresión Gzip y el lector acepta el formato Gzip, las solicitudes posteriores al mismo objeto devolverán siempre la versión Gzip, aunque el lector acepte Brotli y Gzip.

Algunos orígenes personalizados también pueden comprimir objetos. Es posible que el origen pueda comprimir objetos que CloudFront no comprime. Para obtener más información, consulte Tipos de archivos que CloudFront comprime.

Condiciones para la compresión

En la siguiente lista se ofrece más información sobre los casos en los que CloudFront no comprime objetos.

La solicitud utiliza HTTP 1.0

Si una solicitud a CloudFront utiliza HTTP 1.0, CloudFront elimina el encabezado `Accept-Encoding` y no comprime el objeto en la respuesta.

`Accept-Encoding`Encabezado de solicitud

Si el encabezado `Accept-Encoding` no se encuentra en la solicitud de lector o si no contiene `gzip` o `br` como valor, CloudFront no comprime el objeto en la respuesta. Si el encabezado `Accept-Encoding` incluye valores adicionales como `deflate`, CloudFront los elimina antes de reenviar la solicitud al servidor de origen.

Cuando CloudFront se configura para comprimir objetos, incluye el encabezado `Accept-Encoding` en la clave de caché y en las solicitudes de origen de forma automática.

El contenido ya está almacenado en caché al configurar CloudFront para comprimir objetos

CloudFront comprime los objetos cuando los obtiene del origen. Al configurar CloudFront para comprimir objetos, CloudFront no comprime los objetos que ya se han almacenado en caché en ubicaciones de borde. Además, cuando un objeto se vence en una ubicación periférica y CloudFront envía otra solicitud del objeto al origen, CloudFront no comprime el objeto si el origen devuelve un código de estado HTTP 304. Esto significa que la ubicación periférica ya tiene la versión más reciente del objeto. Si desea que CloudFront comprima los objetos que ya se han almacenado en ubicaciones de borde, tiene que invalidar esos objetos. Para obtener más información, consulte Invalidación de archivos para eliminar el contenido.

El origen ya está configurado para comprimir objetos

Si configura CloudFront para comprimir objetos y el origen también comprime objetos, el origen debe incluir un encabezado `Content-Encoding`. Este encabezado indica a CloudFront que el objeto ya está comprimido. CloudFront no comprime un objeto si la respuesta incluye un encabezado `Content-Encoding`, independientemente del valor del encabezado. CloudFront envía la respuesta al lector y almacena en caché el objeto en la ubicación de borde.

Tipos de archivos que CloudFront comprime

Para ver una lista completa, consulte Tipos de archivos que CloudFront comprime.

Tamaño de los objetos que comprime CloudFront

CloudFront comprime objetos con tamaños entre 1000 y 10 000 000 bytes.

`Content-Length`Encabezado

El origen debe incluir un encabezado `Content-Length` en la respuesta para que CloudFront lo use a fin de determinar si el tamaño del objeto se encuentra en el rango que comprime. Si falta el encabezado `Content-Length`, contiene un valor no válido o uno fuera del rango de tamaños que CloudFront comprime, CloudFront no comprime el objeto. Para obtener más información

sobre cómo CloudFront procesa los objetos grandes que pueden superar el rango de tamaño, consulte Cómo CloudFront procesa las solicitudes parciales de un objeto (rango GET).

Código de estado HTTP de la respuesta.

CloudFront comprime los objetos solo cuando el código de estado HTTP de la respuesta es `200`, `403` o `404`.

La respuesta no tiene cuerpo

Cuando la respuesta HTTP del origen no tiene cuerpo, no hay nada para que CloudFront comprima.

`ETag`Encabezado

CloudFront a veces modifica el encabezado `ETag` en la respuesta HTTP cuando comprime objetos. Para obtener más información, consulte the section called "`ETag`Conversión de encabezado".

CloudFront omite la compresión

CloudFront comprime los objetos sobre la base del mejor esfuerzo. En raras ocasiones, CloudFront omite la compresión de un objeto cuando experimenta una gran carga de tráfico. CloudFront toma esta decisión basándose en una serie de factores, como la capacidad del host. Si CloudFront omite la compresión de un objeto, almacena en caché el objeto sin comprimir y continúa atendiéndolo hasta que el objeto se vence, expulsa o invalida.

Tipos de archivos que CloudFront comprime

Si configura CloudFront para comprimir objetos, CloudFront comprime solo los objetos que tienen uno de los siguientes valores en el encabezado de respuesta `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`

`ETag`Conversión de encabezado

Cuando el objeto sin comprimir del origen incluye un encabezado HTTP `ETag` válido y seguro, y CloudFront comprime el objeto, CloudFront también convierte el valor de encabezado `ETag` fuerte en uno `ETag` débil y devuelve el valor `ETag` débil al lector. Los lectores pueden almacenar el valor `ETag` débil y utilizarlo para enviar solicitudes condicionales con el encabezado HTTP `If-None-Match`. Esto permite a los lectores, a CloudFront y al origen tratar las versiones comprimidas y no comprimidas de un objeto como semánticamente equivalentes, lo que reduce la transferencia de datos innecesaria.

Un valor de encabezado `ETag` válido y fuerte comienza y termina con un carácter de comillas dobles (`"`). Para convertir el valor `ETag` fuerte en uno débil, CloudFront agrega los caracteres `W/` al principio del valor `ETag` fuerte.

Cuando el objeto del origen incluye un valor de encabezado `ETag` débil (un valor que comienza con los caracteres `W/`), CloudFront no modifica este valor y lo devuelve al lector tal como se ha recibido del origen.

Cuando el objeto del origen incluye un valor de encabezado `ETag` no válido (el valor no comienza por `"` ni por `W/`), CloudFront elimina el encabezado `ETag` y devuelve el objeto al lector sin el encabezado de respuesta `ETag`.

Para obtener más información, consulte las páginas siguientes en los documentos web de MDN:

- Directivas (encabezado HTTP `ETag`)

- Validación débil (solicitudes condicionales HTTP)
- If-None-Match Encabezado HTTP

Uso de protecciones de AWS WAF

Puede usar AWS WAF para proteger las distribuciones de CloudFront y los servidores de origen. AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API mediante el bloqueo de solicitudes antes de que lleguen a los servidores. Para obtener más información, consulte Aceleración y protección de los sitios web con CloudFront y AWS WAF y Directrices para la implementación de AWS WAF.

Para habilitar las protecciones de AWS WAF, puede hacer lo siguiente:

- Utilice protección con un solo clic en la consola de CloudFront. La protección con un solo clic crea una lista de control de acceso web (ACL web) de AWS WAF, configura reglas para proteger los servidores de las amenazas web comunes y adjunta la ACL web a la distribución de CloudFront por usted. En los temas de esta sección se presupone el uso de protecciones con un solo clic.
- Utilice una ACL (lista de control de acceso) web preconfigurada que cree en la consola de AWS WAF o mediante las API de AWS WAF. Para obtener más información, consulte Listas de control de acceso (ACL) en la Guía para desarrolladores de AWS WAF y AssociateWebACL en la Referencia de la API de AWS WAF

Puede habilitar AWS WAF cuando:

- Creación de una distribución
- Utilice el panel de seguridad para editar la configuración de seguridad de una distribución existente

Cuando utiliza la protección con un solo clic, CloudFront aplica un conjunto de protecciones recomendado por AWS que:

- Bloquear las direcciones IP de posibles amenazas basándose en la inteligencia de amenazas internas de Amazon.
- Proteger contra las vulnerabilidades más comunes que se encuentran en las aplicaciones web, tal y como se describe en el Top 10 de OWASP.
- Defenderse de los actores malintencionados mediante la detección de vulnerabilidades en las aplicaciones.

> **Important**
>
> Debe habilitar AWS WAF si quiere ver las métricas de seguridad en el panel de seguridad de CloudFront. Sin AWS WAF habilitado, solo puede usar el panel de seguridad para habilitar AWS WAF o configurar las restricciones geográficas de CloudFront. Para obtener más información acerca del panel, consulte Administración de las protecciones de seguridad de AWS WAF en el panel de seguridad de CloudFront, más adelante en esta sección.

Temas

- Habilitación de AWS WAF para distribuciones
- Administración de las protecciones de seguridad de AWS WAF en el panel de seguridad de CloudFront
- Configuración del límite de velocidad
- Habilitación de protecciones de seguridad de AWS WAF

Habilitación de AWS WAF para distribuciones

Puede habilitar AWS WAF al crear una distribución, o bien puede habilitar las protecciones de seguridad para una lista de control de acceso (ACL) existente.

Si habilita AWS WAF para la distribución de CloudFront, también puede habilitar el control de bots y configurar la protección de seguridad por categoría de bots.

Temas

- Habilitación de AWS WAF para una nueva distribución
- Utilizar una ACL web existente
- Habilitación del control de bots
- Configuración de la protección por categoría de bots

Habilitación de AWS WAF para una nueva distribución

El siguiente procedimiento muestra cómo habilitar AWS WAF al crear una nueva distribución de CloudFront.

Habilitación de AWS WAF para nuevas distribuciones

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, elija Crear distribución.
3. Según sea necesario, siga los pasos que se indican en Creación de una distribución.
4. En la sección Firewall de aplicaciones web, seleccione Editar y, a continuación, Habilitar protecciones de seguridad.
5. Complete los siguientes campos:
   - Utilizar el modo de supervisión: puede habilitar el modo de supervisión cuando desee recopilar datos para comprobar el funcionamiento de la protección. Cuando habilite el modo de supervisión, las solicitudes no se bloquean si las protecciones estaban activas. En su lugar, el modo de supervisión recopila datos sobre las solicitudes que se bloquearían si las protecciones estuvieran activas. Cuando esté listo para iniciar el bloqueo, puede habilitarlo en la página Seguridad.
   - Protecciones adicionales: elija las opciones que desee activar. Si activa la limitación de velocidad, consulte the section called “Configuración del límite de velocidad” para obtener más información.
   - Estimación de precio: puede abrir la sección para mostrar un campo en el que introducir un número diferente de solicitudes por mes y ver una nueva estimación.
6. Revise el resto de la configuración de distribución y, a continuación, seleccione Crear distribución.

Tras crear una distribución, CloudFront crea un panel de Seguridad. Puede utilizar este panel para habilitar o deshabilitar AWS WAF. Si aún no ha habilitado AWS WAF, los cuadros y gráficos del panel permanecen en blanco.

Utilizar una ACL web existente

Si tiene una ACL web existente, puede utilizarla en lugar de la protección que ofrece AWS WAF.

Para usar una configuración de AWS WAF existente

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Realice una de las siguientes acciones:

   a. Elija Crear distribución y siga los pasos que se indican en Creación de una distribución y, a continuación, vuelva a este tema.
   b. Elija una configuración existente y, a continuación, elija la pestaña Seguridad.
3. En la sección Firewall de aplicaciones web (WAF), seleccione Editar y, a continuación, Habilitar protecciones de seguridad.
4. Elija Usar la configuración de WAF existente. Esta opción solo aparece si tiene configuradas las ACL web.
5. Elija la ACL web existente en la tabla Elegir una ACL web.
6. Revise el resto de la configuración de distribución y, a continuación, seleccione Crear distribución.

Habilitación del control de bots

Si habilita AWS WAF para la distribución de CloudFront, podrá ver las solicitudes de bots durante un intervalo de tiempo determinado en el panel de seguridad de la consola de CloudFront. Puede también habilitar o desactivar el control de bots aquí.

Se generan gastos cuando habilita el control de bots. El panel de seguridad proporciona una estimación de los costos.

Si habilita el control de bots, el panel de seguridad muestra el tráfico de bots por tipo y categoría de bot. Si desactiva el control de bots, el tráfico de bots se muestra en función del muestreo de solicitudes.

Para habilitar el control de bots

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, elija la distribución que desea cambiar.
3. Elija la pestaña Seguridad.
4. Desplácese hacia abajo hasta la sección Solicitudes de bots para un intervalo de tiempo determinado y elija Habilitar el control de bots.
5. En el cuadro de diálogo Control de bots, en Configuración, seleccione la casilla de verificación Habilitar el control de bots para bots comunes.
6. Elija Guardar cambios.

Configuración de la protección por categoría de bots

Al habilitar el control de bots, puede configurar cómo se gestiona cada bot no verificado por categoría de bot. Por ejemplo, puede configurar un bot de biblioteca HTTP en modo de supervisión y asignar un desafío a un verificador de enlaces.

> **Note**
>
> Los bots que se conocen por AWS por ser comunes y verificables, como los rastreadores de motores de búsqueda conocidos, no están sujetos a las acciones que establece aquí. El control de bots confirma que los bots validados provienen del origen que afirman antes de marcarlos como verificados.

Configuración de la protección de una categoría de bot

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, elija la distribución que desea cambiar.
3. Elija la pestaña Seguridad.
4. En el gráfico Solicitudes por categoría de bot, coloque el cursor sobre cualquiera de los elementos de la columna Acción de bot no verificada y elija el icono de lápiz para editarlo.
5. Abra la lista resultante y elija una de las siguientes opciones:
   - Bloque
   - Permitir
   - Modo de supervisión
   - CAPTCHA
   - Desafío
6. Seleccione la marca de verificación situada junto a la lista para guardar el cambio.

Administración de las protecciones de seguridad de AWS WAF en el panel de seguridad de CloudFront

CloudFront crea un panel de seguridad para cada una de las distribuciones. Puede usar los paneles de la consola de CloudFront. Con los paneles, puede usar CloudFront y AWS WAF juntos en una sola ubicación para monitorear y administrar las protecciones de seguridad comunes para las aplicaciones web. Los paneles proporcionan las siguientes tareas y datos:

- Configuración de seguridad: puede habilitar y deshabilitar las protecciones de AWS WAF y ver las protecciones específicas de la aplicación, como las de WordPress.
- Tendencias de seguridad: incluyen las solicitudes permitidas y bloqueadas, las solicitudes de desafío y CAPTCHA y los principales tipos de ataques. Puede ver los índices de tráfico y ver cómo cambian con el tiempo. Por ejemplo, si todas las solicitudes aumentan un 3 %, pero las solicitudes permitidas aumentan un 14 %, significa que ha permitido el paso de una parte mayor del tráfico en el periodo actual.
- Solicitudes de bots: puede ver cuánto tráfico proviene de los bots, qué tipos de bots (verificados o no verificados) y cómo cambian las asignaciones porcentuales de los tipos de bots (verificados o no verificados) a lo largo del tiempo. Para obtener más información sobre la habilitación del control de bots, consulte Habilitación del control de bots.
- Registros de solicitudes: los datos de registro pueden ayudar a responder preguntas sobre las tendencias de seguridad o las solicitudes de bots. Puede buscar en los registros sin necesidad de escribir consultas y ver gráficos agregados para determinar si un conjunto de registros filtrado se basa principalmente en un subconjunto de métodos HTTP, direcciones IP, rutas de URI o países. Puede colocar el cursor sobre los valores de los gráficos y bloquear las direcciones IP y los países. Para obtener más información, consulte Habilitación de registros de AWS WAF.
- Administración de restricciones geográficas: CloudFront y AWS WAF proporciona características de restricción geográfica. CloudFront ofrece restricciones geográficas de forma gratuita, pero las métricas de las restricciones geográficas de CloudFront no se muestran en el panel de seguridad. Para ver las métricas de solicitudes de países bloqueados, debe utilizar las restricciones geográficas de AWS WAF. Para ello, coloque el cursor sobre la barra de un país en el panel de seguridad y bloquee el país. Para obtener más información, consulte Uso de restricciones geográficas de CloudFront.
  - Es posible que la opción Bloquear no esté disponible si anteriormente creó una regla de AWS WAF personalizada fuera de la consola de CloudFront para bloquear países.

Temas

- Requisitos previos
- Habilitación de registros de AWS WAF

Requisitos previos

Debe habilitar AWS WAF si quiere ver las métricas de seguridad en el panel de seguridad de CloudFront. Si no habilita AWS WAF, solo puede usar el panel de seguridad para habilitar AWS WAF o configurar las restricciones geográficas de CloudFront.

Para obtener más información acerca de la habilitación de AWS WAF, consulte Habilitación de AWS WAF para distribuciones.

Habilitación de registros de AWS WAF

Los datos de registro de AWS WAF pueden ayudarle a aislar patrones de tráfico específicos. Por ejemplo, los registros pueden mostrarle de dónde proviene determinado tráfico o qué es lo que hace.

Si habilita el registro de AWS WAF en CloudWatch, el panel de seguridad de CloudFront consulta, agrega y muestra la información de los registros de CloudWatch. No cobramos por usar el panel de seguridad, pero los precios de CloudWatch se aplican a los registros consultados a través del panel. Para obtener más información, consulte Precios de Amazon CloudWatch.

Para habilitar registros

1. Ingrese el volumen de solicitudes esperado en el cuadro Número de solicitudes por mes para estimar los costos de habilitar los registros.
2. Seleccione la casilla de verificación Habilitar registros de AWS WAF.
3. Seleccione Habilitar.

CloudFront crea un grupo de registros de CloudWatch y actualiza la configuración de AWS WAF para empezar a registrarse en CloudWatch. En el primer uso, los datos de registro pueden tardar varios minutos en aparecer. La sección de solicitudes del gráfico muestra cada solicitud. Debajo de las solicitudes individuales, los gráficos de barras agregan datos por método HTTP, rutas de URI principales, direcciones IP principales y países principales. Los gráficos pueden ayudarle a encontrar patrones. Por ejemplo, es posible que vea un volumen desproporcionado de solicitudes procedentes de una sola dirección IP o de datos de un país que no había visto anteriormente en los

registros. Puede filtrar las solicitudes en función del país, el encabezado del host y otros atributos para ayudarle a encontrar tráfico no deseado. Una vez que identifique ese tráfico, coloque el cursor sobre una solicitud individual o un elemento del gráfico y bloquee una dirección IP o un país.

> **Note**
>
> Las métricas mostradas se basan en la ACL web. Por lo tanto, si asocia la misma ACL web a varias distribuciones, verá todas las métricas de dicha ACL, no solo las solicitudes de AWS WAF procesadas para esa distribución.

Configuración del límite de velocidad

El límite de velocidad es una de las recomendaciones que puede recibir al configurar las protecciones de seguridad.

CloudFront siempre activa la limitación de velocidad en el modo de supervisión. Cuando el modo de supervisión está activado, CloudFront captura métricas que indican si se ha superado la velocidad que configuró en el campo Límite de velocidad, con qué frecuencia y en qué medida.

Tras guardar la distribución, CloudFront comienza a recopilar datos en función del número del campo Límite de velocidad.

Puede activar o administrar la configuración de límite de velocidad en la sección Seguridad: Web Application Firewall (WAF) en la pestaña Seguridad de cualquier distribución de CloudFront.

> **Note**
>
> La opción Limitación de la velocidad solo aparece en la consola de CloudFront si especificó un origen personalizado para la distribución que no fuera S3. De lo contrario, solo verá Protecciones principales activadas para la distribución. Para obtener más información acerca de los tipos de origen, consulte Uso de varios orígenes con distribuciones de CloudFront.

Configuración del límite de velocidad

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, elija la distribución que desea cambiar.

3. Elija la pestaña Seguridad.
4. En la sección Seguridad: Web Application Firewall (WAF), seleccione Editar.
5. En Protecciones adicionales, seleccione Limitación de la velocidad. Puede cambiar el límite de velocidad si lo desea. Cuando haya ajustado el límite, seleccione Guardar cambios.
6. En la sección Seguridad: Web Application Firewall (WAF), junto a Limitación de la velocidad, puede elegir Modo de monitoreo y, después, Activar el bloqueo para desactivar el modo de monitoreo. CloudFront empezará a bloquear las solicitudes que superen el límite de velocidad especificado.

Para obtener más información sobre la activación de AWS WAF y la limitación de la velocidad, consulte la entrada del blog Introducing CloudFront Security Dashboard, a Unified CDN and Security Experience.

Habilitación de protecciones de seguridad de AWS WAF

Si la distribución no necesita protecciones de seguridad de AWS WAF, puede deshabilitar esta característica mediante la consola de CloudFront.

Si habilitó previamente la protección de AWS WAF y no eligió una configuración WAF existente (también conocida como protección con un solo clic), CloudFront creó automáticamente una ACL web para usted. En el caso de las ACL web creadas de esta manera, la consola de CloudFront desasociará el recurso y eliminará la ACL web.

Desasociar una ACL web no es lo mismo que eliminarla. Al desasociarla, se elimina la ACL web de la distribución, pero no se elimina de la Cuenta de AWS. Para obtener más información, consulte Associating or disassociating a web ACL with an AWS resource en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

Consulte el siguiente procedimiento para deshabilitar las protecciones de AWS WAF y desasociar la ACL web de la distribución.

Deshabilitación de las protecciones de seguridad de AWS WAF en CloudFront

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones y, a continuación, elija la distribución que desea cambiar.

3. Elija la pestaña Seguridad y, a continuación, elija Editar.
4. En la sección Web Application Firewall (WAF), elija Deshabilitar la protección de AWS WAF.
5. Elija Guardar cambios.

Notas

- Si deshabilitó la protección de seguridad de AWS WAF y aún desea eliminar la ACL web de la Cuenta de AWS, puede eliminarla de forma manual. Siga el procedimiento para eliminar una ACL web. En la consola de AWS WAF y Shield, en la página ACL web, debe elegir la lista Global (CloudFront) para buscar las ACL web.
- Al eliminar una distribución de la consola de CloudFront, CloudFront también intentará eliminar la ACL web si eligió la protección con un solo clic. Es el máximo esfuerzo y no siempre está garantizado. Para obtener más información, consulte Eliminar una distribución.

Configuración de acceso seguro y restricción de acceso a contenido

CloudFront proporciona varias opciones para proteger el contenido que ofrece. A continuación, se muestran algunas formas de utilizar CloudFront para proteger y restringir el acceso al contenido:

- Configure las conexiones HTTPS.
- Impida que los usuarios de ubicaciones geográficas específicas accedan al contenido
- Solicitar a los usuarios que accedan al contenido mediante URL o cookies firmadas de CloudFront
- Configure el cifrado en el nivel de campo para campos de contenido específicos
- Utilizar AWS WAF para controlar el acceso al contenido

También debe implementar una arquitectura resistente a ataques DDoS para la infraestructura y las aplicaciones. Para obtener información, consulte Prácticas recomendadas de AWS para la resiliencia a ataques DDoS.

Para obtener más información, consulte los siguientes temas:

- Securing your content delivery with CloudFront
- SIEM on Amazon OpenSearch Service

Temas

- Uso de HTTPS con CloudFront
- Uso de nombres de dominio alternativos y HTTPS
- Autenticación TLS mutua con CloudFront (mTLS de espectador)
- TLS mutua (origen) con CloudFront
- Distribución de contenido privado con URL firmadas y cookies firmadas
- Restricción del acceso a un origen de AWS
- Restricción del acceso a Application Load Balancer
- Restricción de la distribución geográfica de su contenido
- Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial

Uso de HTTPS con CloudFront

Puede configurar CloudFront para exigir a los lectores que utilicen HTTPS al solicitar sus conexiones, de modo que las conexiones se cifren cuando CloudFront se comunique con los lectores. También puede configurar CloudFront para utilizar HTTPS con su origen, de modo que las conexiones se cifran cuando CloudFront se comunica con el origen.

Si configura CloudFront para exigir HTTPS al comunicarse con lectores y con su origen, esto es lo que ocurre cuando CloudFront recibe una solicitud:

1. Un lector envía una solicitud HTTPS a CloudFront. Hay una negociación SSL/TLS entre el lector y CloudFront. Al final, el espectador envía la solicitud en un formato cifrado.
2. Si la ubicación de borde de CloudFront contiene una respuesta almacenada en la caché, CloudFront cifra la respuesta y la devuelve al lector, quien la descifra.
3. Si la ubicación de borde de CloudFront no contiene una respuesta almacenada en la caché, CloudFront realiza la negociación SSL/TLS con su origen y, cuando se haya completado la negociación, reenvía la solicitud al origen en un formato cifrado.
4. Su origen descifra la solicitud, la procesa (genera una respuesta), cifra la respuesta y la devuelve a CloudFront.
5. CloudFront descifra la respuesta, vuelve a cifrarla y la reenvía al lector. CloudFront también guarda en caché la respuesta en la ubicación de borde para que esté disponible la próxima vez que se solicite.
6. El espectador descifra la respuesta.

El proceso es prácticamente el mismo tanto si el origen es un bucket de Amazon S3, MediaStore o un origen personalizado como si es un servidor HTTP/S:

> **Note**
>
> Para ayudar a frustrar los ataques de tipo SSL renegociación, CloudFront no admite renegociación de lector y las solicitudes de origen.

Como opción alternativa, puede activar la autenticación mutua para la distribución de CloudFront. Para obtener más información, consulte Autenticación TLS mutua con CloudFront (mTLS de espectador).

Para obtener información acerca de cómo solicitar HTTPS entre lectores y CloudFront, y entre CloudFront y su origen, consulte los siguientes temas.

Temas

- Exigencia de HTTPS para la comunicación entre lectores y CloudFront
- Exigencia de HTTPS para la comunicación entre CloudFront y su origen personalizado
- Exigencia de HTTPS para la comunicación entre CloudFront y su origen de Amazon S3
- Protocolos y cifrados admitidos entre lectores y CloudFront
- Protocolos y cifrados admitidos entre CloudFront y el origen

Exigencia de HTTPS para la comunicación entre lectores y CloudFront

Puede configurar uno o varios comportamientos de la caché en la distribución de CloudFront para que requieran HTTPS en la comunicación entre los lectores y CloudFront. También puede configurar uno o varios comportamientos de la caché para permitir HTTP y HTTPS, de forma que CloudFront requiera HTTPS para algunos objetos, pero no para otros. Los pasos de configuración dependerán del nombre de dominio objeto que use en URL de objetos:

- Si utiliza el nombre de dominio que CloudFront ha asignado a su distribución, como, por ejemplo, d111111abcdef8.cloudfront.net, cambie la configuración de Viewer Protocol Policy)Política de protocolo del lector) de uno o varios comportamientos de la caché para que exijan que la comunicación se realice mediante HTTPS. En dicha configuración, CloudFront ofrece el certificado SSL/TLS.

  Para cambiar el valor de Viewer Protocol Policy (Política de protocolo del lector) desde la consola de CloudFront, consulte el procedimiento más adelante en esta sección.

  Para obtener información acerca de cómo utilizar la API de CloudFront para cambiar el valor del elemento `ViewerProtocolPolicy`, consulte UpdateDistribution en la Referencia de la API de Amazon CloudFront.
- Si utiliza su propio nombre de dominio, como example.com, necesita cambiar varias configuraciones de CloudFront. También tiene que utilizar un certificado SSL/TLS proporcionado por AWS Certificate Manager (ACM) o importar a ACM o el almacén de certificados de IAM un certificado de una entidad de certificación externa. Para obtener más información, consulte Uso de nombres de dominio alternativos y HTTPS.

> **Note**
>
> Si desea asegurarse de que los objetos que los lectores obtienen de CloudFront se hayan cifrado cuando CloudFront los obtenga del origen, utilice siempre HTTPS entre CloudFront y el origen. Si ha cambiado recientemente de HTTP a HTTPS entre CloudFront y el origen, le recomendamos que invalide objetos en ubicaciones de borde de CloudFront. CloudFront devolverá un objeto a un lector independientemente de si el protocolo utilizado por dicho lector (HTTP o HTTPS) coincide con el protocolo que CloudFront utilizó para obtener el objeto. Para obtener más información acerca de la eliminación o la sustitución de objetos en una distribución, consulte Agregación, eliminación o sustitución de contenido que distribuye CloudFront.

Exigencia de HTTPS para lectores

Para solicitar HTTPS entre los lectores y CloudFront para uno o varios comportamientos de la caché, siga el siguiente procedimiento.

Para configurar CloudFront para que requiera HTTPS entre lectores y CloudFront

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel superior de la consola de CloudFront, elija el ID de la distribución que desea actualizar.
3. En la pestaña Comportamientos, elija el comportamiento de caché que desee actualizar y, a continuación, elija Editar.
4. Especifique uno de los siguientes valores en Política de protocolo de lector:

   Redireccionamiento de HTTP a HTTPS

   Los espectadores pueden utilizar ambos protocolos. Las solicitudes HTTP `GET` y `HEAD` se redirigen automáticamente a solicitudes HTTPS. CloudFront devuelve el código de estado HTTP 301 (Movido permanentemente) junto con la nueva URL HTTPS. A continuación, el lector vuelve a enviar la solicitud a CloudFront través de la URL HTTPS.

> **Important**
>
> Si envía `POST`, `PUT`, `DELETE`, `OPTIONS` o `PATCH` a través de HTTP a un comportamiento de la caché de HTTP a HTTPS y una versión de protocolo de solicitud HTTP 1.1 o superior, CloudFront redirige la solicitud a una ubicación HTTPS con un código de estado HTTP 307 (Redirección temporal). Esto garantiza que la solicitud se envía de nuevo a la nueva ubicación con el mismo método y carga de cuerpo.
> Si envía solicitudes `POST`, `PUT`, `DELETE`, `OPTIONS` o `PATCH` a través de HTTP a un comportamiento de la caché HTTPS con una protocolo de solicitud de versión inferior a HTTP 1.1, CloudFront devuelve un código de estado HTTP 403 (Prohibido).

Cuando un lector realiza una solicitud HTTP que se redirige a una solicitud HTTPS, se aplican cargos de CloudFront a ambas solicitudes. En el caso de la solicitud HTTP, el cargo es solo para la solicitud y para los encabezados que CloudFront devuelve al lector. En el caso de la solicitud HTTPS, el cargo es por la solicitud y por los encabezados y el objeto que devuelve el origen.

Solo HTTPS

Los espectadores pueden obtener acceso a su contenido solo si utilizan HTTPS. Si un lector envía una solicitud HTTP en lugar de una solicitud HTTPS, CloudFront devuelve código de estado HTTP 403 (Prohibido) y no devuelve el objeto.

5. Seleccione Save changes (Guardar cambios).
6. Repita los pasos 3 a 5 para cada comportamiento de la caché adicional para el que desee solicitar HTTPS entre los lectores y CloudFront.
7. Confirme lo siguiente antes de utilizar la configuración actualizada en un entorno de producción:
   - El patrón de ruta de cada comportamiento de la caché es aplicable únicamente a las solicitudes en las que desea que los espectadores utilicen HTTPS.
   - Los comportamientos de la caché se muestran en el orden en que desee que CloudFront los evalúe. Para obtener más información, consulte Patrón de ruta.
   - Los comportamientos de la caché son solicitudes de redirección hacia los orígenes correctos.

Exigencia de HTTPS para la comunicación entre CloudFront y su origen personalizado

Puede exigir HTTPS para la comunicación entre CloudFront y su origen.

> **Note**
>
> Si su origen es un bucket de Amazon S3 configurado como punto de enlace del sitio web, no puede configurar CloudFront para usar HTTPS con su origen porque Amazon S3 no admite HTTPS para los puntos de enlace del sitio web.

Para requerir HTTPS entre CloudFront y su origen, siga los procedimientos de este tema para completar lo siguiente:

1. En su distribución, cambiar la configuración de Origin Protocol Policy (Política de protocolo de origen) para el origen.
2. Instalar un certificado SSL/TLS en su servidor de origen (no es necesario cuando se utiliza un origen de Amazon S3 o u otros orígenes de AWS determinados).

Temas

- Exigencia de HTTPS para orígenes personalizados
- Instalación de un certificado SSL/TLS en su origen personalizado

Exigencia de HTTPS para orígenes personalizados

En el siguiente procedimiento se explica cómo configurar CloudFront para que utilice HTTPS para comunicarse con un balanceador de carga de Elastic Load Balancing, una instancia de Amazon EC2 u otro origen personalizado. Para obtener información sobre el uso de la API de CloudFront para actualizar una distribución, consulte UpdateDistribution en la Referencia de la API de Amazon CloudFront.

Para configurar CloudFront para que requiera HTTPS entre CloudFront y su origen personalizado

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.

2. En el panel superior de la consola de CloudFront, elija el ID de la distribución que desea actualizar.
3. En la pestaña Orígenes, elija el origen que desee actualizar y, a continuación, elija Editar.
4. Actualice los siguientes valores de configuración:

   Origin Protocol Policy

   Cambie Origin Protocol Policy (Política de protocolo de origen) para los orígenes aplicables en su distribución:

   - HTTPS Only (Solo HTTPS): CloudFront solo utiliza HTTPS para comunicarse con su origen personalizado.
   - Match Viewer (Coincidir con lector): CloudFront se comunica con su origen personalizado mediante HTTP o HTTPS, en función del protocolo de la solicitud del lector. Por ejemplo, si elige Match Viewer (Coincidir con lector) en Origin Protocol Policy (Política de protocolo de origen) y el lector usa HTTPS para solicitar un objeto de CloudFront, CloudFront también usa HTTPS para reenviar la solicitud al origen.

     Elija Match Viewer (Coincidir con espectador) solo si especifica Redirect HTTP to HTTPS (Redireccionamiento de HTTP a HTTPS) o HTTPS Only (Solo HTTPS) en Viewer Protocol Policy (Política de protocolo del espectador).

     Tenga en cuenta que CloudFront almacena en caché el objeto solo una vez, incluso si los lectores realizan solicitudes a través de los protocolos HTTP y HTTPS.

   Origin SSL Protocols

   Elija Origin SSL Protocols (Protocolos SSL de orige) para los orígenes aplicables a su distribución. El protocolo SSLv3 es menos seguro, así que le recomendamos que lo seleccione únicamente si su origen no admite TLSv1 o una versión posterior. El protocolo de enlace TLSv1 es bidireccionalmente compatible con SSLv3, pero no con TLSv1.1 y posteriores. Cuando selecciona SSLv3, CloudFront solo envía solicitudes de protocolo de enlace SSLv3.
5. Seleccione Save changes (Guardar cambios).
6. Repita los pasos 3 a 5 para cada origen adicional para el que desee solicitar HTTPS entre CloudFront y su origen personalizado.
7. Confirme lo siguiente antes de utilizar la configuración actualizada en un entorno de producción:

- El patrón de ruta de cada comportamiento de la caché es aplicable únicamente a las solicitudes en las que desea que los espectadores utilicen HTTPS.
- Los comportamientos de la caché se muestran en el orden en que desee que CloudFront los evalúe. Para obtener más información, consulte Patrón de ruta.
- Los comportamientos de la caché son solicitudes de redirección a los orígenes cuyo valor de Origin Protocol Policy (Política de protocolos de origen) ha cambiado.

Instalación de un certificado SSL/TLS en su origen personalizado

Puede utilizar un certificado SSL/TLS de las siguientes fuentes en su origen personalizado:

- Si su origen es un equilibrador de carga de Elastic Load Balancing, puede utilizar un certificado proporcionado por AWS Certificate Manager (ACM). También puede utilizar un certificado firmado por una entidad de certificación de terceros de confianza e importado a ACM.
- En el caso de orígenes diferentes a balanceadores de carga de Elastic Load Balancing, debe utilizar un certificado firmado por una entidad de certificación (CA) de terceros de confianza, como Comodo, DigiCert o Symantec.

El certificado devuelto del origen debe incluir uno de los siguientes nombres de dominio:

- El nombre de dominio en el campo del origen Origin domain (Dominio de origen) (el campo `DomainName` en la API de CloudFront).
- El nombre de dominio en el encabezado `Host`, si el comportamiento de la caché está configurado para reenviar el encabezado `Host` al origen.

Cuando CloudFront utiliza HTTPS para comunicarse con su origen, CloudFront verifica que el certificado haya sido emitido por una autoridad de certificados de confianza. CloudFront admite las mismas autoridades de certificados que Mozilla. Para consultar la lista actualizada, consulte Mozilla Included CA Certificate List. No se puede utilizar un certificado autofirmado para comunicación HTTPS entre CloudFront y su origen.

> **Important**
>
> En caso de que el servidor de origen devuelva un certificado expirado, no válido o autofirmado, o si el servidor de origen devuelve la cadena de certificados en el orden

incorrecto, CloudFront interrumpe la conexión TCP, devuelve código de estado HTTP 502 (Puerta de enlace incorrecta) y establece el encabezado `X-Cache` como `Error from cloudfront`. Igualmente, si toda la cadena de certificados, incluidos los certificados intermedios, no está presente, CloudFront interrumpe la conexión TCP.

Exigencia de HTTPS para la comunicación entre CloudFront y su origen de Amazon S3

Cuando el origen es un bucket de Amazon S3, las opciones para utilizar HTTPS en las comunicaciones con CloudFront dependerán de cómo se esté utilizando el bucket. Si su bucket de Amazon S3 se configura como un punto de enlace de sitio web, no puede configurar CloudFront para usar HTTPS para comunicarse con su origen porque Amazon S3 no admite conexiones HTTPS en dicha configuración.

Cuando el origen es un bucket de Amazon S3 que permite la comunicación HTTPS, CloudFront reenvía las solicitudes a S3 con el protocolo que los lectores utilizaron para enviar las solicitudes. El valor predeterminado para la configuración Protocolo (solo orígenes personalizados) es Match Viewer (Coincidir con lector) y no puede modificarse. Sin embargo, si habilita el control de acceso de origen (OAC) para el origen de Amazon S3, la comunicación utilizada entre CloudFront y Amazon S3 depende de la configuración. Para obtener más información, consulte Creación de un nuevo control de acceso de origen.

Si desea solicitar HTTPS para la comunicación entre CloudFront y Amazon S3, deberá cambiar el valor de protocolo de Viewer Protocol Policy (Política de protocolo del lector) a Redirect HTTP to HTTPS (Redirigir HTTP a HTTPS) o HTTPS Only (Solo HTTPS). En el procedimiento que se indica más adelante en esta sección se explica cómo usar la consola de CloudFront para cambiar Viewer Protocol Policy (Política de protocolo del lector). Para obtener información sobre el uso de la API de CloudFront para actualizar el elemento `ViewerProtocolPolicy` de una distribución, consulte UpdateDistribution en la Referencia de la API de Amazon CloudFront.

Si utiliza HTTPS con un bucket de Amazon S3 que admite comunicaciones HTTPS, Amazon S3 proporciona el certificado SSL/TLS para que no tenga hacerlo usted.

Exigencia de HTTPS para un origen de Amazon S3

El siguiente procedimiento muestra cómo configurar CloudFront para que se exija HTTPS a su origen de Amazon S3.

Para configurar CloudFront para que requiera HTTPS a su origen de Amazon S3

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel superior de la consola de CloudFront, elija el ID de la distribución que desea actualizar.
3. En la pestaña Behaviors (Comportamientos), elija el comportamiento de la caché que desee actualizar y, a continuación, elija Edit (Editar).
4. Especifique uno de los siguientes valores en Viewer Protocol Policy (Política de protocolo del espectador):

   Redireccionamiento de HTTP a HTTPS

   Los espectadores pueden usar tanto el protocolo HTTP como el HTTPS, pero las solicitudes HTTP se redirigirán automáticamente a solicitudes HTTPS. CloudFront devuelve el código de estado HTTP 301 (Movido permanentemente) junto con la nueva URL HTTPS. A continuación, el lector vuelve a enviar la solicitud a CloudFront través de la URL HTTPS.

   > **Important**
   >
   > CloudFront no redirige las solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` ni `PUT` de HTTP a HTTPS. Si configura un comportamiento de la caché para que redirija a HTTPS, CloudFront responde a solicitudes HTTP `DELETE`, `OPTIONS`, `PATCH`, `POST` o `PUT` de ese comportamiento de la caché con el código de estado HTTP 403 (Prohibido).

   Cuando un lector realiza una solicitud HTTP que se redirige a una solicitud HTTPS, se aplican cargos de CloudFront a ambas solicitudes. En el caso de la solicitud HTTP, el cargo es solo para la solicitud y para los encabezados que CloudFront devuelve al lector. En el caso de la solicitud HTTPS, el cargo es por la solicitud y por los encabezados y el objeto devueltos por el origen.

   Solo HTTPS

   Los espectadores pueden obtener acceso a su contenido solo si utilizan HTTPS. Si un lector envía una solicitud HTTP en lugar de una solicitud HTTPS, CloudFront devuelve código de estado HTTP 403 (Prohibido) y no devuelve el objeto.

5. Elija Yes, Edit (Sí, editar).
6. Repita los pasos 3 a 5 para cada comportamiento de la caché adicional para el que desee solicitar HTTPS entre los lectores y CloudFront, y entre CloudFront y S3.
7. Confirme lo siguiente antes de utilizar la configuración actualizada en un entorno de producción:
   - El patrón de ruta de cada comportamiento de la caché es aplicable únicamente a las solicitudes en las que desea que los espectadores utilicen HTTPS.
   - Los comportamientos de la caché se muestran en el orden en que desee que CloudFront los evalúe. Para obtener más información, consulte Patrón de ruta.
   - Los comportamientos de la caché son solicitudes de redirección hacia los orígenes correctos.

Protocolos y cifrados admitidos entre lectores y CloudFront

Cuando necesite HTTPS entre los lectores y la distribución de CloudFront, debe elegir una política de seguridad, que determina la siguiente configuración.

- El protocolo SSL/TLS mínimo que utiliza CloudFront para comunicarse con los lectores.
- Los cifrados que CloudFront puede utilizar para cifrar la comunicación con los lectores.

Para elegir una política de seguridad, especifique el valor aplicable para Política de seguridad (versión mínima de SSL/TLS). En la siguiente tabla se muestran los protocolos y los cifrados que CloudFront puede utilizar para cada política de seguridad.

Un lector debe admitir al menos uno de los cifrados compatibles para establecer una conexión HTTPS con CloudFront. CloudFront elige un cifrado en el orden mostrado de entre los cifrados que admite el lector. Véase también Nombres de cifrado OpenSSL, s2n y RFC.

	Política de seguridad								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
Protocolos SSL/TLS compatibles									
TLSv1.3	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLSv1.2	♦	♦	♦	♦	♦	♦	♦	♦	

	Política de seguridad								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLSv1.1	♦	♦	♦	♦					
TLSv1	♦	♦	♦						
SSLv3	♦								
Cifrados TLSv1.3 compatibles									
TLS_AES_128_GCM_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_AES_256_GCM_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_CHACHA20_POLY1305_SHA256	♦	♦	♦	♦	♦	♦	♦		♦
Cifrados de ECDSA admitidos									
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA-AES128-SHA256	♦	♦	♦	♦	♦	♦			
ECDHE-ECDSA-AES128-SHA	♦	♦	♦	♦					
ECDHE-ECDSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦	♦	♦	

	Política de seguridad								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
ECDHE-ECDSA-CHACHA20-POLY1305	♦	♦	♦	♦	♦	♦	♦		
ECDHE-ECDSA-AES256-SHA384	♦	♦	♦	♦	♦	♦			
ECDHE-ECDSA-AES256-SHA	♦	♦	♦	♦					
Cifrados de RSA compatibles									
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	♦	♦	♦	♦	♦	♦			

	Política de seguridad								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
ECDHE-RSA-AES256-SHA	♦	♦	♦	♦					
AES128-GCM-SHA256	♦	♦	♦	♦	♦				
AES256-GCM-SHA384	♦	♦	♦	♦	♦				
AES128-SHA256	♦	♦	♦	♦	♦				
AES256-SHA	♦	♦	♦	♦					
AES128-SHA	♦	♦	♦	♦					
DES-CBC3-SHA	♦	♦							
RC4-MD5	♦								

Nombres de cifrado OpenSSL, s2n y RFC

OpenSSL y s2n usan nombres diferentes para cifrar que los estándares de TLS (RFC 2246, RFC 4346, RFC 5246, y RFC 8446). En la siguiente tabla se mapean los nombres de OpenSSL y s2n al nombre de RFC para cada uno de los cifrados.

CloudFront admite los intercambios de claves clásicos y con seguridad cuántica. Para los intercambios de claves clásicos mediante curvas elípticas, CloudFront admite lo siguiente:

- `prime256v1`
- `X25519`
- `secp384r1`

Para los intercambios de claves con seguridad cuántica, CloudFront admite lo siguiente:

- `X25519MLKEM768`
- `SecP256r1MLKEM768`

> **Note**
>
> Los intercambios de claves con seguridad cuántica solo se admiten con TLS 1.3. TLS 1.2 y las versiones anteriores no admiten el intercambio de claves con seguridad cuántica.

Para obtener más información, consulte los temas siguientes:

- Criptografía poscuántica
- Algoritmos de criptografía y Servicios de AWS
- Intercambio de claves híbridas en TLS 1.3

Para obtener más información acerca de los requisitos del certificado de CloudFront, consulte Requisitos para la utilización de certificados SSL/TLS con CloudFront.

Nombre del cifrado OpenSSL y s2n	Nombre del cifrado RFC
Cifrados TLSv1.3 compatibles	
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256
Cifrados de ECDSA admitidos	
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

Nombre del cifrado OpenSSL y s2n	Nombre del cifrado RFC
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
Cifrados de RSA compatibles	
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-CHACHA20-POLY1305	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384

Nombre del cifrado OpenSSL y s2n	Nombre del cifrado RFC
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

Esquemas de firma admitidos entre los lectores y CloudFront

CloudFront admite los siguientes esquemas de firma para conexiones entre lectores y CloudFront.

	Política de seguridad								
Esquemas de firma	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA512	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHE	♦	♦	♦	♦	♦	♦	♦	♦	♦

	Política de seguridad								
Esquemas de firma	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
ME_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	♦	♦	♦	♦	♦	♦	♦		

	Política de seguridad								
Esquemas de firma	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
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	♦	♦	♦	♦					

Protocolos y cifrados admitidos entre CloudFront y el origen

Si elige exigir HTTPS entre CloudFront y su origen, puede decidir el protocolo SSL/TLS que desea permitir para la conexión segura y CloudFront puede conectarse al origen utilizando cualquiera de los cifrados ECDSA o RSA listados en la siguiente tabla. El origen debe admitir al menos uno de estos códigos cifrados de CloudFront para establecer una conexión HTTPS a su origen.

OpenSSL y s2n usan nombres diferentes para cifrar que los estándares de TLS (RFC 2246, RFC 4346, RFC 5246, y RFC 8446). En la siguiente tabla se incluyen los nombres de OpenSSL y s2n y el nombre de RFC para cada uno de los cifrados.

Para los cifrados con algoritmos de intercambio de claves con curvas elípticas, CloudFront admite las siguientes curvas elípticas:

- prime256v1
- secp384r1
- X25519

Nombre del cifrado OpenSSL y s2n	Nombre del cifrado RFC
Cifrados de ECDSA admitidos	
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

Nombre del cifrado OpenSSL y s2n	Nombre del cifrado RFC
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
Cifrados de RSA compatibles	
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_WITH_RC4_128_MD5

Esquemas de firma admitidos entre CloudFront y el origen

CloudFront admite los siguientes esquemas de firma para las conexiones entre CloudFront y el origen.

- 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

Uso de nombres de dominio alternativos y HTTPS

Si desea utilizar su propio nombre de dominio en las URL de los archivos (por ejemplo, `https://www.example.com/image.jpg`) y desea que los lectores utilicen HTTPS, debe completar los pasos descritos en los siguientes temas. (Si utiliza el nombre de dominio de distribución de CloudFront predeterminado en las URL, por ejemplo, `https://d111111abcdef8.cloudfront.net/image.jpg`, siga las instrucciones del siguiente tema: Exigencia de HTTPS para la comunicación entre lectores y CloudFront).

> **Important**
>
> Cuando se agrega un certificado a la distribución, CloudFront propaga inmediatamente el certificado a todas las ubicaciones de borde. A medida que haya nuevas ubicaciones de borde disponibles, CloudFront también propaga el certificado a dichas ubicaciones. No puede restringir las ubicaciones de borde a las que CloudFront propaga los certificados.

Temas

- Elección de la forma en que CloudFront atiende las solicitudes HTTPS
- Requisitos para la utilización de certificados SSL/TLS con CloudFront
- Cuotas al usar certificados SSL/TLS con CloudFront (solo HTTPS entre lectores y CloudFront)
- Configuración de nombres de dominio alternativos y HTTPS
- Determinación del tamaño de la clave pública en un certificado SSL/TLS RSA
- Aumento de las cuotas de certificados SSL/TLS

- Rotación de certificados SSL/TLS
- Reversión de un certificado SSL/TLS personalizado al certificado de CloudFront predeterminado
- Cambio de un certificado SSL/TLS personalizado con direcciones IP dedicadas a SNI

Elección de la forma en que CloudFront atiende las solicitudes HTTPS

Si desea que los lectores usen HTTPS y nombres de dominio alternativos para los archivos, elija una de las opciones siguientes de cómo CloudFront atiende las solicitudes HTTPS:

- Use Server Name Indication (SNI) (Indicación de nombre de servidor [SNI]): recomendado
- Utilizar una dirección IP dedicada en cada ubicación de borde

En esta sección se explica cómo funciona cada opción.

Uso de SNI para atender solicitudes HTTPS (funciona en la mayoría de los clientes)

Server Name Indication (SNI) (Indicación de nombre de servidor [SNI]) es una extensión del protocolo TLS que admiten los navegadores y clientes disponibles desde 2010. Si configura CloudFront para atender solicitudes HTTPS mediante SNI, CloudFront asocia el nombre de dominio alternativo a una dirección IP para cada ubicación de borde. Cuando un espectador envía una solicitud HTTPS de contenido, el servicio DNS dirige la solicitud a la dirección IP de la ubicación de borde correcta. La dirección IP de su nombre de dominio se determina durante la negociación del protocolo SSL/TLS; la dirección IP no es exclusiva de su distribución.

La negociación SSL/TLS se produce muy pronto en el proceso de establecimiento de una conexión HTTPS. Si CloudFront no puede determinar inmediatamente para qué dominio es la solicitud, interrumpe la conexión. Cuando un espectador que admite SNI envía una solicitud HTTPS de contenido, esto es lo que ocurre:

1. El espectador obtiene automáticamente el nombre de dominio de la URL de la solicitud y lo agrega a la extensión SNI del mensaje de saludo del cliente de TLS.
2. Cuando CloudFront recibe el saludo del cliente de TLS, utiliza el nombre de dominio de la extensión SNI para buscar la distribución de CloudFront coincidente y devuelve el certificado de TLS asociado.
3. El lector y CloudFront llevan a cabo la negociación SSL/TLS.
4. CloudFront devuelve el contenido solicitado al lector.

Para obtener una lista actualizada de los navegadores que admiten SNI, consulte la entrada de Wikipedia de Server Name Indication.

Si desea utilizar SNI pero algunos de los navegadores de los usuarios no lo admiten, dispone de varias opciones:

- Configure CloudFront para atender solicitudes HTTPS a través de direcciones IP dedicadas en lugar de SNI. Para obtener más información, consulte Uso de direcciones IP dedicadas para atender solicitudes HTTPS (funciona en todos los clientes).
- Utilice el certificado SSL/TLS de CloudFront en lugar de un certificado personalizado. Esto requiere que utilice el nombre de dominio de CloudFront para la distribución en las URL de los archivos; por ejemplo, `https://d111111abcdef8.cloudfront.net/logo.png`.

  Si utiliza el certificado de CloudFront predeterminado, los lectores deben admitir el protocolo SSL TLSv1 o versiones posteriores. CloudFront no admite SSLv3 con el certificado de CloudFront predeterminado.

  También debe cambiar el certificado SSL/TLS que CloudFront utiliza, de un certificado personalizado al certificado de CloudFront predeterminado:

  - Si no ha usado su distribución para distribuir su contenido, puede simplemente cambiar la configuración. Para obtener más información, consulte Actualizar una distribución.
  - Si ha usado su distribución para distribuir el contenido, debe crear una nueva distribución de CloudFront y cambiar las URL de los archivos para reducir o eliminar la cantidad de tiempo que el contenido no va a estar disponible. Para obtener más información, consulte Reversión de un certificado SSL/TLS personalizado al certificado de CloudFront predeterminado.
- Si puede controlar qué navegador utilizarán los usuarios, haga que lo actualicen a uno que admita SNI.
- Utilice HTTP en lugar de HTTPS.

Uso de direcciones IP dedicadas para atender solicitudes HTTPS (funciona en todos los clientes)

La indicación de nombre de servidor (SNI) es una manera de asociar una solicitud a un dominio. Otra forma es utilizar una dirección IP dedicada. Si tiene usuarios que no pueden actualizar a un navegador o cliente que se haya lanzado después de 2010, puede utilizar una dirección IP dedicada para atender solicitudes HTTPS. Para obtener una lista actualizada de los navegadores que admiten SNI, consulte la entrada de Wikipedia de Server Name Indication.

> **Important**
>
> Si configura CloudFront para atender solicitudes HTTPS mediante direcciones IP dedicadas, se le aplicará una cuota mensual adicional. El cargo comienza cuando asocia el certificado SSL/TLS a una distribución y la habilita. Para obtener más información acerca de los precios de CloudFront, consulte Precios de Amazon CloudFront. Además, consulte Using the Same Certificate for Multiple CloudFront Distributions.

Si configura CloudFront para atender solicitudes HTTPS mediante direcciones IP dedicadas, CloudFront asocia el certificado a una dirección IP dedicada en cada ubicación periférica de CloudFront. Cuando un espectador envía una solicitud HTTPS de contenido, esto es lo que ocurre:

1. El DNS dirige la solicitud hacia la dirección IP de su distribución en la ubicación de borde aplicable.
2. Si una solicitud de cliente proporciona la extensión SNI en el mensaje `ClientHello`, CloudFront busca una distribución que esté asociada a ese SNI.
   - Si hay una coincidencia, CloudFront responde a la solicitud con el certificado SSL/TLS.
   - Si no hay una coincidencia, CloudFront utiliza la dirección IP para identificar la distribución y determinar qué certificado SSL/TLS devolver al lector.
3. El lector y CloudFront llevan a cabo una negociación SSL/TLS con el certificado SSL/TLS.
4. CloudFront devuelve el contenido solicitado al lector.

Este método funciona con cualquier solicitud HTTPS, independientemente del navegador o espectador que esté utilizando el usuario.

> **Note**
>
> Las IP dedicadas no son direcciones IP estáticas y pueden cambiar con el tiempo. La dirección IP que se devuelve para la ubicación periférica se asigna de forma dinámica a partir de los rangos de direcciones IP de la lista de servidores periféricos de CloudFront.
> Los rangos de direcciones IP de los servidores periféricos de CloudFront están sujetos a cambios. Para recibir notificaciones de cambios de dirección IP, Subscribe to AWS Public IP Address Changes via Amazon SNS.

Solicitud de permiso para utilizar tres o más certificados SSL/TLS de direcciones IP dedicadas

Si necesita permiso para asociar de forma permanente tres o más certificados de IP dedicada SSL/TLS con CloudFront, realice el siguiente procedimiento. Para obtener detalles acerca de solicitudes HTTPS, consulte Elección de la forma en que CloudFront atiende las solicitudes HTTPS.

> **Note**
>
> Este es el procedimiento que se debe seguir para utilizar tres o más certificados de direcciones IP dedicadas en las distribuciones de CloudFront. El valor predeterminado es 2. Tenga en cuenta que no puede vincular más de un certificado SSL a una distribución. Solo puede asociar un único certificado SSL/TLS a una distribución de CloudFront cada vez. Este es el total de certificados SSL de IP dedicadas que puede utilizar en todas las distribuciones de CloudFront.

Para solicitar permiso para utilizar tres o más certificados con una distribución de CloudFront

1. Vaya al Centro de soporte y cree un caso.
2. Indique la cantidad de certificados a utilizar para la que necesita permiso y describa las circunstancias en su solicitud. Actualizaremos su cuenta tan pronto como sea posible.
3. Continúe con el siguiente procedimiento.

Requisitos para la utilización de certificados SSL/TLS con CloudFront

En este tema se describen los requisitos de los certificados SSL/TLS. Se aplicarán a estos dos tipos de certificados, salvo que se indique lo contrario:

- Certificados para utilizar HTTPS entre los lectores y CloudFront
- Certificados para utilizar HTTPS entre CloudFront y el origen

Temas

- Emisor de certificados
- Región de AWS para AWS Certificate Manager
- Formato del certificado

- Certificados intermedios
- Tipo de clave
- Clave privada
- Permisos
- Tamaño de la clave de certificado
- Tipos de certificados admitidos
- Fecha de vencimiento y renovación de certificados
- Nombres de dominio en la distribución de CloudFront y en el certificado
- Versión mínima de protocolo SSL/TLS
- Versiones de HTTP compatibles

Emisor de certificados

Le recomendamos que utilice un certificado público emitido por AWS Certificate Manager(ACM). Para obtener información sobre obtener un certificado de parte de ACM, consulte la Guía del usuario de AWS Certificate Manager. Para utilizar un certificado de ACM con una distribución de CloudFront, asegúrese de solicitar (o importar) el certificado en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`).

CloudFront admite las mismas entidades de certificación (CA, por sus siglas en inglés) que Mozilla, por lo que si no utiliza ACM, utilice un certificado emitido por una entidad de certificados de la Lista de certificados de CA incluida en Mozilla.

Los certificados TLS utilizados por el origen que especificó para su distribución de CloudFront también se deben emitir desde la entidad de certificación que figura en la lista de certificados CA incluidos de Mozilla.

Para obtener más información sobre cómo obtener e instalar un certificado SSL/TLS, consulte la documentación de su software del servidor HTTP y la de la entidad de certificados.

Región de AWS para AWS Certificate Manager

Para utilizar un certificado en AWS Certificate Manager (ACM) para solicitar HTTPS entre el lector y CloudFront, asegúrese de solicitar (o importar) el certificado en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`).

Si desea solicitar HTTPS entre CloudFront y su origen y utiliza un equilibrador de carga Elastic Load Balancing como origen, puede solicitar o importar un certificado en cualquier Región de AWS.

Formato del certificado

El certificado debe tener el formato X.509 PEM. Este es el formato predeterminado si utiliza AWS Certificate Manager.

Certificados intermedios

Si utiliza una entidad de certificación (CA) de terceros, incluya una lista de todos los certificados intermedios de la cadena de certificados en el archivo `.pem`, comenzando por uno para la entidad de certificación que firmó el certificado para su dominio. Normalmente, en el sitio web de la CA encontrará un archivo que enumera los certificados intermedios y raíz encadenados de la manera correcta.

> **Important**
>
> No incluya lo siguiente: el certificado raíz y los certificados intermedios que no estén en la ruta de confianza, ni el certificado de clave pública de la CA.

A continuación se muestra un ejemplo:

```
-----BEGIN CERTIFICATE-----
Intermediate certificate 2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate certificate 1
-----END CERTIFICATE-----
```

Tipo de clave

CloudFront admite pares de claves públicas/privadas de RSA y ECDSA.

CloudFront admite conexiones HTTPS tanto a los lectores como a los orígenes mediante certificados RSA y ECDSA. Con AWS Certificate Manager(ACM), puede solicitar e importar certificados RSA o ECDSA y, a continuación, asociarlos a la distribución de CloudFront.

Para las listas de cifrados RSA y ECDSA admitidos por CloudFront que puede negociar en conexiones HTTPS, consulte the section called “Protocolos y cifrados admitidos entre lectores y CloudFront” y the section called “Protocolos y cifrados admitidos entre CloudFront y el origen”.

Clave privada

Si utiliza un certificado de una entidad de certificación (CA) de terceros, tenga en cuenta lo siguiente:

- La clave privada debe coincidir con la clave pública que se encuentra en el certificado.
- La clave privada debe estar en formato PEM.
- La clave privada no puede cifrarse con una contraseña.

Si AWS Certificate Manager (ACM) ha proporcionado el certificado, ACM no divulga la clave privada. La clave privada se almacena en ACM para que la usen los servicios de AWS integrados con ACM.

Permisos

Debe tener permiso para usar e importar el certificado SSL/TLS. Si utiliza AWS Certificate Manager (ACM), le recomendamos que utilice los permisos de AWS Identity and Access Management necesarios para restringir el acceso a los certificados. Para obtener más información, consulte Identity and Access Management en la Guía del usuario de AWS Certificate Manager.

Tamaño de la clave de certificado

El tamaño de clave de certificado que admite CloudFront depende del tipo de clave y el tipo de certificado.

Para certificados RSA:

CloudFront admite claves RSA de 1024, 2048, 3072 y 4096 bits. La longitud máxima de un certificado RSA que se utiliza con CloudFront es de 4096 bits.

Tenga en cuenta que ACM emite certificados RSA con claves de hasta 2048 bits. Para utilizar un certificado RSA de 3072 o 4096 bits, debe obtener el certificado externamente e importarlo a ACM, tras lo cual estará disponible para que lo utilice con CloudFront.

Para obtener más información acerca de cómo determinar el tamaño de la clave RSA, consulte Determinación del tamaño de la clave pública en un certificado SSL/TLS RSA.

Para certificados ECDSA:

CloudFront admite claves de 256 bits. Si desea utilizar un certificado ECDSA en ACM para solicitar HTTPS entre lectores y CloudFront, utilice la curva elíptica prime256v1.

Tipos de certificados admitidos

CloudFront admite todos los tipos de certificados emitidos por una entidad de certificación de confianza.

Fecha de vencimiento y renovación de certificados

Si utiliza certificados obtenidos de una entidad de certificación (CA) de terceros, debe monitorear las fechas de vencimiento y renovar los certificados SSL/TLS que importe en AWS Certificate Manager (ACM) o cargue en el almacén de certificados de AWS Identity and Access Management antes de su vencimiento.

> **Important**
>
> Para evitar problemas de vencimiento de los certificados, renueve o vuelva a importar su certificado al menos 24 horas antes del valor `NotAfter` del certificado actual. Si su certificado vence en 24 horas, solicite un nuevo certificado a ACM o importe uno nuevo a ACM. A continuación, asocie el nuevo certificado a la distribución de CloudFront.
> Es posible que CloudFront siga utilizando el certificado anterior mientras se esté renovando o reimportando el certificado. Este es un proceso asíncrono que puede tardar hasta 24 horas en mostrar los cambios en CloudFront.

Si utiliza certificados proporcionados por ACM, ACM administra las renovaciones de esos certificados por usted. Para obtener más información, consulte la Renovación administrada en la guía del usuario de AWS Certificate Manager.

Nombres de dominio en la distribución de CloudFront y en el certificado

Cuando se utiliza un origen personalizado, el certificado SSL/TLS del origen incluye un nombre de dominio en el campo Common Name (Nombre común) y, posiblemente, varios más en el campo Subject Alternative Names (Nombres alternativos de sujetos). (CloudFront admite caracteres comodín en nombres de dominio de certificados).

Uno de los nombres de dominio del certificado debe coincidir con el nombre de dominio que especifique en Origin Domain Name. Si no coincide ningún nombre de dominio, CloudFront devuelve al lector el código de estado HTTP `502 (Bad Gateway)`.

> **Important**
>
> Cuando se agrega un nombre de dominio alternativo a una distribución, CloudFront comprueba que el nombre de dominio alternativo esté cubierto por el certificado que se ha asociado. El certificado debe cubrir el nombre de dominio alternativo en el campo de nombre alternativo del sujeto (SAN) del certificado. Esto significa que el campo SAN debe contener una concordancia exacta para el nombre de dominio alternativo o un comodín en el mismo nivel del nombre de dominio alternativo que se está agregando.
> Para obtener más información, consulte Requisitos para el uso de nombres de dominio alternativos.

Versión mínima de protocolo SSL/TLS

Si utiliza direcciones IP dedicadas, establezca la versión mínima de protocolo SSL/TLS para la conexión entre lectores y CloudFront eligiendo una política de seguridad.

Para obtener más información, consulte Política de seguridad (versión mínima de SSL/TLS) en el tema Referencia de toda la configuración de distribución.

Versiones de HTTP compatibles

Si asocia un certificado con más de una distribución de CloudFront, todas las distribuciones asociadas con el certificado deben utilizar la misma opción para Versiones de HTTP compatibles. Esta opción se especifica al crear o actualizar una distribución de CloudFront.

Cuotas al usar certificados SSL/TLS con CloudFront (solo HTTPS entre lectores y CloudFront)

Tenga en cuenta las siguientes cuotas en cuanto al uso de certificados SSL/TLS con CloudFront. Estas cuotas se aplican únicamente a los certificados SSL/TLS que aprovisione mediante AWS Certificate Manager (ACM), que importe a ACM o que cargue en el almacén de certificados de IAM para la comunicación con HTTPS entre los lectores y CloudFront.

Para obtener más información, consulte Aumento de las cuotas de certificados SSL/TLS.

Cantidad máxima de certificados por distribución de CloudFront

Puede asociar un máximo de un certificado SSL/TLS con cada distribución de CloudFront.

Cantidad máxima de certificados que se pueden importar a ACM o cargar en el almacén de certificados de IAM

Si ha obtenido sus certificados SSL/TLS de un distribuidor CA de terceros, debe almacenarlos en una de las siguientes ubicaciones:

- AWS Certificate Manager: para conocer la cuota actual de certificados de ACM, consulte Cuotas en la Guía del usuario de AWS Certificate Manager. La cuota mostrada es un total que incluye los certificados que aprovisione mediante ACM y los que importe a ACM.
- Almacén de certificados de IAM: para conocer la cuota (antes denominada límite) actual de certificados que puede cargar en el almacén de certificados de IAM de una cuenta de AWS, consulte Límites de IAM y STS en la Guía del usuario de IAM. Puede solicitar una cuota mayor en la consola de Service Quotas.

Cantidad máxima de certificados por cuenta de AWS (solo direcciones IP dedicadas)

Si desea atender solicitudes HTTPS a través de direcciones IP dedicadas, tenga en cuenta lo siguiente:

- De forma predeterminada, CloudFront le concede permiso para utilizar dos certificados con la cuenta de AWS, uno para uso diario y otro para cuando necesite rotar certificados para numerosas distribuciones.
- Si necesita más de dos certificados SSL/TLS personalizados para su cuenta de AWS, puede solicitar una cuota mayor en la consola de Service Quotas.

Uso del mismo certificado para distribuciones de CloudFront que se crearon con distintas cuentas de AWS

Si utiliza una entidad de certificación externa y desea utilizar el mismo certificado con varias distribuciones de CloudFront creadas con diferentes cuentas de AWS, debe importar el certificado a ACM o cargarlo en el almacén de certificados de IAM una vez por cada cuenta de AWS.

Si utiliza certificados proporcionados por ACM, no puede configurar CloudFront para utilizar certificados creados por una cuenta diferente de AWS.

Uso del mismo certificado para CloudFront y para otros servicios de AWS

Si ha comprado un certificado de una autoridad de certificación de confianza como Comodo DigiCert o Symantec, puede utilizar el mismo certificado para CloudFront y para otros servicios

de AWS. Si importa el certificado a ACM, solo es necesario importarlo una vez para utilizarlo con varios servicios de AWS.

Si utiliza certificados proporcionados por ACM, estos se almacenan en ACM.

Uso del mismo certificado para varias distribuciones de CloudFront

Puede utilizar el mismo certificado para una o todas las distribuciones de CloudFront que utilice para atender solicitudes HTTPS. Tenga en cuenta lo siguiente:

- Puede utilizar el mismo certificado tanto para atender solicitudes mediante direcciones IP dedicadas como para proporcionar solicitudes con SNI.
- Puede asociar solo un certificado a cada distribución.
- Cada distribución debe incluir uno o varios nombres de dominio alternativos que también aparecerán en los campos Common Name o Subject Alternative Names del certificado.
- Si está atendiendo solicitudes HTTPS mediante direcciones IP dedicadas y ha creado todas sus distribuciones con la misma cuenta de AWS, puede reducir significativamente sus costos si utiliza el mismo certificado para todas las distribuciones. CloudFront aplica cargos por cada certificado, no por cada distribución.

  Por ejemplo, suponga que crea tres distribuciones con la misma cuenta de AWS y que utiliza el mismo certificado para las tres distribuciones. Se le aplicará solo un cargo por el uso de direcciones IP dedicadas.

  Sin embargo, si atiende solicitudes HTTPS con direcciones IP dedicadas y con el mismo certificado para crear distribuciones de CloudFront en diferentes cuentas de AWS, a cada cuenta se le aplica el cargo por usar direcciones IP dedicadas. Por ejemplo, si crea tres distribuciones usando tres cuentas diferentes de AWS y utiliza el mismo certificado para las tres distribuciones, a cada cuenta se cobra el cargo completo de uso de direcciones IP dedicadas.

Configuración de nombres de dominio alternativos y HTTPS

Para utilizar nombres de dominio alternativos en las URL de los archivos y utilizar HTTPS entre los lectores y CloudFront, realice los procedimientos aplicables.

Temas

- Obtención de un certificado SSL/TLS
- Importación de un certificado SSL/TLS
- Actualización de la distribución de CloudFront

Obtención de un certificado SSL/TLS

Obtenga un certificado SSL/TLS si aún no dispone de uno. Para obtener más información, consulte la documentación aplicable:

- Para utilizar un certificado proporcionado por AWS Certificate Manager (ACM), consulte la Guía del usuario de AWS Certificate Manager. A continuación, diríjase a Actualización de la distribución de CloudFront.

> **Note**
>
> Le recomendamos que utilice ACM para aprovisionar, administrar e implementar los certificados SSL/TLS en los recursos administrados de AWS. Debe solicitar un certificado de ACM en la región EE. UU. Este (Norte de Virginia).

- Para obtener un certificado de una entidad de certificación (CA) de terceros, consulte la documentación que proporciona. Cuando tenga el certificado, continúe con el siguiente procedimiento.

Importación de un certificado SSL/TLS

Si ha obtenido el certificado de una entidad de certificación de terceros, importe el certificado a ACM o cárguelo en el almacén de certificados de IAM:

ACM (recomendado)

ACM le permite importar certificados de terceros desde la consola de ACM y de forma programada. Para obtener más información sobre la importación de un certificado a ACM, consulte Importación de certificados a AWS Certificate Manager en la Guía del usuario de AWS Certificate Manager. Debe importar el certificado en la región EE. UU. Este (Norte de Virginia).

Almacén de certificados de IAM

(No recomendado) Utilice el siguiente comando de AWS CLI para cargar el certificado de terceros en el almacén de certificados de 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/
```

Tenga en cuenta lo siguiente:

- Cuenta de AWS: debe cargar el certificado en el almacén de certificados de IAM con la misma cuenta de AWS que utilizó para crear la distribución de CloudFront.
- Parámetro --path: al cargar el certificado en IAM, el valor del parámetro `--path` (ruta del certificado) debe comenzar por `/cloudfront/`, por ejemplo, `/cloudfront/production/` o `/cloudfront/test/`. La ruta debe acabar con una /.
- Certificados existentes: debe especificar valores para los parámetros `--server-certificate-name` y `--path` que sean diferentes de los valores asociados con los certificados existentes.
- Uso de la consola de CloudFront: el valor que especifique para el parámetro `--server-certificate-name` en AWS CLI, por ejemplo, `myServerCertificate`, aparece en la lista SSL Certificate (Certificado SSL) de la consola de CloudFront.
- Con la API de CloudFront: anote la cadena alfanumérica que devuelve AWS CLI, por ejemplo, `AS1A2M3P4L5E67SIIXR3J`. Este es el valor que se especifica en el elemento `IAMCertificateId`. No es necesario el ARN de IAM, que también devuelve la CLI.

Para obtener más información sobre AWS CLI, consulte la Guía del usuario de AWS Command Line Interface y la Referencia de comandos de AWS CLI.

Actualización de la distribución de CloudFront

Para actualizar la configuración de su distribución, realice el siguiente procedimiento:

Para configurar la distribución de CloudFront para nombres de dominio alternativos

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la ID de la distribución que desea actualizar.
3. En la pestaña General, seleccione Edit.
4. Actualice los siguientes valores:

   Nombre de dominio alternativo (CNAME)

   Elija Agregar elemento para agregar los nombres de dominio alternativos aplicables. Separe los nombres de dominio con comas o escriba uno por línea.

Certificado SSL personalizado

Seleccione un certificado en el menú desplegable.

Aquí se enumeran hasta 100 certificados. Si tiene más de 100 certificados y no ve el certificado que desea añadir, puede escribir un ARN de certificado en el campo para elegirlo.

Si ha cargado un certificado al almacén de certificados de IAM pero no está en la lista y no puede elegirlo escribiendo el nombre en el campo, revise el procedimiento Importación de un certificado SSL/TLS para confirmar que el certificado se ha cargado correctamente.

> **Important**
>
> Después de asociar el certificado SSL/TLS a la distribución de CloudFront, no elimine el certificado de ACM ni el almacén de certificados de IAM hasta que haya eliminado el certificado de todas las distribuciones y se hayan implementado.

5. Seleccione Save changes (Guardar cambios).
6. Configure CloudFront para que solicite HTTPS entre lectores y CloudFront:
   a. En la pestaña Behaviors (Comportamientos), elija el comportamiento de la caché que desee actualizar y después elija Edit (Editar).
   b. Especifique uno de los siguientes valores en Viewer Protocol Policy (Política de protocolo del espectador):

      Redireccionamiento de HTTP a HTTPS

      Los espectadores pueden usar tanto el protocolo HTTP como el HTTPS, pero las solicitudes HTTP se redirigirán automáticamente a solicitudes HTTPS. CloudFront devuelve el código de estado HTTP `301 (Moved Permanently)` junto con la nueva URL HTTPS. A continuación, el lector vuelve a enviar la solicitud a CloudFront través de la URL HTTPS.

      > **Important**
      >
      > CloudFront no redirige las solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` ni `PUT` de HTTP a HTTPS. Si configura un comportamiento de la caché para que redirija a HTTPS, CloudFront responde a solicitudes HTTP `DELETE`, `OPTIONS`, `PATCH`,

`POST` o `PUT` para ese comportamiento de la caché con el código de estado HTTP `403 (Forbidden)`.

Cuando un lector realiza una solicitud HTTP que se redirige a una solicitud HTTPS, se aplican cargos de CloudFront a ambas solicitudes. En el caso de la solicitud HTTP, el cargo es solo para la solicitud y para los encabezados que CloudFront devuelve al lector. En el caso de la solicitud HTTPS, el cargo es por la solicitud y por los encabezados y el archivo que el origen devuelve.

Solo HTTPS

Los espectadores pueden obtener acceso a su contenido solo si utilizan HTTPS. Si un lector envía una solicitud HTTP en lugar de una solicitud HTTPS, CloudFront devuelve el código de estado HTTP `403 (Forbidden)` y no devuelve el archivo.

c. Elija Yes, Edit (Sí, editar).

d. Repita los pasos de la "a" a la "c" para cada comportamiento de la caché adicional para el que desee exigir HTTPS entre los lectores y CloudFront.

7. Confirme lo siguiente antes de utilizar la configuración actualizada en un entorno de producción:

- El patrón de ruta de cada comportamiento de la caché es aplicable únicamente a las solicitudes en las que desea que los espectadores utilicen HTTPS.
- Los comportamientos de la caché se muestran en el orden en que desee que CloudFront los evalúe. Para obtener más información, consulte Patrón de ruta.
- Los comportamientos de la caché son solicitudes de redirección hacia los orígenes correctos.

Determinación del tamaño de la clave pública en un certificado SSL/TLS RSA

Cuando se usan nombres de dominio alternativos de CloudFront y HTTPS, el tamaño máximo de la clave pública en un certificado SSL/TLS RSA es de 4096 bits. (Este es el tamaño de la clave, no es la cantidad de caracteres de la clave pública). Si utiliza AWS Certificate Manager para sus certificados, tenga en cuenta que aunque ACM admite claves más grandes, no se pueden usar con CloudFront.

Puede determinar el tamaño de la clave pública de RSA al ejecutar el siguiente comando OpenSSL:

```
openssl x509 -in path and filename of SSL/TLS certificate -text -noout
```

Donde:

- `-in` especifica la ruta y el nombre de archivo de su certificado SSL/TLS. RSA
- `-text` provoca que OpenSSL muestre la longitud de la clave pública de RSA en bits.
- `-noout` impide que OpenSSL muestre la clave pública.

Ejemplo de resultados:

```
Public-Key: (2048 bit)
```

Aumento de las cuotas de certificados SSL/TLS

Hay cuotas en cuanto a la cantidad de certificados SSL/TLS que puede importar a AWS Certificate Manager (ACM) o cargar en AWS Identity and Access Management (IAM). También hay una cuota en el número de certificados SSL/TLS que puede utilizar con una Cuenta de AWS al configurar CloudFront para atender solicitudes HTTPS con direcciones IP dedicadas. Sin embargo, puede solicitar una ampliación de dichas cuotas.

Temas

- Aumento de la cuota en certificados importados a ACM
- Aumento de la cuota en certificados subidos a IAM
- Aumento de la cuota en certificados utilizados con direcciones IP dedicadas

Aumento de la cuota en certificados importados a ACM

Para consultar la cuota de certificados que puede importar a ACM, consulte Cuotas en la Guía del usuario de AWS Certificate Manager.

Para solicitar una cuota más alta, use la consola de Service Quotas. Para obtener más información, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas.

Aumento de la cuota en certificados subidos a IAM

Para obtener información sobre la cuota (antes denominada límite) del número de certificados que puede cargar en IAM, consulte Límites de IAM y STS en la Guía del usuario de IAM.

Para solicitar una cuota más alta, use la consola de Service Quotas. Para obtener más información, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas.

Aumento de la cuota en certificados utilizados con direcciones IP dedicadas

Para conocer la cuota en el número de certificados SSL que puede utilizar por cada Cuenta de AWS si atiende solicitudes HTTPS utilizando direcciones IP dedicadas, consulte Cuotas en certificados SSL.

Para solicitar una cuota más alta, use la consola de Service Quotas. Para obtener más información, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas.

Rotación de certificados SSL/TLS

Cuando los certificados SSL/TLS estén a punto de caducar, tendrá que rotarlos para garantizar la seguridad de la distribución y evitar la interrupción del servicio para los lectores. Puede rotarlos de las siguientes formas:

- Para los certificados SSL/TLS proporcionados por AWS Certificate Manager (ACM), no es necesario rotarlos. ACM administra automáticamente las renovaciones de los certificados por usted. Para obtener más información, consulte Renovación administrada de certificados en la Guía del usuario de AWS Certificate Manager.
- Si utiliza una autoridad de certificación de terceros y ha importado certificados a ACM (recomendado) o los ha cargado en el almacén de certificados de IAM, debe sustituir ocasionalmente un certificado por otro.

> **Important**
>
> - ACM no administra renovaciones de certificados que adquiera de autoridades de certificación de terceros y que después importe a ACM.
> - Si configura CloudFront para atender solicitudes HTTPS a través de direcciones IP dedicadas, es posible que se aplique un cargo prorrateado adicional por uso de uno o varios certificados adicionales mientras rota certificados. Le recomendamos actualizar las distribuciones para minimizar los cargos adicionales.

Rotación de certificados SSL/TLS

Para rotar los certificados, realice el siguiente procedimiento. Los espectadores pueden seguir obteniendo acceso a su contenido mientras rota certificados y también una vez completado el proceso.

Para rotar certificados SSL/TLS

1. Aumento de las cuotas de certificados SSL/TLS para determinar si necesita permiso para utilizar más certificados SSL. En caso afirmativo, solicite el permiso y espere hasta que se le conceda antes de continuar con el paso 2.
2. Importe el nuevo certificado a ACM o cárguelo a IAM. Para obtener más información, consulte Importación de un certificado SSL/TLS en la Guía para desarrolladores de Amazon CloudFront.
3. (Solo para certificados de IAM) Actualice las distribuciones de una en una para utilizar el nuevo certificado. Para obtener más información, consulte Actualizar una distribución.
4. (Opcional) Elimine el certificado anterior de ACM o IAM.

> **Important**
>
> No elimine un certificado SSL/TLS hasta eliminarlo de todas las distribuciones y hasta que el estado de las distribuciones que ha actualizado haya cambiado a `Deployed`.

Reversión de un certificado SSL/TLS personalizado al certificado de CloudFront predeterminado

Si ha configurado CloudFront para utilizar HTTPS entre lectores y CloudFront y ha configurado CloudFront para utilizar un certificado SSL/TLS personalizado, puede cambiar la configuración para utilizar el certificado SSL/TLS de CloudFront predeterminado. El proceso depende de si ha utilizado la distribución para distribuir su contenido:

- Si no ha usado su distribución para distribuir su contenido, puede simplemente cambiar la configuración. Para obtener más información, consulte Actualizar una distribución.
- Si ha usado su distribución para distribuir el contenido, debe crear una nueva distribución de CloudFront y cambiar las URL de los archivos para reducir o eliminar la cantidad de tiempo que el contenido no va a estar disponible. Para ello, realice el siguiente procedimiento.

Reversión a certificado de CloudFront predeterminado

El siguiente procedimiento muestra cómo revertir de un certificado SSL/TLS personalizado al certificado de CloudFront predeterminado.

Para volver al certificado de CloudFront predeterminado

1. Cree una nueva distribución de CloudFront con la configuración deseada. En SSL Certificate (Certificado SSL), elija Default CloudFront Certificate (*.cloudfront.net) (Certificado de CloudFront predeterminado [*.cloudfront.net]).

   Para obtener más información, consulte Creación de una distribución.

2. En el caso de los archivos distribuidos con CloudFront, actualice las URL en la aplicación para que utilicen el nombre de dominio que CloudFront ha asignado a la nueva distribución. Por ejemplo, cambie `https://www.example.com/images/logo.png` a `https://d111111abcdef8.cloudfront.net/images/logo.png`.

3. Elimine la distribución asociada con un certificado SSL/TLS personalizado o actualice la distribución para cambiar el valor de SSL Certificate (Certificado SSL) a Default CloudFront Certificate (*.cloudfront.net) (Certificado de CloudFront predeterminado [*.cloudfront.net]). Para obtener más información, consulte Actualizar una distribución.

   > **Important**
   >
   > Hasta que complete este paso, AWS seguirá acumulando cargos por utilizar un certificado SSL/TLS personalizado.

4. Elimine su certificado SSL/TLS personalizado (opcional).

   a. Ejecute el comando AWS CLI de la `list-server-certificates` para obtener el ID del certificado que desea eliminar. Para obtener más información, consulte list-server-certificates en la Referencia de comandos de AWS CLI.

   b. Ejecute el comando `delete-server-certificate` de AWS CLI para eliminar el certificado. Para obtener más información, consulte delete-server-certificate en la Referencia de comandos de AWS CLI.

Cambio de un certificado SSL/TLS personalizado con direcciones IP dedicadas a SNI

Si configura CloudFront para utilizar un certificado SSL/TLS personalizado con direcciones IP dedicadas, puede utilizar un certificado SSL/TLS personalizado con SNI en su lugar y eliminar el cargo asociado a direcciones IP dedicadas.

> **Important**
>
> Esta actualización de la configuración de CloudFront no afecta a los lectores que admiten SNI. Los lectores pueden acceder al contenido antes y después del cambio, así como mientras el cambio se propaga a las ubicaciones de borde de CloudFront. Los espectadores que no admiten SNI no podrán obtener acceso a su contenido tras el cambio. Para obtener más información, consulte Elección de la forma en que CloudFront atiende las solicitudes HTTPS.

Cambio de un certificado personalizado a SNI

El siguiente procedimiento muestra cómo cambiar de un certificado SSL/TLS personalizado con direcciones IP dedicadas a SNI.

Para cambiar de un certificado SSL/TLS personalizado con direcciones IP dedicadas a SNI

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija el ID de la distribución que desea visualizar o actualizar.
3. Elija Distribution Settings (Configuración de distribución).
4. En la pestaña General, seleccione Edit.
5. En Certificación SSL personalizada (opcional), anule la selección de Soporte de clientes heredados.
6. Elija Sí, editar.

Autenticación TLS mutua con CloudFront (mTLS de espectador)

La autenticación TLS mutua (Autenticación de seguridad de la capa de transporte mutua: mTLS) es un protocolo de seguridad que amplía la autenticación TLS estándar al requerir una autenticación bidireccional basada en certificados, en la que tanto el cliente como el servidor deben demostrar su identidad antes de establecer una conexión segura. Con TLS mutua, puede asegurarse de que solo los clientes que presenten certificados TLS de confianza accedan a las distribuciones de CloudFront.

Funcionamiento

En un establecimiento de comunicación de TLS estándar, solo el servidor presenta un certificado que demuestre su identidad al cliente. Con TLS mutua, el proceso de autenticación pasa a ser bidireccional. Cuando un cliente intenta conectarse a la distribución de CloudFront, CloudFront solicita un certificado de cliente durante el establecimiento de comunicación de TLS. El cliente debe presentar un certificado X.509 válido que CloudFront valida en el almacén de confianza configurado antes de establecer la conexión segura.

CloudFront realiza esta validación de certificados en ubicaciones periféricas de AWS, lo que reduce la complejidad de la autenticación de los servidores de origen y, al mismo tiempo, mantiene los beneficios de rendimiento global de CloudFront. Puede configurar mTLS de dos modos: el modo de verificación (que requiere que todos los clientes presenten certificados válidos) o el modo opcional (que valida los certificados cuando se presentan, pero también permite las conexiones sin certificados).

Casos de uso

La autenticación TLS mutua con CloudFront aborda varios escenarios de seguridad críticos en los que los métodos de autenticación tradicionales son insuficientes:

- Autenticación de dispositivos con almacenamiento en caché de contenido: puede autenticar consolas de juegos, dispositivos de IoT o hardware corporativo antes de permitir el acceso a las actualizaciones de firmware, las descargas de juegos o los recursos internos. Cada dispositivo contiene un certificado único que demuestra su autenticidad y, al mismo tiempo, se beneficia de las capacidades de almacenamiento en caché de CloudFront.
- Autenticación de API a API: puede proteger la comunicación de máquina a máquina entre socios comerciales, sistemas de pago o microservicios de confianza. La autenticación basada en certificados elimina la necesidad de compartir secretos o claves de API, al tiempo que proporciona una sólida verificación de identidad para el intercambio de datos automatizado.

Temas

- Almacenes de confianza y administración de certificados
- Habilitación de TLS mutua para las distribuciones de CloudFront
- Asociación de una función de conexión de CloudFront
- Configuración adicional
- Encabezados de mTLS del espectador para las políticas de caché y reenvío al origen
- Revocación mediante la función de conexión de CloudFront y KVS
- Observabilidad mediante registros de conexión

Almacenes de confianza y administración de certificados

La creación y configuración de un almacén de confianza es un requisito obligatorio para implementar la autenticación TLS mutua con CloudFront. Los almacenes de confianza contienen los certificados de la autoridad de certificación (CA) que CloudFront utiliza para validar los certificados de los clientes durante el proceso de autenticación.

¿Qué es un almacén de confianza?

Un almacén de confianza es un repositorio de certificados CA que CloudFront utiliza para validar los certificados de los clientes durante la autenticación TLS mutua. Los almacenes de confianza contienen los certificados CA raíz e intermedios que forman la cadena de confianza para autenticar los certificados de los clientes.

Al implementar un TLS mutuo con CloudFront, el almacén de confianza define las autoridades de certificación en las que confía para emitir certificados de cliente válidos. CloudFront valida cada certificado de cliente con su almacén de confianza durante el establecimiento de comunicación de TLS. Solo los clientes que presenten certificados encadenados a una de las autoridades de certificación del almacén de confianza se autenticarán correctamente.

Los almacenes de confianza de CloudFront son recursos por cuenta que se pueden asociar a varias distribuciones. Esto permite mantener políticas de validación de certificados coherentes en toda la implementación de CloudFront y, al mismo tiempo, simplificar la administración de certificados CA.

Compatibilidad de la autoridad de certificación

CloudFront admite certificados emitidos tanto por una autoridad de certificación privada de AWS como por autoridades de certificación privadas de terceros. Esta flexibilidad permite utilizar la

infraestructura de certificados existente o aprovechar los servicios de certificación administrados de AWS en función de los requisitos de la organización.

- Autoridad de certificación privada de AWS: puede utilizar los certificados emitidos por la autoridad de certificación privada de AWS, que proporciona un servicio de autoridad de certificación privada administrada. Esta integración simplifica la administración del ciclo de vida de los certificados y proporciona una integración perfecta con otros servicios de AWS.
- Autoridades de certificación privadas de terceros: también puede utilizar los certificados de la infraestructura de autoridad de certificación privada existente, incluidas las autoridades de certificación empresariales u otros proveedores de certificados de terceros. Esto permite mantener los procesos actuales de administración de certificados y, al mismo tiempo, agregar las capacidades de mTLS de CloudFront.

Requisitos y especificaciones de certificados

Los almacenes de confianza tienen requisitos específicos para los certificados CA que contienen:

Requisitos de formato de certificado CA

- Formato: formato PEM (Correo con privacidad mejorada)
- Límites de contenido: los certificados deben estar dentro de los límites -----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----
- Comentarios: deben ir precedidos de un carácter # y no deben contener ningún carácter -
- Saltos de línea: no se permiten líneas en blanco entre los certificados

Especificaciones de certificados compatibles

- Tipo de certificado: X.509v3
- Tipos de claves públicas:
  - RSA 2048, RSA 4096
  - ECDSA: secp256r1, secp384r1
- Algoritmos de firma:
  - SHA256, SHA384, SHA512 con RSA
  - SHA256, SHA384, SHA512 con EC
  - SHA256, SHA384, SHA512 con RSASSA-PSS con MGF1

Ejemplo de formato de paquete de certificados

Varios certificados (codificados en PEM):

```
# Root CA Certificate
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIJAKoK/OvD/XqiMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTcwNzEyMTU0NzQ4WhcNMjcwNzEwMTU0NzQ4WjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuuExKvY1xzHFylsHiuowqpmzs7rEcuuylOuEszpFp+BtXh0ZuEtts9LP
-----END CERTIFICATE-----
# Intermediate CA Certificate
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIJAKoK/OvD/XqjMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTcwNzEyMTU0NzQ4WhcNMjcwNzEwMTU0NzQ4WjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuuExKvY1xzHFylsHiuowqpmzs7rEcuuylOuEszpFp+BtXh0ZuEtts9LP
-----END CERTIFICATE-----
```

Creación de un almacén de confianza

Antes de crear un almacén de confianza, debe cargar un paquete de certificados CA en formato PEM en un bucket de Amazon S3. El paquete de certificados debe contener todos los certificados CA raíz e intermedios de confianza necesarios para validar los certificados de los clientes.

El paquete de certificados CA solo se lee una vez desde S3 al crear un almacén de confianza. Si en el futuro se realizan cambios en el paquete de certificados CA, el almacén de confianza tendrá que actualizarse manualmente. No se mantiene ninguna sincronización entre el almacén de confianza y el paquete de certificados CA de S3.

Requisitos previos

- Un paquete de certificados de la autoridad de certificación (CA) cargado en un bucket de Amazon S3
- Los permisos necesarios para crear recursos de CloudFront

Creación de un almacén de confianza (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija Almacenes de confianza.
3. Seleccione Crear almacén de confianza.
4. En Nombre del almacén de confianza, introduzca un nombre para el almacén de confianza.
5. En Paquete de autoridad de certificación (CA), ingrese la ruta de Amazon S3 al paquete de certificados CA de formato PEM.
6. Seleccione Crear almacén de confianza.

Creación de un almacén de confianza (CLI de AWS)

```
aws cloudfront create-trust-store \
  --name MyTrustStore \
  --certificate-authority-bundle-s3-location Bucket=my-bucket,Key=ca-bundle.pem \
  --tags Items=[{Key=Environment,Value=Production}]
```

Asociación del almacén de confianza con las distribuciones

Tras crear un almacén de confianza, debe asociarlo a una distribución de CloudFront para habilitar la autenticación TLS mutua.

Requisitos previos

- Una distribución de CloudFront existente con la política de protocolo de espectador solo HTTPS habilitada y la compatibilidad con HTTP3 desactivada.

Asociación de un almacén de confianza (consola)

Hay dos formas de asociar un almacén de confianza a la consola de CloudFront: a través de la página de detalles del almacén de confianza o a través de la página de configuración de distribución.

Asociación de un almacén de confianza a través de la página de detalles del almacén de confianza:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija Almacenes de confianza.

3. Elija el nombre del almacén de confianza que desea asociar.
4. Elija Asociar a distribución.
5. Configure las opciones de mTLS de espectador disponibles:
   - Modo de validación del certificado de cliente: elija entre el modo obligatorio y el opcional. En el modo obligatorio, todos los clientes deben presentar los certificados. En el modo opcional, se validan los clientes que presentan certificados, mientras que a los clientes que no los presentan se les permite el acceso.
   - Anuncie los nombres de las autoridades de certificación de los almacenes de confianza: elija si desea anunciar los nombres de las autoridades de certificación del almacén de confianza a los clientes durante el establecimiento de comunicación de TLS.
   - Omita la fecha de caducidad del certificado: elija si desea permitir las conexiones con certificados caducados (se seguirán aplicando otros criterios de validación).
   - Función de conexión: se puede asociar una función de conexión opcional para permitir o denegar las conexiones en función de otros criterios personalizados.
6. Seleccione una o varias distribuciones para asociarlas al almacén de confianza. Solo las distribuciones con HTTP3 desactivado y con comportamientos de caché exclusivos de HTTPS pueden admitir los mTLS de espectador.
7. Elija Asociar.

Asociación de un almacén de confianza a través de la página de configuración de distribución:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleccione la distribución que desea asociar.
3. En la pestaña General, dentro del contenedor Configuración, elija Editar en la esquina superior derecha.
4. Desplácese hacia abajo hasta la parte inferior de la página, dentro del contenedor Conectividad, active el interruptor mTLS de espectador.
5. Configure las opciones de mTLS de espectador disponibles:
   - Modo de validación del certificado de cliente: elija entre el modo obligatorio y el opcional. En el modo obligatorio, todos los clientes deben presentar los certificados. En el modo opcional, se validan los clientes que presentan certificados, mientras que a los clientes que no los presentan se les permite el acceso.

- Anuncie los nombres de las autoridades de certificación de los almacenes de confianza: elija si desea anunciar los nombres de las autoridades de certificación del almacén de confianza a los clientes durante el establecimiento de comunicación de TLS.
- Omita la fecha de caducidad del certificado: elija si desea permitir las conexiones con certificados caducados (se seguirán aplicando otros criterios de validación).
- Función de conexión: se puede asociar una función de conexión opcional para permitir o denegar las conexiones en función de otros criterios personalizados.

6. Elija Guardar cambios en la esquina inferior derecha.

Asociación de un almacén de confianza (CLI de AWS)

Los almacenes de confianza se pueden asociar a las distribuciones mediante la propiedad DistributionConfig.ViewerMtlsConfig. Esto significa que primero debemos buscar la configuración de distribución y, a continuación, proporcionar ViewerMtlsConfig en una solicitud de UpdateDistribution posterior.

```
// First fetch the distribution
aws cloudfront get-distribution {DISTRIBUTION_ID}

// Update the distribution config, for example:
Distribution config, file://distConf.json:
{
  ...other fields,
  ViewerMtlsConfig: {
    Mode: 'required',
    TrustStoreConfig: {
        AdvertiseTrustStoreCaNames: false,
        IgnoreCertificateExpiry: true,
        TrustStoreId: {TRUST_STORE_ID}
    }
  }
}

aws cloudfront update-distribution \
   --id {DISTRIBUTION_ID} \
   --if-match {ETAG} \
   --distribution-config file://distConf.json
```

Administración de almacenes de confianza

Consulta de los detalles del almacén de confianza

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija Almacenes de confianza.
3. Elija el nombre del almacén de confianza para ver su página de detalles.

La página de detalles muestra:

- Nombre e ID del almacén de confianza
- Número de certificados CA
- Fecha de creación y fecha de última modificación
- Distribuciones asociadas
- Etiquetas

Modificación de un almacén de confianza

Para reemplazar un paquete de certificados CA:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija Almacenes de confianza.
3. Elija el nombre del almacén de confianza.
4. Elija Acciones y, a continuación, Editar.
5. Para el paquete de autoridades de certificación (CA), ingrese la ubicación de Amazon S3 del archivo PEM del paquete de autoridad de certificación actualizado.
6. Elija Actualización del almacén de confianza.

Eliminación de un almacén de confianza

Requisitos previos: primero debe desasociar el almacén de confianza de todas las distribuciones de CloudFront.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación izquierdo, elija Almacenes de confianza.
3. Elija el nombre del almacén de confianza.
4. Elija Eliminar almacén de confianza.
5. Elija Eliminar para confirmar.

Siguientes pasos

Tras crear y asociar el almacén de confianza a una distribución de CloudFront, puede proceder a habilitar la autenticación TLS mutua en la distribución y configurar ajustes adicionales, como el reenvío de los encabezados de los certificados a los orígenes. Para obtener instrucciones detalladas sobre cómo habilitar mTLS en las distribuciones, consulte Habilitación de TLS mutua para las distribuciones de CloudFront.

Habilitación de TLS mutua para las distribuciones de CloudFront

Requisitos previos y requisitos

El modo de verificación de TLS mutua de CloudFront exige que todos los clientes presenten certificados válidos durante el establecimiento de comunicación de TLS y rechaza las conexiones sin certificados válidos. Antes de habilitar TLS mutua en una distribución de CloudFront, asegúrese de que dispone de:

- Se ha creado un almacén de confianza con los certificados de autoridad de certificación
- Se ha asociado el almacén de confianza a la distribución de CloudFront
- Se ha asegurado que todos los comportamientos de la caché de distribución utilizan una política de protocolo de espectador solo HTTPS
- Se ha asegurado que la distribución utilice HTTP/2 (la configuración predeterminada, mTLS de espectador no es compatible con HTTP/3)

> **Note**
>
> La autenticación TLS mutua requiere conexiones HTTPS entre espectadores y CloudFront. No puede habilitar mTLS en una distribución con ningún comportamiento de caché que admita conexiones HTTP.

Habilitación de TLS mutua (consola)

Para distribuciones nuevas

mTLS de espectador no se puede configurar durante el proceso de creación de una nueva distribución en la consola de CloudFront. Primero cree la distribución por cualquier medio (consola, CLI, API) y, a continuación, edite la configuración de distribución para habilitar mTLS de espectador según las instrucciones de distribución existentes que se indican a continuación.

Para distribuciones existentes

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En la lista de distribución, seleccione la distribución que desee modificar.
3. Asegúrese de que la política del protocolo del espectador se establece en Redireccionamiento de HTTP a HTTPS o Solo HTTPS para todos los comportamientos de la caché. (Puede elegir la pestaña Comportamientos de la caché para ver y actualizar cualquier comportamiento de la caché con las políticas del protocolo HTTP).
4. Elija la pestaña General.
5. En la sección Settings (Configuración), elija Editar.
6. En la sección Conectividad, busque la Autenticación mutua del espectador (mTLS).
7. Active la opción Habilitar la autenticación mutua.
8. Para Modo de validación de certificados de cliente, seleccione Obligatorio (todos los clientes deben presentar certificados) u Opcional (los clientes pueden presentar certificados de forma opcional).
9. Para Almacén de confianza, seleccione el almacén de confianza que creó anteriormente.
10. (Opcional) Active la opción Anunciar nombres de autoridad de certificación de almacenes de confianza si desea que CloudFront envíe nombres de autoridades de certificación a los clientes durante el establecimiento de comunicación de TLS.

11. (Opcional) Active la opción Ignorar la fecha de caducidad del certificado si desea permitir las conexiones con certificados caducados.
12. Seleccione Save changes (Guardar cambios).

Habilitación de TLS mutua (CLI de AWS)

Para distribuciones nuevas

El siguiente ejemplo muestra cómo crear un archivo de configuración de distribución (distribution-config.json) que incluya la configuración de mTLS:

```
{
  "CallerReference": "cli-example-1",
  "Origins": {
    "Quantity": 1,
    "Items": [
      {
        "Id": "my-origin",
        "DomainName": "example.com",
        "CustomOriginConfig": {
          "HTTPPort": 80,
          "HTTPSPort": 443,
          "OriginProtocolPolicy": "https-only"
        }
      }
    ]
  },
  "DefaultCacheBehavior": {
    "TargetOriginId": "my-origin",
    "ViewerProtocolPolicy": "https-only",
    "MinTTL": 0,
    "ForwardedValues": {
      "QueryString": false,
      "Cookies": {
        "Forward": "none"
      }
    }
  },
  "ViewerCertificate": {
    "CloudFrontDefaultCertificate": true
  },
  "ViewerMtlsConfig": {
```

```
    "Mode": "required",
    "TrustStoreConfig": {
        "TrustStoreId": {TRUST_STORE_ID},
        "AdvertiseTrustStoreCaNames": true,
        "IgnoreCertificateExpiry": true
    }
  },
  "Enabled": true
}
```

Cree la distribución con mTLS habilitado mediante el siguiente comando de ejemplo:

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

Para distribuciones existentes

Obtenga la configuración de distribución actual mediante el siguiente comando de ejemplo:

```
aws cloudfront get-distribution-config --id E1A2B3C4D5E6F7 --output json > dist-
config.json
```

Edite el archivo para agregar la configuración de mTLS. Agregue la sección de ejemplo siguiente a la configuración de distribución:

```
"ViewerMtlsConfig": {
    "Mode": "required",
    "TrustStoreConfig": {
        "TrustStoreId": {TRUST_STORE_ID},
        "AdvertiseTrustStoreCaNames": true,
        "IgnoreCertificateExpiry": true
    }
}
```

Elimine el campo ETag del archivo, pero guarde su valor de forma independiente.

Actualice la distribución con la nueva configuración mediante el comando de ejemplo siguiente:

```
aws cloudfront update-distribution \
    --id E1A2B3C4D5E6F7 \
    --if-match YOUR-ETAG-VALUE \
```

```
    --distribution-config file://dist-config.json
```

Políticas de protocolo para espectadores

Cuando se utiliza TLS mutua, todos los comportamientos de la caché distribuida se deben configurar con una política de protocolo de espectador solo HTTPS:

- Redirección de HTTP a HTTPS: redirige las solicitudes HTTP a HTTPS antes de realizar la validación del certificado.
- Solo HTTPS: solo acepta solicitudes HTTPS y realiza la validación del certificado.

> **Note**
>
> La política de protocolo de espectador HTTP y HTTPS no es compatible con TLS mutua, ya que las conexiones HTTP no pueden realizar la validación de los certificados.

Siguientes pasos

Tras habilitar TLS del espectador en la distribución de CloudFront, puede asociar las funciones de conexión para implementar una lógica de validación de certificados personalizada. Las funciones de conexión le permiten ampliar las capacidades de autenticación mTLS integradas con reglas de validación, comprobación de la revocación de certificados y registros personalizados. Para obtener más información sobre la creación y asociación de funciones de conexión, consulte Asociación de una función de conexión de CloudFront.

Asociación de una función de conexión de CloudFront

Las funciones de conexión de CloudFront permiten implementar una lógica de validación de certificados personalizada durante los establecimientos de comunicación de TLS, lo que amplía las capacidades de autenticación mTLS integradas.

¿Qué son las funciones de conexión?

Las funciones de conexión son funciones de JavaScript que se ejecutan durante el establecimiento de comunicación de TLS después de que se hayan validado los certificados de cliente. El certificado de cliente validado se pasa a la función de conexión, momento en el que la función de conexión puede tomar una decisión adicional sobre si conceder o no el acceso. Para obtener información

detallada sobre las funciones de conexión, consulte Personalización en la periferia con CloudFront Functions.

Cómo funcionan las funciones de conexión con mTLS

Cuando un cliente intenta establecer una conexión de mTLS con la distribución de CloudFront, se produce la siguiente secuencia:

1. El cliente inicia el establecimiento de comunicación de TLS con la ubicación periférica de CloudFront.
2. CloudFront solicita y recibe el certificado de cliente.
3. CloudFront realiza una validación de certificados estándar en un almacén de confianza.
4. Si el certificado pasa la validación estándar, CloudFront invoca la función de conexión. Si IgnoreCertificateExpiry está activado en ViewerMtlsConfig, los certificados vencidos (pero válidos por lo demás) también se transfieren a la función de conexión. Si los certificados de cliente no son válidos, no se invocarán las funciones de conexión.
5. La función de conexión recibe la información del certificado analizada y los detalles de la conexión.
6. La función toma una decisión de permitir o denegar en función de una lógica personalizada.
7. CloudFront completa o finaliza la conexión de TLS en función de su decisión.

Las funciones de conexión se invocan tanto en el modo de verificación como en el modo opcional (cuando los clientes presentan certificados).

Solicitud de un aumento de la cuota de la función de conexión

Solicite un aumento de la cuota de la función de conexión para la Cuenta de AWS.

Solicitud de un aumento de la cuota de la función de conexión

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleccione Funciones en el panel de navegación.
3. Elija la pestaña Funciones de conexión.
4. En Solicitar, elija el enlace para ponerse en contacto con el departamento de ingeniería de soporte de CloudFront.

5. Los ingenieros de soporte de CloudFront revisan su solicitud. El proceso de revisión puede tardar hasta dos días.

Una vez aprobada la solicitud, puede crear una función de conexión en la cuenta y asociarla a una o varias distribuciones mediante TLS mutua.

Creación de una función de conexión

Puede crear funciones de conexión mediante la consola de CloudFront o la CLI de AWS.

Creación de una función de conexión (consola)

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleccione Funciones en el panel de navegación.
3. Elija la pestaña Funciones de conexión y, a continuación, elija Crear función de conexión.
4. Ingrese un nombre de función que sea exclusivo dentro de la cuenta de AWS.
5. Elija Continuar.
6. En el editor de funciones, escriba el código de JavaScript para la validación del certificado. El controlador de funciones debe llamar a permitir o rechazar.
7. Opcional: se puede asociar un almacén KeyValue a la función de conexión para implementar el control de revocación.
8. Seleccione Save changes (Guardar cambios).

Creación de una función de conexión (CLI de AWS)

En el siguiente ejemplo, se muestra cómo crear una función de conexión:

Escriba el código de la función en un archivo independiente, por ejemplo, code.js:

```
function connectionHandler(connection) {
  connection.allow();
}
```

```
aws cloudfront create-connection-function \
  --name "certificate-validator" \
  --connection-function-config '{
```

```
      "Comment": "Client certificate validation function",
      "Runtime": "cloudfront-js-2.0"
  }' \
  --connection-function-code fileb://code.js
```

Estructura de código de la función de conexión

Las funciones de conexión implementan la función connectionHandler que recibe un objeto de conexión que contiene el certificado y la información de conexión. La función debe utilizar una de las dos opciones, `connection.allow()` o `connection.deny()`, para tomar una decisión sobre la conexión.

Ejemplo de función de conexión básica

En el siguiente ejemplo, se muestra una función de conexión sencilla que verifica el campo de asunto de los certificados de cliente:

```
function connectionHandler(connection) {
    // Only process if a certificate was presented
    if (!connection.clientCertificate) {
        console.log("No certificate presented");
        connection.deny();
    }

    // Check the subject field for specific organization
    const subject = connection.clientCertificate.certificates.leaf.subject;
    if (!subject.includes("O=ExampleCorp")) {
        console.log("Certificate not from authorized organization");
       connection.deny();
    } else {
        // All checks passed
        console.log("Certificate validation passed");
        connection.allow();
    }
}
```

La especificación completa de las propiedades del certificado de cliente disponibles en el objeto de conexión está disponible aquí:

```
{
  "connectionId": "Fdb-Eb7L9gVn2cFakz7wWyBJIDAD4-oNO6g8r3vXDV132BtnIVtqDA==", // Unique
 identifier for this TLS connection
```

```
  "clientIp": "203.0.113.42", // IP address of the connecting client (IPv4 or IPv6)
  "clientCertificate": {
    "certificates": {
      "leaf": {
        "subject": "CN=client.example.com,O=Example Corp,C=US", // Distinguished Name
 (DN) of the certificate holder
        "issuer": "CN=Example Corp Intermediate CA,O=Example Corp,C=US", //
 Distinguished Name (DN) of the certificate authority that issued this certificate
        "serialNumber": "4a:3f:5c:92:d1:e8:7b:6c", // Unique serial number assigned by
 the issuing CA (hexadecimal)
        "validity": {
          "notBefore": "2024-01-15T00:00:00Z", // Certificate validity start date (ISO
 8601 format)
          "notAfter": "2025-01-14T23:59:59Z"   // Certificate expiration date (ISO 8601
 format)
        },
        "sha256Fingerprint": "a1b2c3d4e5f6...abc123def456", // SHA-256 hash of the
 certificate (64 hex characters)
      },
    },
  },
}
```

Asociación de una función de conexión

Tras crear la función de conexión, debe publicarla en la etapa ACTIVA y asociarla a la distribución.

Publicación y asociación de una función de conexión (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleccione Funciones en el panel de navegación
3. Elija la pestaña Funciones de conexión y seleccione la función de conexión.
4. Elija Publicar para moverla a la etapa ACTIVA.
5. Elija Agregar asociación en la tabla de distribuciones asociadas situada debajo de la sección de publicación.
6. Seleccione la distribución que desee asociar con mTLS de espectador habilitado.

Como opción alternativa, las funciones de conexión publicadas también se pueden asociar desde la página de detalles de la distribución.

1. Diríjase a la página de inicio de la consola, donde se muestran todas las distribuciones.
2. Seleccione la distribución que desea asociar.
3. Elija la pestaña General.
4. En la sección Settings (Configuración), elija Editar.
5. En la sección Conectividad, busque la Autenticación mutua del espectador (mTLS).
6. Para Función de conexión, seleccione la función.
7. Seleccione Save changes (Guardar cambios).

Asociación de una función de conexión (CLI de AWS)

En el siguiente ejemplo, se muestra cómo asociar una función de conexión a una distribución:

```
// DistributionConfig:
{
   ...other settings,
    "ConnectionFunctionAssociation": {
        "Id": "cf_30c2CV2elHwCoInb3LtcaUJkZeD"
    }
}
```

Casos de uso para funciones de conexión

Las funciones de conexión permiten varios casos de uso avanzados de mTLS:

- Validación de los atributos de los certificados: verifique campos específicos de los certificados de los clientes, como los requisitos de las unidades organizativas o los patrones de nombres alternativos de los temas.
- Comprobación de la revocación de certificados: Implemente una comprobación de revocación de certificados personalizada mediante KeyValueStore para almacenar los números de serie de los certificados revocados.
- Políticas de certificados basadas en IP: aplique diferentes políticas de certificación en función de las direcciones IP de los clientes o de las restricciones geográficas.
- Validación multiusuario: implemente reglas de validación específicas para cada inquilino en las que se apliquen diferentes requisitos de certificación en función de los nombres de host o los atributos de certificados.

> **Note**
>
> Las funciones de conexión se ejecutan una vez por conexión de cliente durante el establecimiento de comunicación de TLS.
> Las funciones de conexión solo pueden permitir o denegar las conexiones, no modificar las solicitudes o respuestas HTTP.
> Solo las funciones de etapa ACTIVA (publicadas) se pueden asociar a las distribuciones.
> Cada distribución puede tener como máximo una función de conexión.

Siguientes pasos

Tras asociar una función de conexión a la distribución de CloudFront, puede configurar los ajustes opcionales para personalizar el comportamiento de la implementación de mTLS. Para obtener instrucciones detalladas sobre cómo configurar ajustes adicionales, como un modo de validación de certificados de cliente opcional, consulte Configuración adicional.

Configuración adicional

Tras habilitar la autenticación TLS mutua básica, puede configurar ajustes adicionales para personalizar el comportamiento de autenticación para casos de uso y requisitos específicos.

Modo opcional de validación de certificados de cliente

CloudFront ofrece un modo de validación de certificados de cliente opcional alternativo que valida los certificados de cliente que se presentan, pero permite el acceso a los clientes que no presentan certificados.

Comportamiento del modo opcional

- Otorga la conexión a los clientes con certificados válidos (se deniegan los certificados no válidos).
- Permite la conexión a clientes sin certificados.
- Permite escenarios de autenticación de clientes mixtos a través de una única distribución.

El modo opcional es ideal para la migración gradual a la autenticación mTLS, para dar soporte a clientes con certificados y clientes sin certificados, o para mantener la compatibilidad con versiones anteriores de clientes antiguos.

> **Note**
>
> En el modo opcional, las funciones de conexión se siguen invocando incluso cuando los clientes no presentan certificados. Esto permite implementar una lógica personalizada, como registrar las direcciones IP de los clientes o aplicar diferentes políticas en función de si se presentan los certificados.

Configuración del modo opcional (consola)

1. En la configuración de distribución, vaya a la pestaña General y elija Editar.
2. Desplácese hasta la sección Autenticación mutua (mTLS) del espectador en el contenedor Conectividad.
3. Para Modo de validación de certificado de cliente, seleccione Opcional.
4. Guarde los cambios.

Configuración del modo opcional (CLI de AWS)

En el siguiente ejemplo, se muestra cómo configurar el modo opcional:

```
"ViewerMtlsConfig": {
   "Mode": "optional",
   ...other settings
}
```

Anuncio de la autoridad de certificación

El campo AdvertiseTrustStoreCaNames controla si CloudFront envía la lista de nombres de autoridad de certificación de confianza a los clientes durante el establecimiento de comunicación de TLS, lo que ayuda a los clientes a seleccionar el certificado adecuado.

Configuración de la publicidad de la autoridad de certificación (consola)

1. En la configuración de distribución, vaya a la pestaña General y elija Editar.
2. Desplácese hasta la sección Autenticación mutua (mTLS) del espectador en el contenedor Conectividad.

3. Active o desactive la casilla de verificación Anunciar nombres de autoridad de certificación de almacenes de confianza.
4. Seleccione Save changes (Guardar cambios).

Configuración de la publicidad de la autoridad de certificación (CLI de AWS)

En el ejemplo siguiente, se muestra cómo habilitar la publicidad de la autoridad de certificación:

```
"ViewerMtlsConfig": {
   "Mode": "required", // or "optional"
   "TrustStoreConfig": {
      "AdvertiseTrustStoreCaNames": true,
      ...other settings
   }
}
```

Gestión de caducidad de certificados

La propiedad IgnoreCertificateExpiry determina cómo responde CloudFront a los certificados de cliente caducados. De forma predeterminada, CloudFront rechaza los certificados de cliente caducados, pero puede configurarlo para que los acepte cuando sea necesario. Por lo general, esto se habilita para dispositivos con certificados caducados que no se pueden actualizar fácilmente.

Configuración de la gestión de la caducidad de los certificados (consola)

1. En la configuración de distribución, vaya a la pestaña General y elija Editar.
2. Desplácese hasta la sección Autenticación mutua (mTLS) del espectador del contenedor Conectividad.
3. Seleccione o desmarque la casilla de verificación Omitir la fecha de caducidad del certificado.
4. Seleccione Save changes (Guardar cambios).

Configuración de la gestión de la caducidad de los certificados (CLI de AWS)

En el siguiente ejemplo, se muestra cómo ignorar la caducidad de un certificado:

```
"ViewerMtlsConfig": {
  "Mode": "required", // or "optional"
```

```
  "TrustStoreConfig": {
     "IgnoreCertificateExpiry": false,
     ...other settings
  }
}
```

> **Note**
>
> IgnoreCertificateExpiry solo se aplica a las fechas de validez de los certificados. Se siguen aplicando todas las demás comprobaciones de validación de certificados (cadena de confianza, validación de firmas).

Siguientes pasos

Tras configurar ajustes adicionales, puede configurar el reenvío de encabezados para transferir la información del certificado a los orígenes, implementar la revocación de certificados mediante funciones de conexión y KeyValueStore, y habilitar los registros de conexión para su supervisión. Para obtener más información sobre cómo reenviar la información de los certificados a los orígenes, consulte Reenviar encabezados a los orígenes.

Encabezados de mTLS del espectador para las políticas de caché y reenvío al origen

Al utilizar la autenticación TLS mutua, CloudFront puede extraer información de los certificados de cliente y reenviarla a los orígenes como encabezados HTTP. Esto permite que los servidores de origen accedan a los detalles de los certificados sin implementar una lógica de validación de certificados.

Los siguientes encabezados están disponibles para crear comportamientos de caché:

Nombre del encabezado	Descripción	Ejemplo de valor
CloudFront-Viewer-Cert-Serial-Number	Representación hexadecimal del número de serie del certificado	4a:3f:5c:92:d1:e8:7b:6c

Nombre del encabezado	Descripción	Ejemplo de valor
CloudFront-Viewer-Cert-Issuer	Representación de cadena RFC2253 del nombre distintivo (DN) del emisor	CN=rootcamtls.com,OU=rootCA,O=mTLS,L=Seattle,ST=Washington,C=US
CloudFront-Viewer-Cert-Subject	Representación de cadena RFC2253 del nombre distintivo (DN) del sujeto	CN=client_.com,OU=client-3,O=mTLS,ST=Washington,C=US
CloudFront-Viewer-Cert-Present	1 (presente) o 0 (no presente) indican si el certificado está presente. Este valor siempre es 1 en el modo obligatorio.	1
CloudFront-Viewer-Cert-Sha256	El hash SHA256 del certificado del cliente	01fbf94fef5569753420c349f49adbfd80af5275377816e3ab1fb371b29cb586

Para las solicitudes de origen, se proporcionan dos encabezados adicionales, además de los encabezados anteriores disponibles para los comportamientos de la caché:

Nombre del encabezado	Descripción	Ejemplo de valor
CloudFront-Viewer-Cert-Validity	Formato ISO8601 de la fecha notBefore y notAfter	CloudFront-Viewer-Cert-Validity: NotBefore=2023-09-21T01:50:17Z;NotAfter=2024-09-20T01:50:17Z
CloudFront-Viewer-Cert-Pem	Formato PEM codificado en URL del certificado de hoja	CloudFront-Viewer-Cert-Pem: -----BEGIN%20CERTIFICATE-----%0AMIIG<...reduced...>NmrUlw%0A-----END%20CERTIFICATE-----%0A

Configuración del reenvío de encabezados

Consola

En el modo de verificación, CloudFront agrega automáticamente los encabezados CloudFront-Viewer-Cert-* a todas las solicitudes de los espectadores. Reenvío de estos encabezados al origen:

1. En la página principal de distribuciones de la lista, seleccione la distribución con el mTLS de espectador habilitado y vaya a la pestaña Comportamientos.
2. Seleccione el comportamiento de caché y elija Editar.
3. En la sección Política de solicitudes de origen, elija Crear política o seleccione una política existente.
4. Asegúrese de que los siguientes encabezados estén incluidos en la política de solicitud de origen:
   - CloudFront-Viewer-Cert-Serial-Number
   - CloudFront-Viewer-Cert-Issuer
   - CloudFront-Viewer-Cert-Subject
   - CloudFront-Viewer-Cert-Present
   - Cloudfront-Viewer-Cert-Sha256
   - CloudFront-Viewer-Cert-Validity
   - CloudFront-Viewer-Cert-Pem
5. Elija Crear (para políticas nuevas) o Guardar cambios (para políticas existentes).
6. Seleccione la política que se ajuste al comportamiento de la memoria caché y guarde los cambios.

Uso de la CLI de AWS

En el siguiente ejemplo se muestra cómo crear una política de solicitud de origen que incluya encabezados mTLS para el modo de verificación:

```
aws cloudfront create-origin-request-policy \
  --origin-request-policy-config '{
    "Name": "MTLSHeadersPolicy",
    "HeadersConfig": {
      "HeaderBehavior": "whitelist",
```

```
      "Headers": {
        "Quantity": 5,
        "Items": [
          "CloudFront-Viewer-Cert-Serial-Number",
          "CloudFront-Viewer-Cert-Issuer",
          "CloudFront-Viewer-Cert-Subject",
          "CloudFront-Viewer-Cert-Validity",
          "CloudFront-Viewer-Cert-Pem"
        ]
      }
    },
    "CookiesConfig": {
      "CookieBehavior": "none"
    },
    "QueryStringsConfig": {
      "QueryStringBehavior": "none"
    }
  }'
```

Consideraciones sobre el procesamiento de encabezados

Cuando trabaje con encabezados de certificados, tenga en cuenta estas prácticas recomendadas:

- Validación de encabezados: compruebe los valores de los encabezados de los certificados en el origen como medida de seguridad adicional
- Límites de tamaño de los encabezados: los encabezados de los certificados PEM pueden ser grandes, asegúrese de que el servidor de origen pueda gestionarlos
- Consideraciones sobre la caché: el uso de encabezados de certificado en la clave de caché aumenta la fragmentación de la caché
- Solicitudes de origen cruzado: si la aplicación usa CORS, es posible que deba configurarla para permitir los encabezados de los certificados

Siguientes pasos

Tras configurar el reenvío de encabezados, puede implementar la comprobación de la revocación de certificados mediante funciones de conexión de CloudFront y KeyValueStore. Para obtener más información sobre la implementación de las comprobaciones de revocación, consulte Revocación mediante la función de conexión de CloudFront y KVS.

Revocación mediante la función de conexión de CloudFront y KVS

Puede implementar la comprobación de revocación de certificados para la autenticación TLS mutua combinando funciones de conexión de CloudFront con KeyValueStore. Este enfoque proporciona un mecanismo de revocación de certificados escalable y en tiempo real que complementa la validación de certificados integrada en CloudFront.

Las funciones de conexión son funciones de JavaScript que se ejecutan durante el establecimiento de la conexión de TLS en las ubicaciones periféricas de CloudFront y permiten implementar una lógica de validación de certificados personalizada para la autenticación mTLS. Para obtener información detallada sobre las funciones de conexión, consulte Asociación de una función de conexión de CloudFront.

Cómo funciona la revocación de certificados con funciones de conexión

La validación de certificados estándar de CloudFront verifica la cadena, la firma y la caducidad del certificado, pero no incluye la comprobación de revocación de certificados integrada. Al usar funciones de conexión, puede implementar una comprobación de revocación personalizada durante el establecimiento de comunicación de TLS.

El proceso de revocación de certificados funciona de la siguiente manera:

1. Guarde los números de serie de los certificados revocados en un KeyValueStore de CloudFront.
2. Cuando un cliente presenta un certificado, se invoca la función de conexión.
3. La función compara el número de serie del certificado con el KeyValueStore.
4. Si el número de serie se encuentra en la tienda, se revoca el certificado.
5. Su función deniega la conexión en el caso de los certificados revocados.

Este enfoque permite comprobar las revocaciones prácticamente en tiempo real en toda la red de periferia global de CloudFront.

Configuración de KeyValueStore para certificados revocados

En primer lugar, cree un KeyValueStore para almacenar los números de serie de los certificados revocados:

Creación de un KeyValueStore (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Almacenes de valores de claves.
3. Elija Creación de un almacén de valores de claves.
4. Ingrese un nombre para el almacén de valores de claves (por ejemplo, certificados revocados).
5. (Opcional) Añada una descripción.
6. Elija Creación de un almacén de valores de claves.

Creación de un KeyValueStore (CLI de AWS)

En el ejemplo siguiente se muestra cómo crear un KeyValueStore:

```
aws cloudfront create-key-value-store \
  --name "revoked-certificates" \
  --comment "Store for revoked certificate serial numbers"
```

Importación de los números de serie de los certificados revocados

Después de crear un KeyValueStore, debe importar los números de serie de los certificados revocados:

Preparación de los datos de revocación

Cree un archivo JSON con los números de serie de los certificados revocados:

```
{
  "data": [
    {
      "key": "ABC123DEF456",
      "value": ""
    },
    {
      "key": "789XYZ012GHI",
      "value": ""
    }
```

```
  ]
}
```

Importar desde S3

1. Carga del archivo JSON en un bucket de S3
2. Importación del archivo al KeyValueStore:

```
aws cloudfront create-key-value-store \
  --name "revoked-certificates" \
  --import-source '{
    "SourceType": "S3",
    "SourceARN": "arn:aws:s3:::amzn-s3-demo-bucket1/revoked-serials.json"
  }'
```

Creación de una función de conexión para comprobar las revocaciones

Cree una función de conexión que compruebe los números de serie de los certificados con el KeyValueStore:

Ejemplo de código de función de conexión

En el ejemplo siguiente, se muestra una función de conexión que realiza la comprobación de la revocación de certificados:

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Get client certificate serial number
    const clientSerialNumber =
 connection.clientCertificate.certificates.leaf.serialNumber;

    // Check if the serial number exists in the KeyValueStore
    const isRevoked = await kvsHandle.exists(clientSerialNumber.replaceAll(':', ''));

    if (isRevoked) {
        console.log(`Certificate ${clientSerialNumber} is revoked. Denying
 connection.`);
```

```
        connection.logCustomData(`REVOKED:${clientSerialNumber}`);
        connection.deny();
    } else {
        console.log(`Certificate ${clientSerialNumber} is valid. Allowing
 connection.`);
        connection.allow();
    }

}
```

Creación de la función de conexión (CLI de AWS)

En el siguiente ejemplo, se muestra cómo crear una función de conexión con la asociación de KeyValueStore:

```
aws cloudfront create-connection-function \
  --name "revocation-checker" \
  --connection-function-config '{
      "Comment": "Certificate revocation checking function",
      "Runtime": "cloudfront-js-2.0",
      "KeyValueStoreAssociations": {
          "Quantity": 1,
          "Items": [
              {
                  "KeyValueStoreARN": "arn:aws:cloudfront::123456789012:key-value-
store/revoked-certificates"
              }
          ]
      }
  }' \
  --connection-function-code fileb://revocation-checker.js
```

Asociación de la función con la distribución

Tras crear y publicar la función de conexión, asóciela a la distribución de CloudFront compatible con mTLS, tal y como se describe en la sección Asociación de una función de conexión de CloudFront.

Observabilidad mediante registros de conexión

Los registros de conexión de CloudFront proporcionan una visibilidad detallada de los eventos de autenticación TLS mutua, lo que permite supervisar la validación de los certificados, realizar un seguimiento de los intentos de conexión y solucionar problemas de autenticación.

¿Qué son los registros de conexión?

Los registros de conexión recopilan información detallada sobre los establecimientos de comunicación de TLS y la validación de certificados en el caso de distribuciones mutuas compatibles con TLS. A diferencia de los registros de acceso estándar que registran la información de las solicitudes HTTP, los registros de conexión se centran específicamente en la fase de establecimiento de la conexión de TLS, e incluyen:

- Estado de la conexión (éxito/error)
- Detalles del certificado del cliente
- Información de cifrado y protocolo TLS
- Métricas de temporización de conexión
- Datos personalizados de funciones de conexión

Estos registros proporcionan una visibilidad completa de los eventos de autenticación basados en certificados, lo que lo ayuda a supervisar la seguridad, solucionar problemas y cumplir con los requisitos de conformidad.

Habilitación de registros de conexión

Los registros de conexión solo están disponibles para las distribuciones con la autenticación TLS mutua habilitada. Puede enviar registros de conexión a varios destinos, incluidos registros de CloudWatch, Amazon Data Firehose y Amazon S3.

Requisitos previos

Antes de habilitar los registros de conexión:

- Configure TLS mutua para la distribución de CloudFront.
- Habilite los registros de conexión para la distribución de CloudFront.
- Asegúrese de que dispone de los permisos necesarios para el destino de registro elegido.
- Para realizar entregas entre cuentas, configure las políticas de IAM adecuadas.

Habilitación de registros de conexión (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En la lista de distribución, seleccione la distribución compatible con mTLS.
3. Elija la pestaña Logging (Registro).
4. Elija Agregar.
5. Seleccione el servicio para recibir los registros:
   - Registros de CloudWatch
   - Firehose
   - Amazon S3
6. Para Destino, seleccione el recurso para el servicio elegido:
   - Para registros de CloudWatch, ingrese el Nombre del grupo de registro.
   - Para Firehose, seleccione el Flujo de entrega de Firehose.
   - Para Amazon S3, ingrese el Nombre del bucket (opcionalmente con un prefijo)
7. (Opcional) Configure ajustes adicionales:
   - Selección de campos: seleccione los campos de registro específicos que desee incluir.
   - Formato de salida: elija entre JSON, Plain, w3c, Raw o Parquet (solo S3).
   - Delimitador de campo: especifique cómo separar los campos de registro.
8. Elija Guardar cambios.

Habilitación de los registros de conexión (CLI de AWS)

En el siguiente ejemplo, se muestra cómo habilitar registros de conexión mediante la API de CloudWatch:

```
# Step 1: Create a delivery source
aws logs put-delivery-source \
  --name "cf-mtls-connection-logs" \
  --resource-arn "arn:aws:cloudfront::123456789012:distribution/E1A2B3C4D5E6F7" \
  --log-type CONNECTION_LOGS

# Step 2: Create a delivery destination
aws logs put-delivery-destination \
```

```
  --name "s3-destination" \
  --delivery-destination-configuration \
  "destinationResourceArn=arn:aws:s3:::amzn-s3-demo-bucket1"

# Step 3: Create the delivery
aws logs create-delivery \
  --delivery-source-name "cf-mtls-connection-logs" \
  --delivery-destination-arn "arn:aws:logs:us-east-1:123456789012:delivery-
destination:s3-destination"
```

> **Note**
>
> Al utilizar la API de CloudWatch, debe especificar la región Este de EE. UU. (Norte de Virginia) (us-east-1), incluso al entregar registros a otras regiones.

Campos de registro de conexión

Los registros de conexión incluyen información detallada sobre cada intento de conexión de TLS:

Campo	Descripción	Ejemplo
`eventTimestamp`	Marca temporal ISO 8601 de cuando se estableció la conexión o se produjo un error	1731620046814
`connectionId`	Identificador único para la conexión de TLS	`oLHiEKbQSn8lkvJfA3D4gFowK3_iZ0g4i5nMUjE1Akod8TuAzn5nzg==`
`connectionStatus`	El estado del intento de conexión de mTLS.	`Success` o `Failed`
`clientIp`	La dirección IP del cliente que se conecta	`2001:0db8:85a3:0000:0000:8a2e:0370:7334`
`clientPort`	Puerto utilizado por el cliente	12137
`serverIp`	Dirección IP del servidor perimetral de CloudFront	`99.84.71.136`

Campo	Descripción	Ejemplo
distributionId	ID de distribución de CloudFront	E2DX1SLDPK0123
distributionTenantId	ID de inquilino de distribución de CloudFront (cuando proceda)	dt_2te1Ura9X3R2iCGNjW123
tlsProtocol	La versión del protocolo TLS usado	TLSv1.3
tlsCipher	Conjunto de cifrado TLS utilizado para la conexión	TLS_AES_128_GCM_SHA256
tlsHandshakeDuration	Duración del establecimiento de comunicación de TLS en milisegundos	153
tlsSni	Valor de indicación del nombre del servidor obtenido del establecimiento de comunicación de TLS	d111111abcdef8.cloudfront.net
clientLeafCertSerialNumber	Número de serie del certificado del cliente	00:b1:43:ed:93:d2:d8:f3:9d
clientLeafCertSubject	Campo de asunto del certificado del cliente	C=US, ST=WA, L=Seattle, O=Amazon.com, OU=CloudFront, CN=client.test.mtls.net
clientLeafCertIssuer	Campo de emisor del certificado del cliente	C=US, ST=WA, L=Seattle, O=Amazon.com, OU=CloudFront, CN=test.mtls.net
clientLeafCertValidity	Periodo de validez del certificado del cliente	NotBefore=2025-06-05T23:28:21Z;NotAfter=2125-05-12T23:28:21Z

Campo	Descripción	Ejemplo
`connectionLogCustomData`	Datos personalizados agregados a través de las funciones de conexión	`REVOKED:00:b1:43:ed:93:d2:d8:f3:9d`

Códigos de error de conexión

```
Failed:ClientCertMaxChainDepthExceeded
Failed:ClientCertMaxSizeExceeded
Failed:ClientCertUntrusted
Failed:ClientCertNotYetValid
Failed:ClientCertExpired
Failed:ClientCertTypeUnsupported
Failed:ClientCertInvalid
Failed:ClientCertIntentInvalid
Failed:ClientCertRejected
Failed:ClientCertMissing
Failed:TcpError
Failed:TcpTimeout
Failed:ConnectionFunctionError
Failed:ConnectionFunctionDenied
Failed:Internal
Failed:UnmappedConnectionError
```

Cuando las conexiones producen un error, CloudFront registra códigos de motivo específicos:

Código	Descripción
ClientCertMaxChainDepthExceeded	Se ha superado la profundidad máxima de la cadena de certificados
ClientCertMaxSizeExceeded	Se ha superado el tamaño máximo de certificado
ClientCertUntrusted	El certificado no es de confianza
ClientCertNotYetValid	El certificado aún no es válido
ClientCertExpired	El certificado ha caducado

Código	Descripción
ClientCertTypeUnsupported	El tipo de certificado de cliente no es compatible
ClientCertInvalid	El certificado no es válido
ClientCertIntentInvalid	La finalidad del certificado no es válida
ClientCertRejected	Se ha rechazado el certificado mediante validación personali zada
ClientCertMissing	Certificado faltante
TcpError	Se ha producido un error al intentar establecer conexión
TcpTimeout	No se pudo establecer la conexión dentro del periodo de espera
ConnectionFunctionError	Se produjo una excepción no detectada durante la ejecución de la función de conexión
Interna	Se ha producido un error de servicio interno
UnmappedConnectionError	Se ha producido un error que no pertenece a ninguna de las otras categorías

TLS mutua (origen) con CloudFront

La autenticación TLS mutua (Autenticación de seguridad de la capa de transporte mutua: mTLS) es un protocolo de seguridad que amplía la autenticación TLS estándar al requerir una autenticación bidireccional basada en certificados, en la que tanto el cliente como el servidor deben demostrar su identidad antes de establecer una conexión segura.

mTLS de espectador frente a mTLS de origen

La autenticación mutua (mTLS) se puede habilitar entre los espectadores y la distribución de CloudFront (mTLS de espectador) o también entre la distribución de CloudFront y el origen (mTLS de origen). Esta documentación se refiere a la configuración de mTLS de origen. Para la configuración de mTLS del espectador consulte: Autenticación TLS mutua con CloudFront (mTLS de espectador).

TLS mutua (origen) permite a CloudFront autenticarse en los servidores de origen mediante certificados de cliente. Con TLS mutua (origen), puede asegurarse de que solo las distribuciones autorizadas de CloudFront puedan establecer conexiones con los servidores de aplicaciones, lo que ayuda a protegerse contra los intentos de acceso no autorizados.

> **Note**
>
> En las conexiones TLS (origen) mutuas, CloudFront actúa como cliente y presenta su certificado de cliente al servidor de origen durante el establecimiento de comunicación de TLS. CloudFront no valida el certificado del cliente ni el estado de revocación, esto es responsabilidad del servidor de origen. La infraestructura de origen debe estar configurada para validar el certificado de cliente con respecto al almacén de confianza, comprobar la caducidad del certificado y realizar comprobaciones de revocación (como la validación de CRL u OCSP) de acuerdo con los requisitos de seguridad. El rol de CloudFront se limita a presentar el certificado; los servidores de origen aplican toda la lógica de validación de certificados y las políticas de seguridad.

Funcionamiento

En un establecimiento de comunicación de TLS estándar entre CloudFront y un origen, solo el servidor de origen presenta un certificado que demuestre su identidad a CloudFront. Con TLS mutua (origen), el proceso de autenticación pasa a ser bidireccional. Cuando CloudFront intenta conectarse al servidor de origen, CloudFront presenta un certificado de cliente durante el establecimiento de comunicación de TLS. El servidor de origen valida este certificado con su almacén de confianza antes de establecer la conexión segura.

Casos de uso

TLS mutua (origen) aborda varios escenarios de seguridad críticos en los que los métodos de autenticación tradicionales crean una sobrecarga operativa:

- Seguridad híbrida y multinube: puede proteger las conexiones entre CloudFront y los orígenes alojados fuera de AWS o los orígenes públicos en AWS. Esto elimina la necesidad de administrar las listas de direcciones IP permitidas o las soluciones de encabezados personalizadas, lo que proporciona una autenticación coherente basada en certificados en AWS, los centros de datos en las instalaciones y proveedores de terceros. Las empresas de medios de comunicación, los

minoristas y las empresas que operan infraestructuras distribuidas se benefician de los controles de seguridad estandarizados en toda su infraestructura.

- API de B2B y seguridad de backend: puede proteger las API y microservicios de backend de los intentos de acceso directo y, al mismo tiempo, conservar los beneficios de rendimiento de CloudFront. Las plataformas SaaS, los sistemas de procesamiento de pagos y las aplicaciones empresariales con requisitos de autenticación estrictos pueden comprobar que las solicitudes de API se originan solo en distribuciones de CloudFront autorizadas, lo que evita los ataques de intermediarios y los intentos de acceso no autorizados.

Importante: requisitos del servidor de origen

TLS mutua (origen) requiere que los servidores de origen estén configurados para admitir la autenticación TLS mutua. Su infraestructura de origen debe ser capaz de:

- Solicitar y validar los certificados de los clientes durante los establecimientos de comunicación de TLS.
- Mantener un almacén de confianza con los certificados de la autoridad de certificación que emitió los certificados de cliente de CloudFront.
- Registrar y supervisar los eventos de conexión TLS mutua.
- Administrar las políticas de validación de certificados y gestionar los errores de autenticación.

CloudFront se encarga de la presentación de los certificados del cliente, pero los servidores de origen son responsables de validar estos certificados y administrar la conexión TLS mutua. Asegúrese de que la infraestructura de origen esté configurada correctamente antes de habilitar TLS mutua (origen) en CloudFront.

Introducción

Para implementar TLS mutua (origen) con CloudFront, tendrá que importar el certificado de cliente en AWS Certificate Manager, configurar el servidor de origen para que requiera TLS mutua y habilitar TLS mutua (origen) en la distribución de CloudFront. En las siguientes secciones, se proporcionan instrucciones paso a paso para cada tarea de configuración.

Temas

- Administración de certificados con AWS Certificate Manager
- Habilitación de TLS mutua (origen) para las distribuciones de CloudFront

- Uso de CloudFront Functions con TLS mutua (origen)

Administración de certificados con AWS Certificate Manager

AWS Certificate Manager (ACM) almacena los certificados de cliente que CloudFront presenta a los servidores de origen durante la autenticación de TLS mutua (origen).

Compatibilidad de la autoridad de certificación

CloudFront Mutual TLS (origen) requiere certificados de cliente con uso ampliado de claves (EKU) para la autenticación de clientes de TLS. Debido a este requisito, debe emitir los certificados de la autoridad de certificación e importarlos a AWS Certificate Manager. Las características automáticas de aprovisionamiento y renovación de certificados de ACM no están disponibles para los certificados de cliente de TLS mutuas (de origen). CloudFront Mutual TLS (origen) admite certificados de cliente de dos orígenes:

- Autoridad de certificación privada de AWS: puede emitir certificados desde una autoridad de certificación privada de AWS mediante plantillas de certificados que incluyan la autenticación de cliente de TLS en el campo Uso ampliado de claves (como la plantilla EndEntityClientAuthCertificate). Después de emitir el certificado de la autoridad de certificación privada de AWS, debe importarla en ACM en la región Este de EE. UU. (Norte de Virginia) (us-east-1). Este enfoque proporciona los beneficios de seguridad de autoridad de certificación privada de AWS y, al mismo tiempo, permite controlar la administración del ciclo de vida de los certificados.
- Autoridades de certificación privada de terceros: también puede emitir certificados desde su infraestructura de autoridad de certificación privada existente e importarlos a ACM. Esto permite mantener los procesos actuales de administración de certificados y, al mismo tiempo, aprovechar las capacidades de TLS mutuo (origen) de CloudFront. Los certificados deben incluir la autenticación de cliente de TLS en el campo Uso ampliado de claves y deben estar en formato PEM con el certificado, la clave privada y la cadena de certificados.

> **Important**
>
> Tanto para las autoridades de certificación privadas de AWS como para las de terceros, es responsable de supervisar las fechas de caducidad de los certificados e importar los certificados renovados a ACM antes de que caduquen. La característica de renovación

automática de ACM no se aplica a los certificados importados que se utilizan para TLS mutua (origen).

Requisitos y especificaciones de certificados

Requisitos del certificado de cliente

- Formato: formato PEM (Correo con privacidad mejorada)
- Componentes: certificado, clave privada y cadena de certificado
- Profundidad máxima de la cadena de certificados: 3 (certificado de hoja + certificado intermedio + certificado raíz)
- Tamaño máximo de la cadena de certificados: 64 KB
- Tamaño del certificado: no puede superar los 96 KB
- Tamaño máximo de clave privada: 5 KB (restricción de ACM)
- Número máximo de ARN de certificados mTLS de origen único que se pueden agregar o modificar por cada llamada a la API de creación o actualización de distribución de CloudFront: 5
- Región: los certificados se deben almacenar en ACM en la región Este de EE. UU. (Norte de Virginia) (us-east-1)

Especificaciones de certificados compatibles

- Tipo de certificado: X.509v3
- Algoritmos de clave pública:
  - RSA: 2048 bits
  - ECDSA: P-256
- Algoritmos de firma:
  - SHA256, SHA384, SHA512 con RSA
  - SHA256, SHA384, SHA512 con ECDSA
  - SHA256, SHA384, SHA512 con RSASSA-PSS con MGF1
- Uso ampliado de claves (obligatorio): el certificado requiere la extensión del uso ampliado de claves (EKU) configurada como autenticación de cliente de TLS, lo que garantiza que está autorizado para fines de mTLS

Requisitos del certificado del servidor

Los servidores de origen deben presentar certificados de autoridades de certificación de confianza pública durante el establecimiento de comunicación de TLS mutua. Para obtener detalles completos sobre los requisitos del certificado del servidor de origen, consulte Requisitos para usar certificados SSL/TLS con CloudFront.

Solicitud o importación de un certificado

Antes de habilitar TLS mutua (origen), debe tener un certificado de cliente disponible en ACM.

Solicitud e importación de un certificado de la autoridad de certificación privada de AWS

Requisitos previos:

- Una autoridad de certificación privada de AWS configurada en la cuenta
- Permiso para emitir certificados de la autoridad de certificación privada de AWS
- Permiso para importar certificados en ACM
- Un ARN de plantilla de certificado con `Extended key usage:TLS web client authentication` que se adapta al caso de uso
- Instale OpenSSL, AWS CLI y jq (para analizar JSON).

Solicitud de un certificado de PCA e importación en ACM (AWS CLI)

1. Configure el ARN de la autoridad de certificación privada en una variable para facilitar su reutilización.

```
PCA_ARN="arn:aws:acm-pca:region:account:certificate-authority/12345678..."
```

2. Utilice OpenSSL para generar una clave privada ECDSA P-256 (curva prime256v1) y una solicitud de firma de certificado (CSR), lo que garantiza que el indicador -nodes se utilice para mantener la clave privada sin cifrar, tal como se requiere para la importación de ACM.

```
openssl req -new -newkey ec -pkeyopt ec_paramgen_curve:prime256v1 -nodes \
    -keyout private.key \
    -out request.csr \
    -subj "/CN=client.example.com"
```

3. Envíe CSR a la autoridad de certificación privada de AWS para emitir un certificado, que devuelva el ARN del certificado recién emitido.

```
CERT_ARN=$(aws acm-pca issue-certificate \
    --certificate-authority-arn "$PCA_ARN" \
    --csr fileb://request.csr \
    --signing-algorithm "SHA256WITHECDSA" \
    --validity Value=365,Type="DAYS" \
    --template-arn arn:aws:acm-pca:::template/EndEntityCertificate/V1 \
    --query 'CertificateArn' --output text)
```

4. Recupere el paquete de certificados de AWS PCA mediante el comando get-certificate, que devuelve el certificado de hoja y la cadena. A continuación, utilice jq para separarlos en archivos distintos.

```
# Retrieve the full certificate bundle in JSON format
aws acm-pca get-certificate \
    --certificate-authority-arn "$PCA_ARN" \
    --certificate-arn "$CERT_ARN" \
    --output json > full_cert.json

# Split into Leaf and Chain
jq -r '.Certificate' full_cert.json > leaf_cert.pem
jq -r '.CertificateChain' full_cert.json > cert_chain.pem
```

5. Importe la clave privada no cifrada, el certificado de hoja y la cadena de certificados a AWS ACM mediante el protocolo fileb:// para gestionar correctamente los datos de los archivos binarios en la CLI.

```
aws acm import-certificate \
    --certificate fileb://leaf_cert.pem \
    --private-key fileb://private.key \
    --certificate-chain fileb://cert_chain.pem \
    --region us-east-1 \
    --query 'CertificateArn' \
    --output text
```

Importación de un certificado de una autoridad de certificación de terceros

Requisitos previos:

- Un certificado, una clave privada no cifrada y la cadena de certificados de la autoridad de certificación en formato PEM

- El certificado debe incluir el uso ampliado de claves para la autenticación del cliente de TLS
- Permisos para importar certificados en ACM

Importación de un certificado en ACM (AWS CLI)

```
aws acm import-certificate \
  --certificate fileb://certificate.pem \
  --private-key fileb://private-key.pem \
  --certificate-chain fileb://certificate-chain.pem \
  --region us-east-1 \
  --query 'CertificateArn' \
  --output text
```

Siguientes pasos

Tras obtener o importar el certificado de cliente en ACM, puede configurar el servidor de origen para que requiera la autenticación de TLS mutua y habilite TLS mutua (origen) en la distribución de CloudFront. Para obtener instrucciones sobre cómo habilitar TLS mutua (origen) en CloudFront, consulte la siguiente sección “Habilitar TLS mutua (origen) para las distribuciones de CloudFront”.

Habilitación de TLS mutua (origen) para las distribuciones de CloudFront

Tras obtener un certificado de cliente a través de AWS Certificate Manager y configurar el servidor de origen para requerir TLS mutua, puede habilitar TLS mutua (origen) en la distribución de CloudFront.

Requisitos previos y requisitos

Antes de habilitar TLS mutua (origen) en una distribución de CloudFront, asegúrese de que dispone de:

- Un certificado de cliente almacenado en AWS Certificate Manager en la región Este de EE. UU. (Norte de Virginia) (us-east-1).
- Servidores de origen configurados para requerir la autenticación de TLS mutua y validar los certificados de los clientes.
- Servidores de origen que presentan certificados de autoridades de certificación de confianza pública.
- Permisos para modificar las distribuciones de CloudFront.
- TLS mutua (origen) solo está disponible en los planes Business, Premium o planes de precio de pago por uso.

> **Note**
>
> TLS mutua (origen) se puede configurar para orígenes personalizados (incluidos los orígenes alojados fuera de AWS) y orígenes de AWS que admiten TLS mutua, como Equilibrador de carga de aplicación y API Gateway.

> **Important**
>
> Las siguientes características de CloudFront no son compatibles con TLS mutua (origen):
>
> - Tráfico de gRPC: el protocolo de gRPC no es compatible con los orígenes con TLS mutua (origen) habilitado.
> - Conexiones WebSocket: el protocolo WebSocket no es compatible con orígenes con TLS mutua (origen) habilitado.
> - Orígenes de VPC: TLS mutua (origen) no se puede usar con orígenes de VPC.
> - Desencadenadores de solicitud de origen y respuesta de origen con Lambda@Edge: las funciones de Lambda@Edge en las posiciones de solicitud de origen y respuesta de origen no se admiten con TLS mutua (origen).
> - POP incrustados: TLS mutua (origen) no es compatible con POP incrustados.

Habilitación de TLS mutua (origen)

La configuración por origen permite especificar distintos certificados de cliente para distintos orígenes dentro de la misma distribución. Este enfoque proporciona la máxima flexibilidad cuando los orígenes tienen diferentes requisitos de autenticación.

Para distribuciones nuevas (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Crear distribución.
3. Seleccione un plan de precios: elija Business o Premium o Pago por uso (TLS mutua (origen) no está disponible en el plan gratuito)
4. En la sección de configuración de origen, elija Tipo de origen como otro.
5. En la sección Configuración de origen, elija Personalizar configuración de origen.

6. Configure el primer origen (nombre de dominio, protocolo, etc.).
7. En la configuración de origen, busque TLS mutua (origen).
8. Active la opción Habilitar TLS mutua (origen).
9. Para Certificado de cliente, seleccione el certificado de AWS Certificate Manager.
10. (Opcional) Agregue orígenes adicionales con sus propias configuraciones de TLS mutua (origen).
11. Complete el resto de la configuración de distribución y elija Crear distribución.

Para distribuciones existentes (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En la lista de distribución, seleccione la distribución que desee modificar. (Nota: Asegúrese de que la distribución esté en un plan de precios Pro o Premium o Pago por uso. De lo contrario, debe actualizar el plan de precios antes de habilitar TLS mutua [origen]).
3. Elija la pestaña Orígenes.
4. Seleccione el origen que quiere configurar y elija Editar.
5. En la configuración de origen, encuentre TLS mutua (origen).
6. Active la opción Habilitar TLS mutua (origen).
7. Para Certificado de cliente, seleccione el certificado de AWS Certificate Manager. (Nota: Solo se mostrarán los certificados de cliente con la propiedad EKU (Uso ampliado de claves) establecida en “Autenticación de cliente de TLS”)
8. Elija Guardar cambios.
9. Repetición de orígenes adicionales según sea necesario

Uso de la CLI de AWS

Para la configuración por origen, especifique los ajustes de TLS mutua (origen) dentro de la configuración de cada origen:

```
{
  "Origins": {
    "Quantity": 2,
    "Items": [
```

```
      {
        "Id": "origin-1",
        "DomainName": "api.example.com",
        "CustomOriginConfig": {
          "HTTPSPort": 443,
          "OriginProtocolPolicy": "https-only"
        },
        "OriginMtlsConfig": {
          "ClientCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
cert-1"
        }
      },
      {
        "Id": "origin-2",
        "DomainName": "backend.example.com",
        "CustomOriginConfig": {
          "HTTPSPort": 443,
          "OriginProtocolPolicy": "https-only"
        },
        "OriginMtlsConfig": {
          "CertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/cert-2"
        }
      }
    ]
  }
}
```

> **Note**
>
> CloudFront no proporcionará el certificado de cliente si el servidor no lo solicita, lo que permitirá que la conexión continúe con normalidad.

Siguientes pasos

Tras habilitar TLS mutua (origen) en la distribución de CloudFront, puede supervisar los eventos de autenticación mediante los registros de acceso de CloudFront.

Uso de CloudFront Functions con TLS mutua (origen)

CloudFront Functions proporciona computación periférica ligera y sin servidor para personalizar la entrega de contenido. Cuando se utiliza TLS mutua (origen) con CloudFront Functions, hay

comportamientos y limitaciones específicos que hay que tener en cuenta en relación con la selección y la manipulación del origen.

Operaciones de CloudFront Functions admitidas

Las CloudFront Functions pueden interactuar con orígenes habilitados de TLS mutua (origen) de las siguientes maneras:

updateRequestOrigin()

La función updateRequestOrigin() admite modificaciones limitadas cuando se trabaja con orígenes habilitados de TLS mutua (origen):

- Cambiar entre orígenes de TLS mutua (origen): puede actualizar la solicitud para que se dirija a un origen diferente que utilice TLS mutua (origen), siempre que ambos orígenes utilicen el mismo certificado de cliente. Esto permite implementar una lógica de enrutamiento personalizada y, al mismo tiempo, mantener la autenticación de TLS mutua.
- Desactivación de TLS mutua (origen): puede cambiar de un origen habilitado de TLS mutua (origen) a un origen de TLS no mutua configurando `mTLSConfig: 'off'` en la función. Esto proporciona flexibilidad para desactivar condicionalmente la autenticación de TLS mutua en función de las características de la solicitud.

Ejemplo: Cambio entre orígenes de TLS mutua (origen) con el mismo certificado

```
function handler(event) {
    var request = event.request;

    // Route to different origin based on request path
    if (request.uri.startsWith('/api/v2')) {
        request.origin = {
            domainName: 'api-v2.example.com',
            customHeaders: {},
            // Both origins must use the same certificate
        };
    }

    return request;
}
```

Ejemplo: Desactivación condicional de TLS mutua (origen)

```
function handler(event) {
    var request = event.request;

    // Disable mTLS for specific paths
    if (request.uri.startsWith('/public')) {
        request.origin = {
            domainName: 'public-origin.example.com',
            customHeaders: {},
            mTLSConfig: 'off'
        };
    }

    return request;
}
```

Operaciones de CloudFront Functions no admitidas

Las siguientes operaciones de CloudFront Functions no admiten orígenes habilitados de TLS mutua (origen) en condiciones de disponibilidad general:

selectRequestOriginById()

La función `selectRequestOriginById()` no puede seleccionar un origen que tenga habilitado TLS mutua (origen). Si se intenta seleccionar un origen habilitado de TLS mutua (origen) mediante esta función, se producirá un error de validación.

Si su caso de uso requiere una selección de origen dinámica con TLS mutua (origen), utilice `updateRequestOrigin()` en su lugar, asegurándose de que todos los orígenes de destino utilicen el mismo certificado de cliente.

createRequestOriginGroup()

La función `createRequestOriginGroup()` no admite la creación de grupos de orígenes que incluyan orígenes habilitados de TLS mutua (origen). Los grupos de origen con orígenes de TLS mutua (origen) no se pueden crear dinámicamente mediante CloudFront Functions.

Si necesita capacidades de conmutación por error de origen con TLS mutua (origen), configure los grupos de origen directamente en la configuración de distribución de CloudFront, en lugar de crearlos de forma dinámica en funciones.

Distribución de contenido privado con URL firmadas y cookies firmadas

Muchas empresas que distribuyen contenido a través de Internet desean restringir el acceso a documentos, información corporativa, transmisiones multimedia o contenido destinado a una selección de usuarios; por ejemplo, a los usuarios que hayan pagado una determinada tarifa. Para ofrecer este contenido privado de forma segura a través de CloudFront, puede hacer lo siguiente:

- Solicite que los usuarios accedan al contenido privado mediante URL firmadas o cookies firmadas especiales de CloudFront.
- Solicite que los usuarios accedan al contenido a través de URL de CloudFront, no URL que accedan al contenido directamente en el servidor de origen (por ejemplo, Amazon S3 o un servidor HTTP privado). No es necesario solicitar URL de CloudFront, pero lo recomendamos para impedir que los usuarios eludan las restricciones que especifique en URL firmadas o cookies firmadas.

Para obtener más información, consulte Restricción del acceso a archivos.

Distribución de contenido privado

Para configurar CloudFront para que distribuya contenido privado, realice las siguientes tareas:

1. Solicite a los usuarios que accedan al contenido solo a través de CloudFront (opcional pero recomendado). El método que utilice depende de si utiliza Amazon S3 u orígenes personalizados:

   - Amazon S3: consulte the section called “Restricción del acceso a un origen de Amazon S3”.
   - Origen personalizado: consulte Restricción del acceso a archivos en orígenes personalizados.

   Los orígenes personalizados incluyen Amazon EC2, buckets de Amazon S3 configurados como puntos de enlace del sitio web, Elastic Load Balancing y sus propios servidores web HTTP.
2. Especifique los grupos de claves de confianza o los signatarios de confianza que desea utilizar para crear URL firmadas o cookies firmadas. Le recomendamos que utilice grupos de claves de confianza. Para obtener más información, consulte Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas.

3. Escriba la aplicación para responder a las solicitudes de los usuarios autorizados con URL firmadas o con encabezados `Set-Cookie` que establezcan cookies firmadas. Siga los pasos en uno de los siguientes temas:

   - Uso de URL firmadas
   - Uso de cookies firmadas

   Si no está seguro de qué método utilizar, consulte Decisión de utilizar URL firmadas o cookies firmadas.

Temas

- Restricción del acceso a archivos
- Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas
- Decisión de utilizar URL firmadas o cookies firmadas
- Uso de URL firmadas
- Uso de cookies firmadas
- Comandos de Linux y OpenSSL para codificación y cifrado base64
- Ejemplos de código para la creación de una firma para una URL firmada

Restricción del acceso a archivos

Puede controlar el acceso de los usuarios al contenido privado de dos maneras:

- Restringir el acceso a los archivos en las cachés de CloudFront.
- Restrinja el acceso a los archivos en su origen de la siguiente manera:
  - Configure un control de acceso de origen (OAC) para su bucket de Amazon S.
  - Configure encabezados personalizados para un servidor HTTP privado (un origen personalizado).

Restricción del acceso a archivos en las cachés de CloudFront

Puede configurar CloudFront para que solicite que los usuarios accedan a los archivos mediante URL firmadas o cookies firmadas. Después, deberá desarrollar la aplicación para crear y distribuir URL firmadas para los usuarios autenticados o para enviar encabezados `Set-Cookie` que

establecen cookies firmadas para usuarios autenticados. (También puede crear URL firmadas manualmente para ofrecer a unos pocos usuarios acceso largo plazo a un número reducido de archivos).

Si crea URL o cookies firmadas para controlar el acceso a sus archivos, puede especificar las siguientes restricciones:

- La fecha y la hora de finalización, a partir de la cual la URL deja de ser válida.
- La fecha y la hora a la que la URL pasa a ser válida (opcional).
- La dirección IP o a un rango de direcciones IP de los equipos desde los que se puede obtener acceso a su contenido.

A una parte de una URL firmada o una cookie firmada se le aplica el algoritmo hash y se firma con la clave privada de un par de claves públicas-privadas. Cuando alguien utiliza una URL firmada o una cookie firmada para acceder a un archivo, CloudFront compara las partes firmadas y sin firmar de la URL o de la cookie. Si no coinciden, CloudFront no envía el archivo.

Debe utilizar claves privadas RSA 2048 o ECDSA 256 para firmar URL o cookies.

Restricción del acceso a archivos en buckets de Amazon S3

Si lo desea, puede proteger el contenido de su bucket de Amazon S3 para que los usuarios puedan acceder a él a través de la distribución de CloudFront especificada, pero no puedan acceder directamente mediante las URL de Amazon S3. Esto evita que se eluda CloudFront y se use la URL de Amazon S3 para obtener el contenido cuyo acceso desea restringir. Este paso no es necesario para utilizar URL firmadas, pero recomendamos seguirlo.

Para solicitar que los usuarios accedan al contenido a través de URL de CloudFront, realice las siguientes tareas:

- Conceder un permiso de control de acceso de origen de CloudFront para leer los archivos del bucket de S3.
- Crear el control de acceso de origen y asociarlo con su distribución de CloudFront.
- Quite a todos los demás el permiso para usar URL de Amazon S3 para leer los archivos.

Para obtener más información, consulte the section called “Restricción del acceso a un origen de Amazon S3”.

Restricción del acceso a archivos en orígenes personalizados

Si utiliza un origen personalizado, tiene la opción de configurar encabezados personalizados para restringir el acceso. Para que CloudFront obtenga los archivos de un origen personalizado, debe ser posible el acceso de CloudFront a los archivos mediante una solicitud HTTP estándar (o HTTPS). Sin embargo, mediante el uso de encabezados personalizados, puede restringir aún más el acceso al contenido para que los usuarios puedan acceder al mismo solo a través de CloudFront, no directamente. Este paso no es necesario para utilizar URL firmadas, pero recomendamos seguirlo.

Para solicitar que los usuarios accedan al contenido a través de CloudFront, cambie la siguiente configuración de las distribuciones de CloudFront:

Encabezados personalizados de origen

Configure CloudFront para reenviar encabezados personalizados al origen. Consulte Configuración de CloudFront para agregar encabezados personalizados a solicitudes de origen.

Viewer Protocol Policy

Configure la distribución para solicitar a los lectores que utilicen HTTPS para acceder a CloudFront. Consulte Política de protocolo para lectores.

Origin Protocol Policy

Configure la distribución para solicitar a CloudFront que utilice el mismo protocolo que los lectores para reenviar solicitudes al origen. Consulte Protocolo (solo orígenes personalizados).

Después de haber realizado estos cambios, actualice la aplicación en el origen personalizado para aceptar solo solicitudes que incluyan los encabezados personalizados que ha configurado para que CloudFront los envíe.

La combinación de Viewer Protocol Policy (Política de protocolo del lector) y Origin Protocol Policy (Política de protocolo de origen) garantiza que los encabezados personalizados se cifren en tránsito. Sin embargo, le recomendamos realizar periódicamente las siguientes acciones para rotar los encabezados personalizados que CloudFront reenvía al origen:

1. Actualice la distribución de CloudFront para comenzar a reenviar un nuevo encabezado al origen personalizado.
2. Actualice la aplicación para aceptar el nuevo encabezado a modo de confirmación de que la solicitud proviene de CloudFront.

3. Cuando las solicitudes ya no incluyan el encabezado que ha reemplazado, actualice la aplicación para que ya no acepte el encabezado anterior a modo de confirmación de que la solicitud proviene de CloudFront.

Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas

Temas

- Elección entre grupos de claves de confianza (recomendado) y Cuentas de AWS
- Creación de pares de claves para los firmantes
- Volver a formatear la clave privada (solo .NET y Java)
- Agregación de un firmante a una distribución
- Rotación de pares de claves

Para crear URL firmadas o cookies firmadas, necesita un signatario. Un signatario es un grupo de claves de confianza que se crea en CloudFront o una cuenta de AWS que contiene un par de claves de CloudFront. Le recomendamos que utilice grupos de claves de confianza con URL firmadas y cookies firmadas. Para obtener más información, consulte Elección entre grupos de claves de confianza (recomendado) y Cuentas de AWS.

El signatario tiene dos fines:

- Tan pronto como agregue el signatario a la distribución, CloudFront comienza a requerir que los lectores utilicen URL firmadas o cookies firmadas para acceder a los archivos.
- Al crear URL firmadas o cookies firmadas, se utiliza la clave privada del par de claves del signatario para firmar una parte de la URL o la cookie. Cuando alguien solicita un archivo restringido, CloudFront compara la firma de la URL o la cookie con la URL o la cookie sin firmar, para verificar que no se ha manipulado. CloudFront también verifica que la URL o la cookie sean válidas, es decir, por ejemplo, que la fecha y la hora de vencimiento no han pasado todavía.

Cuando se especifica un signatario, también se especifican indirectamente los archivos que requieren URL firmadas o cookies firmadas al agregar el signatario a un comportamiento de la caché. Si la distribución solo dispone de un comportamiento de la caché, los lectores deben utilizar URL o cookies firmadas para acceder a cualquier archivo de la distribución. Si crea varios comportamientos

de la caché y agrega signatarios a algunos de ellos pero no a otros, puede exigir que los lectores utilicen URL o cookies firmadas para acceder a algunos archivos y no a otros.

Para especificar los signatarios (las claves privadas) autorizados para crear URL firmadas o cookies firmadas y para agregar los signatarios a la distribución de CloudFront, realice las siguientes tareas:

1. Decida si desea utilizar un grupo de claves de confianza o una Cuenta de AWS como firmante. Recomendamos utilizar un grupo de claves de confianza. Para obtener más información, consulte Elección entre grupos de claves de confianza (recomendado) y Cuentas de AWS.
2. Para el signatario que eligió en el paso 1, cree un par de claves privadas-públicas. Para obtener más información, consulte Creación de pares de claves para los firmantes.
3. Si utiliza .NET o Java para crear URL firmadas o cookies firmadas, vuelva a formatear la clave privada. Para obtener más información, consulte Volver a formatear la clave privada (solo .NET y Java).
4. En la distribución para la que va a crear URL firmadas o cookies firmadas, especifique el signatario. Para obtener más información, consulte Agregación de un firmante a una distribución.

Elección entre grupos de claves de confianza (recomendado) y Cuentas de AWS

Para utilizar URL firmadas o cookies firmadas, necesita un signatario. Un firmante es un grupo de claves de confianza que se crea en CloudFront o una Cuenta de AWS que contiene un par de claves de CloudFront. Se recomienda utilizar grupos de claves de confianza, por los siguientes motivos:

- Con los grupos de claves de CloudFront no es necesario usar el usuario raíz de la cuenta de AWS para administrar las claves públicas de las URL firmadas y las cookies firmadas de CloudFront. Las prácticas recomendadas de AWS indican no utilizar el usuario raíz cuando no es necesario.
- Con los grupos de claves de CloudFront, puede administrar claves públicas, grupos de claves y signatarios de confianza mediante la API de CloudFront. Puede usar la API para automatizar la creación de claves y la rotación de claves. Cuando se utiliza el usuario raíz de AWS, se debe utilizar la Consola de administración de AWS para administrar pares de claves de CloudFront, de modo que no se puede automatizar el proceso.
- Dado que puede administrar grupos de claves con la API de CloudFront, también puede utilizar las políticas de permisos de AWS Identity and Access Management (IAM) para limitar lo que los distintos usuarios pueden hacer. Por ejemplo, puede permitir a los usuarios cargar claves públicas, pero no eliminarlas. También puede permitir que los usuarios eliminen claves públicas, pero solo cuando se cumplen ciertas condiciones, como el uso de la autenticación multifactor, el envío de

la solicitud desde una red determinada o el envío de la solicitud dentro de un intervalo de fecha y hora determinado.

- Con los grupos de claves de CloudFront, puede asociar un número mayor de claves públicas con la distribución de CloudFront, lo que le concede más flexibilidad en la forma de usar y administrar las claves públicas. De forma predeterminada, puede asociar hasta cuatro grupos de claves con una sola distribución y puede tener hasta cinco claves públicas en un grupo de claves.

  Cuando utiliza el usuario raíz de la cuenta de AWS para administrar pares de claves de CloudFront, solo puede tener hasta dos pares de claves activos de CloudFront por cuenta de AWS.

Creación de pares de claves para los firmantes

Cada signatario que utilice para crear URL firmadas o cookies firmadas de CloudFront debe tener un par de claves públicas-privadas. El signatario utiliza la clave privada para firmar la URL o las cookies y CloudFront utiliza la clave pública para comprobar la firma.

La forma en que se crea un par de claves depende de si se utiliza un grupo de claves de confianza como el signatario (recomendado) o un par de claves de CloudFront. Para obtener más información, consulte las siguientes secciones. El par de claves que cree debe cumplir los siguientes requisitos:

- Debe ser un par de claves SSH-2 RSA 2048 o ECDSA 256.
- Debe encontrarse en formato PEM codificado en Base64.

Para ayudar a proteger las aplicaciones, le recomendamos que cambie los pares de claves periódicamente. Para obtener más información, consulte Rotación de pares de claves.

Crear un par de claves para un grupo de claves de confianza (recomendado)

Para crear un par de claves para un grupo de claves de confianza, realice los siguientes pasos:

1. Cree el par de claves públicas-privadas.
2. Cargue la clave pública en CloudFront.
3. Agregue la clave pública a un grupo de claves de CloudFront.

Para obtener más información, consulte los siguientes procedimientos.

Para crear un par de claves

> **Note**
>
> En los siguientes pasos se utiliza OpenSSL como ejemplo de un método para crear un par de claves. Hay muchas otras formas de crear un par de claves RSA o ECDSA.

1. Ejecute uno de los siguientes comandos de ejemplo:

   - El siguiente comando de ejemplo utiliza OpenSSL para generar un par de claves RSA con una longitud de 2048 bits y guardarlo en el archivo denominado `private_key.pem`.

     ```
     openssl genrsa -out private_key.pem 2048
     ```

   - El siguiente comando de ejemplo utiliza OpenSSL para generar un par de claves ECDSA con la curva `prime256v1` y guárdelo en el archivo denominado `private_key.pem`.

     ```
     openssl ecparam -name prime256v1 -genkey -noout -out privatekey.pem
     ```

2. El archivo resultante contiene tanto la clave pública como la privada. El siguiente comando de ejemplo extrae la clave pública del archivo denominado `private_key.pem`.

   ```
   openssl rsa -pubout -in private_key.pem -out public_key.pem
   ```

   Se carga la clave pública (en el archivo `public_key.pem`) más adelante, en el siguiente procedimiento.

Para cargar la clave pública en CloudFront

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el menú de navegación, elija Claves públicas.
3. Elija Crear clave pública.
4. En la ventana Crear clave pública, haga lo siguiente:

a. En Key name (Nombre de la clave), escriba un nombre para identificar la clave pública.

b. En Key value (Valor de clave), pegue la clave pública. Si ha seguido los pasos del procedimiento anterior, la clave pública se encuentra en el archivo denominado `public_key.pem`. Para copiar y pegar el contenido de la clave pública, puede:

   - Use el comando cat en la línea de comandos de macOS o Linux, así:

     ```
     cat public_key.pem
     ```

     Copie el resultado de ese comando y péguelo en el campo Key value (Valor de clave).

   - Abra el archivo `public_key.pem` con un editor de texto sin formato como el Bloc de notas (en Windows) o TextEdit (en macOS). Copie el contenido del archivo y péguelo en el campo Key value (Valor de clave).

c. (Opcional) En Comment (Comentario), agregue un comentario para describir la clave pública.

Cuando haya terminado, elija Add (Agregar).

5. Registre el ID de la clave pública. Lo usará más adelante cuando cree URL firmadas o cookies firmadas, como valor del campo `Key-Pair-Id`.

Para agregar la clave pública a un grupo de claves

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el menú de navegación, elija Grupos de claves.
3. Elija Add key group (Agregar grupo de claves).
4. En la página Create key group (Crear grupo de claves), haga lo siguiente:

   a. En Key group name (Nombre del grupo de claves), escriba un nombre para identificar el grupo de claves.

   b. (Opcional) En Comment (Comentario), escriba un comentario para describir el grupo de claves.

   c. En Public keys (Claves públicas), seleccione la clave pública que desea agregar al grupo de claves y, a continuación, elija Add (Agregar). Repita este paso para cada clave pública que desee agregar al grupo de claves.

5. Elija Create key group (Crear grupo de claves).
6. Registre el nombre del grupo de claves. Se utiliza más adelante para asociar el grupo de claves con un comportamiento de la caché en una distribución de CloudFront. (En la API de CloudFront, se utiliza el ID del grupo de claves para asociar el grupo de claves con un comportamiento de la caché).

Creación de un par de claves de CloudFront (no recomendado, se requiere el usuario raíz de la Cuenta de AWS)

> **Important**
>
> Se recomienda crear una clave pública para un grupo de claves de confianza en lugar de seguir estos pasos. Para obtener información sobre la forma recomendada de crear claves públicas para URL firmadas y cookies firmadas, consulte Crear un par de claves para un grupo de claves de confianza (recomendado).

Puede crear un par de claves de CloudFront de las siguientes maneras:

- Crear un par de claves en la Consola de administración de AWS y descargar la clave privada. Consulte el procedimiento siguiente.
- Cree un par de claves RSA usando una aplicación como OpenSSL y, a continuación, cargue la clave pública en la Consola de administración de AWS. Para obtener más información acerca de la creación de un par de claves RSA, consulte Crear un par de claves para un grupo de claves de confianza (recomendado).

Para crear pares de claves de CloudFront en la Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS con las credenciales del usuario raíz de la cuenta de AWS.

   > **Important**
   >
   > Los usuarios de IAM no pueden crear pares de claves de CloudFront. Debe iniciar sesión con credenciales de usuario raíz para crear pares de claves.

2. Elija el nombre de la cuenta y, a continuación, elija My Security Credentials (Mis credenciales de seguridad).
3. Elija CloudFront key pairs (Pares de claves de CloudFront).
4. Confirme que no tiene más de un par de claves activas. No se puede crear un par de claves si ya dispone de dos pares de claves activos.
5. Elija Create New Key Pair (Crear un nuevo par de claves).

> **Note**
>
> También puede elegir crear su propio par de claves y cargar la clave pública. Los pares de claves de CloudFront admiten claves de 1024, 2048 o 4096 bits.

6. En el cuadro de diálogo Create Key Pair (Crear par de claves), elija Download Private Key File (Descargar archivo de claves privadas) y, a continuación, guarde el archivo en el equipo.

> **Important**
>
> Guarde la clave privada del par de claves de CloudFront en un lugar seguro y establezca permisos en el archivo para que solo los administradores que usted decida puedan leerlo. Si alguien obtiene su clave privada, puede generar URL y cookies firmadas válidas y descargar su contenido. No podrá obtener la clave privada de nuevo, por lo que si la pierde o la elimina, deberá crear un nuevo par de claves de CloudFront.

7. Registre el ID de su par de claves. (En la Consola de administración de AWS, esto se denomina Access Key ID [ID de clave de acceso]). Lo utilizará al crear URL firmadas o cookies firmadas.

Volver a formatear la clave privada (solo .NET y Java)

Si utiliza .NET o Java para crear URL firmadas o cookies firmadas, no puede utilizar la clave privada del par de claves en el formato PEM predeterminado para crear la firma. En su lugar, haga lo siguiente:

- .NET framework: convierte la clave privada en el formato XML que utiliza .NET Framework. Hay varias herramientas disponibles.
- Java: convierte la clave privada en formato DER. Una forma de hacerlo es con el siguiente comando de OpenSSL. En el siguiente comando, `private_key.pem` es el nombre del archivo

que contiene la clave privada con formato PEM y `private_key.der` es el nombre del archivo que contiene la clave privada con formato DER después de ejecutar el comando.

```
openssl pkcs8 -topk8 -nocrypt -in private_key.pem -inform PEM -out private_key.der -
outform DER
```

Para asegurarse de que el codificador funciona correctamente, agregue el recurso JAR de la API de criptografía Java Bouncy Castle a su proyecto y, a continuación, agregue el proveedor Bouncy Castle.

Agregación de un firmante a una distribución

Un signatario es el grupo de claves de confianza (recomendado) o el par de claves de CloudFront que puede crear URL firmadas y cookies firmadas para una distribución. Para utilizar URL firmadas o cookies firmadas con una distribución de CloudFront, debe especificar un signatario.

Los signatarios se asocian con comportamientos de la caché. Esto le permite exigir URL firmadas o cookies firmadas para algunos archivos y no para otros dentro de la misma distribución. Una distribución requiere URL o cookies firmadas solo para los archivos asociados con los comportamientos de la caché correspondientes.

Del mismo modo, un signatario solo puede firmar URL o cookies para archivos asociados con los comportamientos de la caché correspondientes. Por ejemplo, si tiene un signatario para un comportamiento de la caché y un signatario diferente para un comportamiento de la caché diferente, ninguno de los dos signatarios puede crear URL o cookies firmadas para los archivos asociados con el otro comportamiento de la caché.

> **Important**
>
> Antes de agregar un signatario a la distribución, haga lo siguiente:
>
> - Defina cuidadosamente los patrones de ruta y la secuencia de los comportamientos de la caché para no conceder a los usuarios acceso no deseado al contenido o impedir que accedan al contenido que desea que esté disponible para todos.
>
> Supongamos que una solicitud coincide con el patrón de ruta de dos comportamientos de la caché. El primer comportamiento de la caché no requiere URL firmadas ni cookies firmadas y el segundo comportamiento de la caché sí. Los usuarios podrán acceder a los

archivos sin usar URL ni cookies firmadas porque CloudFront procesa el comportamiento de la caché que está asociado con la primera coincidencia.

Para obtener más información acerca de patones de rutas, consulte Patrón de ruta.

- Para una distribución que ya utiliza para distribuir contenido, asegúrese de que está listo para comenzar a generar URL firmadas y cookies firmadas antes de agregar un signatario. Cuando se agrega un signatario, CloudFront rechaza las solicitudes que no incluyen una URL firmada o una cookie firmada válidas.

Puede agregar signatarios a la distribución utilizando la consola de CloudFront o la API de CloudFront.

Console

En los siguientes pasos se muestra cómo agregar un grupo de claves de confianza como signatario. También puede agregar una Cuenta de AWS como firmante de confianza, pero no es recomendable hacerlo.

Para agregar un signatario a una distribución mediante la consola

1. Registre el ID del grupo de claves del grupo de claves que desea utilizar como signatario de confianza. Para obtener más información, consulte Crear un par de claves para un grupo de claves de confianza (recomendado).
2. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
3. Elija la distribución cuyos archivos desea proteger con URL firmadas o cookies firmadas.

   > **Note**
   >
   > Para agregar un signatario a una distribución nueva, se especifica la misma configuración que se describe en el paso 6 al crear la distribución.

4. Elija la pestaña Behaviors (Comportamientos).
5. Seleccione el comportamiento de caché cuyo patrón de ruta coincida con los archivos que desea proteger con URL firmadas o cookies firmadas y, a continuación, elija Edit (Editar).
6. En la página Edit Behavior (Editar comportamiento), haga lo siguiente:

   a. En Restrict Viewer Access (Use Signed URLs or Signed Cookies) (Restringir el acceso a lectores [mediante URL o cookies firmadas]), elija Yes (Sí).
   b. En Trusted Key Groups or Trusted Signer (Grupos de claves de confianza o signatario de confianza), elija Trusted Key Groups (Grupos de claves de confianza).
   c. En Trusted Key Groups (Grupos de claves de confianza), elija el grupo de claves que desea agregar y, a continuación, elija Add (Agregar). Repita el procedimiento si desea agregar más de un grupo de claves.
7. Elija Yes, Edit (Sí, Editar) para actualizar el comportamiento de la caché.

API

Puede usar la API de CloudFront para agregar un grupo de claves de confianza como signatario. Puede agregar un signatario a una distribución existente o a una distribución nueva. En cualquier caso, deberá especificar los valores en el elemento `TrustedKeyGroups`.

También puede agregar una Cuenta de AWS como firmante de confianza, pero no es recomendable hacerlo.

Consulte los siguientes temas en la Referencia de la API de Amazon CloudFront:

- Actualizar una distribución existente: UpdateDistribution
- Crear una nueva distribución: CreateDistribution

Rotación de pares de claves

Se recomienda rotar periódicamente (cambiar) los pares de claves para las URL firmadas y las cookies firmadas. Para rotar pares de claves que utiliza para crear URL firmadas o cookies firmadas sin invalidar las URL o cookies que no hayan vencido todavía, realice las siguientes tareas:

1. Cree un nuevo par de claves y agregue la clave pública a un grupo de claves. Para obtener más información, consulte Crear un par de claves para un grupo de claves de confianza (recomendado).
2. Si ha creado un nuevo grupo de claves en el paso anterior, agregue el grupo de claves a la distribución como signatario.

> **Important**
>
> No elimine ninguna clave pública existente del grupo de claves ni ningún grupo de claves de la distribución todavía. Solo agregue los nuevos.

3. Actualice la aplicación para crear firmas con la clave privada del nuevo par de claves. Confirme que las URL firmadas o las cookies firmadas con las nuevas claves privadas funcionan.
4. Espere hasta que pase la fecha de vencimiento de las URL o las cookies firmadas con la clave privada anterior. A continuación, elimine la clave pública anterior del grupo de claves. Si ha creado un nuevo grupo de claves en el paso 2, elimine el grupo de claves anterior de la distribución.

Decisión de utilizar URL firmadas o cookies firmadas

Las URL firmadas y las cookies firmadas de CloudFront proporcionan la misma funcionalidad básica: le permiten controlar quién puede obtener acceso al contenido. Si desea distribuir contenido privado a través de CloudFront e intenta decidir si utilizar URL firmadas o cookies firmadas, tenga en cuenta lo siguiente.

Utilice URL firmadas en los casos siguientes:

- Si desea restringir el acceso a archivos individuales, por ejemplo, una descarga de instalación para su aplicación.
- Si sus usuarios utilizan un cliente (por ejemplo, un cliente HTTP personalizado) que no admite cookies.

Utilice cookies firmadas en los casos siguientes:

- Si desea proporcionar acceso a varios archivos restringidos (por ejemplo, a todos los archivos de un vídeo en formato HLS o a todos los archivos del área de suscriptores de un sitio web).
- Si no quiere cambiar las URL actuales.

Si en la actualidad no utiliza URL firmadas y si sus URL (sin firmar) contienen cualquiera de los siguientes parámetros de cadenas de consulta, no puede utilizar cookies firmadas ni URL firmadas:

- `Expires`
- `Policy`

- `Signature`
- `Key-Pair-Id`

CloudFront asume que las URL que contienen cualquiera de los parámetros de cadenas de consulta son URL firmadas y, por lo tanto, no examina las cookies firmadas.

Uso de URL firmadas y cookies firmadas

Las URL firmadas tienen prioridad sobre las cookies firmadas. Si utiliza URL firmadas y cookies firmadas para controlar el acceso a los mismos archivos y un lector utiliza una URL firmada para solicitar un archivo, CloudFront determina si debe devolver el objeto al lector basándose únicamente en la URL firmada.

Uso de URL firmadas

Una URL firmada incluye información adicional, por ejemplo, una fecha y hora de vencimiento, lo que permite un mayor control sobre el acceso a su contenido. Esta información adicional aparece en una instrucción de política basada en una política predefinida o personalizada. Las diferencias entre las políticas personalizadas y las predefinidas se explican en las próximas dos secciones.

> **Note**
>
> Puede crear algunas URL firmadas con políticas predefinidas y crear otras con políticas personalizadas para la misma distribución.

Temas

- Decisión de utilizar políticas predefinidas o personalizadas para URL firmadas
- Cómo funcionan las URL firmadas
- Decisión del tiempo de validez de las URL firmadas
- Cuándo comprueba CloudFront la fecha y hora de vencimiento de una URL firmada
- Código de ejemplo y herramientas de terceros
- Creación de una URL firmada mediante una política predefinida
- Creación de una URL firmada mediante una política personalizada

Decisión de utilizar políticas predefinidas o personalizadas para URL firmadas

Al crear una URL firmada, se escribe una instrucción de política en formato JSON que especifica las restricciones en la URL firmada, por ejemplo, el tiempo de validez de la URL. Puede utilizar una política predefinida o personalizada. A continuación, se presenta una comparación entre las políticas predefinidas y las personalizadas:

Descripción	Política predefinida	Política personalizada
Puede reutilizar la instrucción de la política con varios archivos. Para reutilizar la instrucción de política, debe utilizar caracteres comodín en el objeto `Resource`. Para obtener más información, consulte Valores que se especifican en la instrucción de política de una URL firmada que utiliza una política personalizada).	No	Sí
Puede especificar la fecha y la hora a la que los usuarios pueden empezar a obtener acceso a su contenido.	No	Sí (opcional)
Puede especificar la fecha y la hora a la que los usuarios dejan de obtener acceso a su contenido.	Sí	Sí
Puede especificar la dirección IP o a un rango de direcciones IP de los usuarios que pueden obtener acceso a su contenido.	No	Sí (opcional)
La URL firmada incluye una versión de la política con codificación de tipo base64, lo que resulta en una URL más larga.	No	Sí

Para obtener información acerca de cómo crear URL firmadas mediante una política predefinida, consulte Creación de una URL firmada mediante una política predefinida.

Para obtener información acerca de cómo crear URL firmadas mediante una política personalizada, consulte Creación de una URL firmada mediante una política personalizada.

Cómo funcionan las URL firmadas

A continuación, se muestra información general de cómo se configura CloudFront y Amazon S3 para URL firmadas y cómo responde CloudFront cuando un usuario utiliza una URL firmada para solicitar un archivo.

1. En la distribución de CloudFront, especifique uno o más grupos de claves de confianza, que contienen las claves públicas que CloudFront puede utilizar para comprobar la firma de URL. Se utilizan las claves privadas correspondientes para firmar las URL.

   CloudFront admite direcciones URL firmadas con firmas de claves RSA 2048 y ECDSA 256.

   Para obtener más información, consulte Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas.
2. Desarrolle la aplicación para determinar si un usuario debe tener acceso al contenido y crear URL firmadas para los archivos o partes de la aplicación a las que desea restringir el acceso. Para obtener más información, consulte los siguientes temas:

   - Creación de una URL firmada mediante una política predefinida
   - Creación de una URL firmada mediante una política personalizada
3. Un usuario solicita un archivo que va a requerir URL firmadas.
4. La aplicación verifica si el usuario tiene derecho para obtener acceso al archivo: si ha iniciado sesión, si ha pagado por obtener acceso al contenido o si ha cumplido algún otro requisito para obtener acceso.
5. Su aplicación crea una URL firmada y la devuelve el usuario.
6. Las URL firmadas permiten al usuario descargar o transmitir el contenido.

   Este paso es automático; el usuario normalmente no tiene que hacer nada más para obtener acceso al contenido. Por ejemplo, si un usuario accede a su contenido desde un navegador web, la aplicación devuelve la URL firmada al navegador. El navegador utiliza inmediatamente la URL firmada para acceder al archivo de la caché de borde de CloudFront sin necesidad de que el usuario intervenga.
7. CloudFront utiliza la clave pública para validar la firma y confirmar que la URL no se ha manipulado. Si la firma no es válida, se rechaza la solicitud.

   Si la firma es válida, CloudFront examina la instrucción de la política en la URL (o crea una si utiliza una política predefinida) para confirmar que la solicitud sigue siendo válida. Por ejemplo,

si especifica una fecha y hora de inicio y fin de la URL, CloudFront confirma que el usuario intenta acceder al contenido durante el periodo que usted ha decidido permitir dicho acceso.

Si la solicitud cumple los requisitos de la instrucción de política, CloudFront realiza las operaciones estándar: determina si el archivo ya está en la caché de borde, reenvía la solicitud al origen en caso necesario y devuelve el archivo al usuario.

> **Note**
>
> Si una URL sin firmar contiene parámetros de cadena de consulta, asegúrese de incluirlos en la parte de la dirección URL que firma. Si agrega una cadena de consulta a una URL firmada después de firmarla, la URL devuelve un estado HTTP 403.

Decisión del tiempo de validez de las URL firmadas

Puede distribuir contenido privado mediante una URL firmada cuyo periodo de validez sea corto, incluso de unos pocos minutos. Las URL firmadas con un tiempo de validez tan corto son adecuadas para distribuir contenido sobre la marcha a un usuario con una finalidad específica, como la distribución de películas de alquiler o descargas de música bajo demanda para clientes. Si el periodo de validez de las URL firmadas es corto, es recomendable generarlas automáticamente con una aplicación que puede desarrollar. Cuando el usuario comienza a descargar un archivo o a reproducir un archivo multimedia, CloudFront compara la fecha y hora de vencimiento de la URL con el momento actual para determinar si la URL todavía es válida.

También puede distribuir contenido privado mediante una URL firmada con un periodo de validez más largo, de incluso años. Las URL válidas durante periodos largos resultan útiles para distribuir contenido privado a usuarios conocidos, como, por ejemplo, la distribución de un plan de negocio a inversores o la distribución de materiales de formación a los empleados. Puede desarrollar una aplicación para generar estas URL firmadas a largo plazo para usted.

Cuándo comprueba CloudFront la fecha y hora de vencimiento de una URL firmada

CloudFront comprueba la fecha y hora de vencimiento de una URL firmada al realizarse la solicitud HTTP. Si un cliente comienza a descargar un archivo grande inmediatamente antes de la fecha de vencimiento, la descarga se realizará por completo incluso si se sobrepasa la hora de vencimiento durante la descarga. Si la conexión TCP se interrumpe y el cliente intenta reiniciar la descarga después de la fecha de vencimiento, la descarga fallará.

Si un cliente utiliza rangos GET para obtener un archivo en partes más pequeñas, cualquier solicitud GET que se produzca después de la fecha de vencimiento no se procesará. Para obtener más información acerca de Range GET, consulte Cómo CloudFront procesa las solicitudes parciales de un objeto (rango GET).

Código de ejemplo y herramientas de terceros

Para ver un código de ejemplo que crea la parte de las URL firmadas y a la que se le haya aplicado una función hash, consulte los siguientes temas:

- Crear una firma de URL con Perl
- Crear una firma de URL con PHP
- Crear una firma de URL mediante C# y .NET Framework
- Crear una firma de URL con Java

Creación de una URL firmada mediante una política predefinida

Para crear una URL firmada mediante una política predefinida, complete los pasos siguientes.

Para crear una URL firmada mediante una política predefinida

1. Si utiliza. NET o Java para crear URL firmadas y no ha reformateado la clave privada del par de claves del formato .pem predeterminado a un formato compatible con .NET o con Java, hágalo ahora. Para obtener más información, consulte Volver a formatear la clave privada (solo .NET y Java).
2. Concatene los siguientes valores. Puede utilizar el formato de este ejemplo de URL firmada.

```
https://d111111abcdef8.cloudfront.net/
image.jpg?color=red&size=medium&Expires=1767290400&Signature=nitfHRCrtziwO2HwPfWw~yYDhUF5Ew
j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-
Pair-Id=K2JCJMDEHXQW5F
```

   Elimine todos los espacios vacíos (incluidos tabuladores y caracteres de línea nueva). Es posible que tenga que incluir caracteres de escape en la cadena del código de la aplicación. Todos los valores tienen un tipo de `String`.

1. ***URL base del archivo***

   La URL base es la URL de CloudFront que utilizaría para acceder al archivo si no utilizara las URL firmadas, incluidos los parámetros de la cadena de consulta propios, si los hay. En el ejemplo anterior, la URL base es `https://d111111abcdef8.cloudfront.net/image.jpg`. Para obtener más información acerca del formato de las URL para distribuciones, consulte Personalización del formato de URL para archivos en CloudFront.

   - La siguiente URL de CloudFront es para un archivo de imagen en una distribución (utilizando el nombre de dominio de CloudFront). `image.jpg` está en un directorio `images`. La ruta hacia el archivo de la URL debe coincidir con la ruta hacia el archivo del servidor HTTP o del bucket de Amazon S3.

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

   - La siguiente URL de CloudFront incluye una cadena de consulta:

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

   - Las siguientes URL de CloudFront corresponden a archivos de imagen de una distribución. Ambas usan un nombre de dominio alternativo. La segunda incluye una cadena de consulta:

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

     ```
     https://www.example.com/images/image.jpg?color=red
     ```

   - La siguiente URL de CloudFront corresponde a un archivo de imagen de una distribución que utiliza un nombre de dominio alternativo y el protocolo HTTPS:

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

2. **?**

   ? indica que los parámetros de consulta siguen la URL base. Incluya el parámetro ? par si no especifica ningún otro parámetro de consulta.

   > **Note**
   >
   > Puede especificar los siguientes parámetros de consulta en cualquier orden.

3. ***Sus parámetros de cadena de consulta, de haberlos*&**

   (Opcional) Puede introducir sus propios parámetros de la cadena de consulta. Para ello, agregue un signo y (`&`) entre cada uno de ellos; por ejemplo, `color=red&size=medium`. Puede especificar los parámetros de consulta en cualquier orden dentro de la URL.

   > **Important**
   >
   > Los parámetros de la cadena de consulta no podrán llamarse `Expires`, `Signature` ni `Key-Pair-Id`.

4. **`Expires=`*fecha y hora en formato de tiempo Unix (en segundos), en hora universal coordinada (UTC)***

   La fecha y la hora en las que desea que la URL deje de permitir el acceso al archivo.

   Especifique la fecha y la hora de vencimiento en formato de tiempo Unix (en segundos) y hora universal coordinada (UTC). Por ejemplo, 1 de enero de 2026 a las 10:00 UTC pasa a ser `1767290400` en formato de tiempo Unix, como se muestra en el ejemplo al principio de este tema.

   Para utilizar el tiempo de época, especifique un número entero de 64 bits para una fecha que no sea posterior a `9223372036854775807` (viernes, 11 de abril de 2262 a las 23:47:16.854 UTC).

   Para obtener información acerca de UTC, consulte RFC 3339, fecha y hora en Internet: marcas temporales.

5. **`&Signature=`*versión firmada y a la que se le ha aplicado una función hash de la instrucción de política***

   Una versión firmada, a la que se le ha aplicado una función hash y codificada en base64 de la instrucción de política JSON. Para obtener más información, consulte Creación de una firma para una URL firmada que utiliza una política predefinida.

6. **`&Key-Pair-Id=`*`ID de clave pública para la clave pública de CloudFront cuya clave privada correspondiente va a utilizar para generar la firma`***

   El ID de una clave pública de CloudFront, por ejemplo, `K2JCJMDEHXQW5F`. El ID de clave pública indica a CloudFront qué clave pública usar para validar la URL firmada. CloudFront compara la información de la firma con la información de la instrucción de política para comprobar que la URL no se ha manipulado.

   Esta clave pública debe pertenecer a un grupo de claves que tiene un signatario de confianza en la distribución. Para obtener más información, consulte Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas.

Creación de una firma para una URL firmada que utiliza una política predefinida

Para crear la firma para una URL firmada que utilice una política predefinida, realice los procedimientos indicados a continuación.

Temas

- Creación de una instrucción de política para una URL firmada que utiliza una política predefinida
- Creación de una firma para una URL firmada que utiliza una política predefinida

Creación de una instrucción de política para una URL firmada que utiliza una política predefinida

Al crear una URL firmada mediante una política predefinida, el parámetro `Signature` es una versión firmada y a la que se le ha aplicado una función hash de una instrucción de política. En el caso de URL firmadas que utilizan una política predefinida, la instrucción de política no se incluye en la URL, a diferencia de las URL firmadas que utilizan una política personalizada. Para crear la instrucción de política, siga el procedimiento que se indica a continuación.

Para crear una instrucción de política para una URL firmada que use una política predefinida

1. Cree la instrucción de política utilizando el siguiente formato JSON y codificación de caracteres UTF-8. Incluya toda la puntuación y otros valores literalmente, tal como se especifica. Para obtener más información acerca de los parámetros `Resource` y `DateLessThan`, consulte Valores que se especifican en la instrucción de política de una URL firmada que utiliza una política predefinida.

   ```
   {
   ```

```
    "Statement": [
        {
            "Resource": "base URL or stream name",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": ending date and time in Unix time format and
 UTC
                }
            }
        }
    ]
}
```

2. Elimine todos los espacios vacíos (incluidos tabuladores y caracteres de línea nueva) de la instrucción de la política. Es posible que tenga que incluir caracteres de escape en la cadena del código de la aplicación.

Valores que se especifican en la instrucción de política de una URL firmada que utiliza una política predefinida

Al crear una instrucción de política para una política predefinida, debe especificar los siguientes valores.

Recurso

> **Note**
>
> Puede especificar solo un valor en `Resource`.

La URL base incluye las cadenas de consulta, de haberlas, pero excluye los parámetros de CloudFront `Expires`, `Signature` y `Key-Pair-Id`, por ejemplo:

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

Tenga en cuenta lo siguiente:

- Protocol (Protocolo): el valor debe comenzar con `http://` o `https://`.
- Query string parameters (Parámetros de cadena de consulta): si no tiene parámetros de cadena de consulta, omita el signo de interrogación.

- Alternate domain names (Nombres de dominio alternativos): si especifica un nombre de dominio alternativo (CNAME) en la URL, debe especificarlo al hacer referencia al archivo en la página web o aplicación. No especifique la URL de Amazon S3 del objeto.

DateLessThan

La fecha y hora de vencimiento de la URL en formato de tiempo Unix (en segundos) y hora universal coordinada (UTC). Por ejemplo, 1 de enero de 2026 a las 10:00 UTC pasa a ser 1767290400 en formato de tiempo Unix.

Este valor debe coincidir con el valor del parámetro de cadena de consulta `Expires` de la URL firmada. No incluya el valor entre comillas.

Para obtener más información, consulte Cuándo comprueba CloudFront la fecha y hora de vencimiento de una URL firmada.

Ejemplo de instrucción de política para una URL firmada que utiliza una política predefinida

Cuando se utiliza la siguiente instrucción de política de ejemplo en una URL firmada, un usuario puede acceder al archivo `https://d111111abcdef8.cloudfront.net/horizon.jpg` hasta el 1 de enero de 2026 a las 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Creación de una firma para una URL firmada que utiliza una política predefinida

Para crear el valor del parámetro `Signature` en una URL firmada, aplique una función hash y firme la instrucción de política que ha creado en Creación de una instrucción de política para una URL firmada que utiliza una política predefinida.

Para obtener más información y ejemplos de cómo resumir, aplicar una función hash y codificar la instrucción de política, consulte:

- Comandos de Linux y OpenSSL para codificación y cifrado base64
- Ejemplos de código para la creación de una firma para una URL firmada

Opción 1: para crear una firma mediante una política predefinida

1. Use la función hash SHA-1 y la clave privada RSA o ECDSA generada para codificar y firmar la instrucción de política creada en el procedimiento Para crear una instrucción de política para una URL firmada que use una política predefinida. Utilice la versión de la instrucción de política que ya no incluye espacios vacíos.

   Para la clave privada requerida por la función hash, utilice una clave privada cuya clave pública esté en un grupo de claves de confianza activo para la distribución.

   > **Note**
   >
   > El método que utilice para resumir y aplicar una función hash la instrucción de política depende de su lenguaje de programación y plataforma. Para ver código de muestra, consulte Ejemplos de código para la creación de una firma para una URL firmada.

2. Elimine los espacios vacíos (incluidos tabuladores y caracteres de línea nueva) de la cadena a la que se le ha aplicado una función hash y firmada.
3. Codifique la cadena con codificación base64 de MIME. Para obtener más información, consulte la Section 6.8, Base64 Content-Transfer-Encoding de RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Sustituya caracteres no válidos en una cadena de consulta de URL por caracteres válidos. En la siguiente tabla se muestran los caracteres válidos y no válidos.

Sustituya los caracteres no válidos	Por estos caracteres válidos
+	- (guion)
=	_ (guion bajo)
/	~ (tilde)

5. Añada el valor resultante a la URL firmada después de `&Signature=` y vuelva a Para crear una URL firmada mediante una política predefinida para terminar de encadenar las partes de la URL firmada.

Creación de una URL firmada mediante una política personalizada

Para crear una URL firmada mediante una política personalizada, realice el procedimiento que se indica a continuación.

Para crear una URL firmada mediante una política personalizada

1. Si utiliza. NET o Java para crear URL firmadas y no ha reformateado la clave privada del par de claves del formato .pem predeterminado a un formato compatible con .NET o con Java, hágalo ahora. Para obtener más información, consulte Volver a formatear la clave privada (solo .NET y Java).
2. Concatene los siguientes valores. Puede utilizar el formato de este ejemplo de URL firmada.

```
https://d111111abcdef8.cloudfront.net/
image.jpg?color=red&size=medium&Policy=eyANCiAgICEXAMPLEW1lbnQiOiBbeyANCiAgICAgICJSZXNvdXJj
j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-
Pair-Id=K2JCJMDEHXQW5F
```

Elimine todos los espacios vacíos (incluidos tabuladores y caracteres de línea nueva). Es posible que tenga que incluir caracteres de escape en la cadena del código de la aplicación. Todos los valores tienen un tipo de `String`.

1. ***URL base del archivo***

   La URL base es la URL de CloudFront que utilizaría para acceder al archivo si no utilizara las URL firmadas, incluidos los parámetros de la cadena de consulta propios, si los hay. En el ejemplo anterior, la URL base es `https://d111111abcdef8.cloudfront.net/image.jpg`. Para obtener más información acerca del formato de las URL para distribuciones, consulte Personalización del formato de URL para archivos en CloudFront.

   Los siguientes ejemplos muestran valores que especifica para distribuciones.

   - La siguiente URL de CloudFront es para un archivo de imagen en una distribución (utilizando el nombre de dominio de CloudFront). `image.jpg` está en un directorio

`images`. La ruta hacia el archivo de la URL debe coincidir con la ruta hacia el archivo del servidor HTTP o del bucket de Amazon S3.

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

- La siguiente URL de CloudFront incluye una cadena de consulta:

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

- Las siguientes URL de CloudFront corresponden a archivos de imagen de una distribución. Ambas utilizan un nombre de dominio alternativo; la segunda incluye una cadena de consulta:

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

```
https://www.example.com/images/image.jpg?color=red
```

- La siguiente URL de CloudFront corresponde a un archivo de imagen de una distribución que utiliza un nombre de dominio alternativo y el protocolo HTTPS:

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

2. **?**

? indica que los parámetros de la cadena de consulta siguen a la URL base. Incluya el parámetro ? par si no especifica ningún otro parámetro de consulta.

> **Note**
>
> Puede especificar los siguientes parámetros de consulta en cualquier orden.

3. ***Sus parámetros de cadena de consulta, de haberlos*&**

(Opcional) Puede introducir sus propios parámetros de la cadena de consulta. Para ello, agregue un signo y (&) entre cada uno de ellos; por ejemplo, `color=red&size=medium`. Puede especificar los parámetros de consulta en cualquier orden dentro de la URL.

> **Important**
>
> Los parámetros de la cadena de consulta no podrán llamarse `Policy`, `Signature` ni `Key-Pair-Id`.

Si añade sus propios parámetros, incluya un & después de cada uno, incluso después del último.

4. **`Policy=`*`versión codificada con base64 de la instrucción de política`***

   La instrucción de política en formato JSON después de haber eliminado los espacios vacíos y, a continuación, codificada con base64. Para obtener más información, consulte Creación de una instrucción de política para una URL firmada que utiliza una política personalizada.

   La instrucción de política controla el acceso que una URL firmada concede a un usuario. Incluye la URL del archivo, una fecha y hora de vencimiento, una fecha y hora opcionales en que la URL se convierte en válida y una dirección IP opcional o un intervalo de direcciones IP a las que se permite acceder al archivo.

5. **`&Signature=`*`versión firmada y a la que se le ha aplicado una función hash de la instrucción de política`***

   Una versión firmada, a la que se le ha aplicado una función hash y codificada en base64 de la instrucción de política JSON. Para obtener más información, consulte Creación de una firma para una URL firmada que utiliza una política personalizada.

6. **`&Key-Pair-Id=`*`ID de clave pública para la clave pública de CloudFront cuya clave privada correspondiente va a utilizar para generar la firma`***

   El ID de una clave pública de CloudFront, por ejemplo, `K2JCJMDEHXQW5F`. El ID de clave pública indica a CloudFront qué clave pública usar para validar la URL firmada. CloudFront compara la información de la firma con la información de la instrucción de política para comprobar que la URL no se ha manipulado.

   Esta clave pública debe pertenecer a un grupo de claves que tiene un signatario de confianza en la distribución. Para obtener más información, consulte Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas.

Creación de una instrucción de política para una URL firmada que utiliza una política personalizada

Complete los siguientes pasos para crear una instrucción de política para una URL firmada que utiliza una política personalizada.

Para consultar instrucciones de políticas de ejemplo que controlan el acceso a archivos de distintas maneras, consulte the section called “Instrucciones de políticas de ejemplo para una URL firmada que utiliza una política personalizada”.

Para crear una instrucción de política para una URL firmada que use una política personalizada

1. Cree la instrucción de política en el siguiente formato JSON. Sustituya los símbolos menor que (<) y mayor que (>) y las descripciones que contienen, por sus propios valores. Para obtener más información, consulte the section called “Valores que se especifican en la instrucción de política de una URL firmada que utiliza una política personalizada”.

```
{
    "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>"
                }
            }
        }
    ]
}
```

Tenga en cuenta lo siguiente:

- Puede incluir solo una instrucción en la política.
- Utilice la codificación de caracteres UTF-8.
- Incluya toda la puntuación y los nombres de parámetros exactamente como se especifica. No se aceptan abreviaturas de nombres de parámetros.
- El orden de los parámetros de la sección `Condition` no importa.

- Para obtener información acerca de valores para `Resource`, `DateLessThan`, `DateGreaterThan` y `IpAddress`, consulte the section called "Valores que se especifican en la instrucción de política de una URL firmada que utiliza una política personalizada".

2. Elimine todos los espacios vacíos (incluidos tabuladores y caracteres de línea nueva) de la instrucción de la política. Es posible que tenga que incluir caracteres de escape en la cadena del código de la aplicación.
3. Codifique la instrucción de política con codificación base64 de MIME. Para obtener más información, consulte la Section 6.8, Base64 Content-Transfer-Encoding de RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Sustituya caracteres no válidos en una cadena de consulta de URL por caracteres válidos. En la siguiente tabla se muestran los caracteres válidos y no válidos.

Sustituya los caracteres no válidos	Por estos caracteres válidos
+	- (guion)
=	_ (guion bajo)
/	~ (tilde)

5. Añada el valor resultante a la URL firmada después de `Policy=`.
6. Cree una firma para la URL firmada aplicando una función hash, firmando y codificando con base64 la instrucción de política. Para obtener más información, consulte the section called "Creación de una firma para una URL firmada que utiliza una política personalizada".

Valores que se especifican en la instrucción de política de una URL firmada que utiliza una política personalizada

Al crear una instrucción de política para una política personalizada, debe especificar los siguientes valores.

Resource

La URL, incluidas las cadenas de consulta, pero excluyendo los parámetros de CloudFront `Policy`, `Signature` y `Key-Pair-Id`. Por ejemplo:

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg\?
size=large&license=yes
```

Puede especificar solo un valor de URL para `Resource`.

> **Important**
>
> Puede omitir el parámetro `Resource` en una política, pero hacerlo significa que cualquiera con la URL firmada puede acceder a todos los archivos en cualquier distribución asociada con el par de claves que utiliza para crear la URL firmada.

Tenga en cuenta lo siguiente:

- Protocolo: el valor debe comenzar con `http://`, `https://` o `*://`.
- Parámetros de cadena de consulta: si la URL tiene parámetros de cadena de consulta, no utilice una barra oblicua inversa (\) para evitar el signo de interrogación (?) que comienza la cadena de consulta. Por ejemplo:

  ```
  https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
  size=large&license=yes
  ```

- Caracteres comodín: puede utilizar caracteres comodín en la URL de la política. Se admiten los siguientes caracteres comodín:
  - asterisco (*), que busca coincidencias con cero o más caracteres
  - el signo de interrogación de cierre (?), que busca coincidencias exactamente con un carácter

  Cuando CloudFront hace coincidir la URL de la política con la URL de la solicitud HTTP, la URL de la política se divide en cuatro secciones (protocolo, dominio, ruta y cadena de consulta) de la siguiente manera:

  ```
  [protocol]://[domain]/[path]\?[query string]
  ```

  Al utilizar un carácter comodín en la URL de la política, la coincidencia de caracteres comodín solo se aplica dentro de los límites de la sección que contiene el comodín. Por ejemplo, considere esta URL en una política:

  ```
  https://www.example.com/hello*world
  ```

  En este ejemplo, el comodín asterisco (*) solo se aplica a la sección de rutas, por lo que coincide con las URL `https://www.example.com/helloworld` y `https://www.example.com/hello-world`, pero no con la URL `https://www.example.net/hello?world`.

Las siguientes excepciones se aplican a los límites de las secciones para la coincidencia de caracteres comodín:

- Un asterisco al final de la sección de rutas implica un asterisco en la sección de cadenas de consulta. Por ejemplo, `http://example.com/hello*` equivale a `http://example.com/hello*\?*`.
- Un asterisco al final de la sección de dominio implica un asterisco en la secciones de ruta y cadena de consulta. Por ejemplo, `http://example.com*` equivale a `http://example.com*/*\?*`.
- Una URL en la política puede omitir la sección de protocolo y empezar con un asterisco en la sección de dominio. En ese caso, la sección de protocolo se establece implícitamente en un asterisco. Por ejemplo, la URL `*example.com` en una política es equivalente a `*://*example.com/`.
- Un asterisco por sí solo (`"Resource": "*"`) coincide con cualquier URL.

Por ejemplo, el valor: `https://d111111abcdef8.cloudfront.net/*game_download.zip*` en una política coincide con todas las URL siguientes:

- `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`

- Nombres de dominio alternativos: si especifica un nombre de dominio alternativo (CNAME) en la URL de la política, la solicitud HTTP debe usar el nombre de dominio alternativo en la página web o aplicación. No especifique la URL de Amazon S3 para el archivo en una política.

DateLessThan

La fecha y hora de vencimiento de la URL en formato de tiempo Unix (en segundos) y hora universal coordinada (UTC). En la política, no incluya el valor entre comillas. Para obtener información acerca de UTC, consulte Fecha y hora en Internet: marcas temporales.

Por ejemplo, el 31 de enero de 2023 a las 10:00 UTC pasa a ser 1675159200 en formato de tiempo Unix.

Este es el único parámetro requerido en la sección `Condition`. CloudFront requiere este valor para impedir que los usuarios tengan acceso permanente al contenido privado.

Para obtener más información, consulte the section called “Cuándo comprueba CloudFront la fecha y hora de vencimiento de una URL firmada”

DateGreaterThan (opcional)

Una fecha y hora de inicio opcionales de la URL en formato de tiempo Unix (en segundos) y hora universal coordinada (UTC). Los usuarios no pueden acceder al archivo en la fecha y hora especificadas ni antes. No incluya el valor entre comillas.

IpAddress (opcional)

La dirección IP del cliente que hace la solicitud HTTP. Tenga en cuenta lo siguiente:

- Para permitir que cualquier dirección IP obtenga acceso al archivo, omita el parámetro `IpAddress`.
- Puede especificar una dirección IP o a un rango de direcciones IP. No puede usar la política para permitir el acceso si la dirección IP del cliente está en uno de dos rangos separados.
- Para permitir el acceso desde una única dirección IP, especifique:

  `"Dirección IP IPv/32"`
- Debe especificar rangos de direcciones IP en formato estándar IPv4 CIDR (por ejemplo, `192.0.2.0/24`). Para obtener más información, consulte Enrutamiento entre dominios sin clases (CIDR): Asignación de dirección de Internet y plan de agregación.

> **Important**
>
> Las direcciones IP en formato IPv6, como 2001:0db8:85a3::8a2e:0370:7334, no son compatibles.

Si está utilizando una política personalizada que incluya `IpAddress`, no habilite IPv6 para la distribución. Si desea restringir el acceso a algún contenido por dirección IP y admite solicitudes IPv6 de otro contenido, puede crear dos distribuciones. Para obtener más información, consulte the section called “Habilitación de IPv6 (solicitudes de espectadores)” en el tema the section called “Toda la configuración de distribución”.

Instrucciones de políticas de ejemplo para una URL firmada que utiliza una política personalizada

En los siguientes ejemplos de instrucciones de políticas, se muestra cómo controlar el acceso a un archivo específico, a todos los archivos de un directorio o a todos los archivos asociados a un ID

de par de claves. Los ejemplos también muestran cómo controlar el acceso desde una dirección IP individual o a un rango de direcciones IP, y cómo impedir que los usuarios utilicen la URL firmada después de una fecha y hora específicas.

Si copia y pega cualquiera de estos ejemplos, elimine los espacios vacíos (incluidos los tabuladores y los caracteres de línea nueva), sustituya los valores por sus propios valores e incluya un carácter de línea nueva después de la llave de cierre (`}`).

Para obtener más información, consulte the section called “Valores que se especifican en la instrucción de política de una URL firmada que utiliza una política personalizada”.

Temas

- Ejemplo de instrucción de política: acceso a un archivo desde un intervalo de direcciones IP
- Ejemplo de instrucción de política: acceso a todos los archivos de un directorio desde un intervalo de direcciones IP
- Ejemplo de instrucción de política: acceso a todos los archivos asociados con un ID de par de claves desde una dirección IP

Ejemplo de instrucción de política: acceso a un archivo desde un intervalo de direcciones IP

En el siguiente ejemplo de política personalizada de una URL firmada se especifica que un usuario puede acceder al archivo `https://d111111abcdef8.cloudfront.net/game_download.zip` desde las direcciones IP del intervalo `192.0.2.0/24` hasta el 31 de enero de 2023 a las 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
                }
            }
        }
    ]
```

```
}
```

Ejemplo de instrucción de política: acceso a todos los archivos de un directorio desde un intervalo de direcciones IP

La siguiente política personalizada de ejemplo le permite crear URL firmadas para cualquier archivo del directorio `training`, tal y como indica el carácter comodín asterisco (`*`) del parámetro `Resource`. Los usuarios pueden acceder al archivo desde una dirección IP incluida en el rango `192.0.2.0/24` hasta el 31 de enero de 2023 a las 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/training/*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675159200
                }
            }
        }
    ]
}
```

Cada URL firmada con la que utilice esta política tiene una URL que identifica a un archivo específico, por ejemplo:

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Ejemplo de instrucción de política: acceso a todos los archivos asociados con un ID de par de claves desde una dirección IP

La siguiente política personalizada de ejemplo le permite crear URL firmadas para cualquier archivo asociado a cualquier distribución, tal y como indica el carácter comodín asterisco (`*`) del parámetro `Resource`. La URL firmada debe usar el protocolo `https://`, no `http://`. El usuario debe utilizar la dirección IP `192.0.2.10/32`. (El valor `192.0.2.10/32` en notación CIDR se refiere a la dirección IP individual `192.0.2.10`). Los archivos solo van a estar disponibles desde el 31 de enero de 2023 a las 10:00 UTC hasta el 2 de febrero de 2023 a las 10:00 UTC:

```
{
    "Statement": [
       {
            "Resource": "https://*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.10/32"
                },
                "DateGreaterThan": {
                    "AWS:EpochTime": 1675159200
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675332000
                }
            }
        }
    ]
}
```

Cada URL firmada con la que utilice esta política tiene una URL que identifica un archivo específico de una distribución de CloudFront específica; por ejemplo:

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

La URL firmada también incluye un ID de par de claves que se debe asociar con un grupo de claves de confianza en la distribución (d111111abcdef8.cloudfront.net) que se especifica en la URL.

Creación de una firma para una URL firmada que utiliza una política personalizada

La firma de una URL firmada que utiliza una política personalizada es una versión de la instrucción de política a la que se le ha aplicado una función hash, firmada y codificada con base64. Para crear una firma para una política personalizada, complete los pasos siguientes.

Para obtener más información y ejemplos de cómo resumir, aplicar una función hash y codificar la instrucción de política, consulte:

- Comandos de Linux y OpenSSL para codificación y cifrado base64
- Ejemplos de código para la creación de una firma para una URL firmada

Opción 1: para crear una firma mediante una política personalizada

1. Use la función hash SHA-1 y la clave privada RSA o ECDSA generada para codificar y firmar la instrucción de política JSON creada en el procedimiento Para crear una instrucción de política para una URL firmada que use una política personalizada. Utilice la versión de la instrucción de política que ya no incluye espacios vacíos pero que aún no se ha codificado con base64.

   Para la clave privada requerida por la función hash, utilice una clave privada cuya clave pública esté en un grupo de claves de confianza activo para la distribución.

   > **Note**
   >
   > El método que utilice para resumir y aplicar una función hash la instrucción de política depende de su lenguaje de programación y plataforma. Para ver código de muestra, consulte Ejemplos de código para la creación de una firma para una URL firmada.

2. Elimine los espacios vacíos (incluidos tabuladores y caracteres de línea nueva) de la cadena a la que se le ha aplicado una función hash y firmada.
3. Codifique la cadena con codificación base64 de MIME. Para obtener más información, consulte la Section 6.8, Base64 Content-Transfer-Encoding de RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Sustituya caracteres no válidos en una cadena de consulta de URL por caracteres válidos. En la siguiente tabla se muestran los caracteres válidos y no válidos.

Sustituya los caracteres no válidos	Por estos caracteres válidos
+	- (guion)
=	_ (guion bajo)
/	~ (tilde)

5. Añada el valor resultante a la URL firmada después de `&Signature=` y vuelva a Para crear una URL firmada mediante una política personalizada para terminar de encadenar las partes de la URL firmada.

Uso de cookies firmadas

Las cookies firmadas de CloudFront le permiten controlar quién puede acceder al contenido cuando no desea cambiar las URL actuales o cuando desea proporcionar acceso a varios archivos restringidos, por ejemplo, todos los archivos del área de suscriptores de un sitio web. En este tema se explica qué tomar en cuenta al utilizar cookies firmadas y describe cómo configurarlas mediante políticas predefinidas o personalizadas.

Temas

- Decisión de utilizar políticas predefinidas o personalizadas para cookies firmadas
- Cómo funcionan las cookies firmadas
- Prevención del uso indebido de cookies firmadas
- Cuándo comprueba CloudFront la fecha y hora de vencimiento de una cookie firmada
- Código de muestra y herramientas de terceros
- Establecimiento de cookies firmadas mediante una política predefinida
- Establecimiento de cookies firmadas mediante una política personalizada
- Create signed cookies using PHP

Decisión de utilizar políticas predefinidas o personalizadas para cookies firmadas

Al crear una cookie firmada, se escribe una instrucción de política en formato JSON que especifica las restricciones en la cookie firmada, por ejemplo, el tiempo de validez de la cookie. Puede utilizar políticas predefinidas o personalizadas. En la siguiente tabla se comparan las políticas predefinidas y las personalizadas:

Descripción	Política predefinida	Política personalizada
Puede reutilizar la instrucción de la política con varios archivos. Para reutilizar la instrucción de política, debe utilizar caracteres comodín en el objeto `Resource`. Para obtener más información, consulte). Valores que se especifican en la instrucción de política de una política personalizada para cookies firmadas.)	No	Sí

Descripción	Política predefinida	Política personalizada
Puede especificar la fecha y la hora a la que los usuarios pueden empezar a obtener acceso a su contenido.	No	Sí (opcional)
Puede especificar la fecha y la hora a la que los usuarios dejan de obtener acceso a su contenido.	Sí	Sí
Puede especificar la dirección IP o a un rango de direcciones IP de los usuarios que pueden obtener acceso a su contenido.	No	Sí (opcional)

Para obtener información acerca de cómo crear cookies firmadas mediante una política predefinida, consulte Establecimiento de cookies firmadas mediante una política predefinida.

Para obtener información acerca de cómo crear cookies firmadas mediante una política personalizada, consulte Establecimiento de cookies firmadas mediante una política personalizada.

Cómo funcionan las cookies firmadas

A continuación, se muestra información general acerca de cómo configurar CloudFront para cookies firmadas y cómo responde CloudFront cuando un usuario envía una solicitud que contiene una cookie firmada.

1. En la distribución de CloudFront, especifique uno o más grupos de claves de confianza, que contienen las claves públicas que CloudFront puede utilizar para comprobar la firma de URL. Se utilizan las claves privadas correspondientes para firmar las URL.

   Para obtener más información, consulte Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas.

2. Desarrolle una aplicación para determinar si un usuario debe obtener acceso a su contenido y, en caso de que sí, que envíe 3 encabezados `Set-Cookie` al espectador. (Cada encabezado `Set-Cookie` puede contener solo un par de nombre-valor y una cookie de CloudFront firmada requiere tres pares de nombre-valor). Debe enviar los encabezados `Set-Cookie` al espectador antes de que el usuario solicite su contenido privado. Si configura un periodo de vencimiento

corto en la cookie, le recomendamos enviar tres encabezados `Set-Cookie` más en respuesta a solicitudes posteriores, de modo que el usuario continúe teniendo acceso.

Normalmente, la distribución de CloudFront tendrá al menos dos comportamientos de la caché: uno que no requiere autenticación y otro que sí. La página de error de la parte segura del sitio incluye un redirector o un enlace a una página de inicio de sesión.

Si configura la distribución para que el almacenamiento de archivos en la caché dependa de las cookies, CloudFront no almacenará archivos independientes en la caché en función de los atributos de las cookies firmadas.

3. Un usuario inicia sesión en su sitio web y paga por el contenido o cumple algún otro requisito para el acceso.
4. Su aplicación devuelve los encabezados `Set-Cookie` en la respuesta, y el espectador almacena los pares nombre-valor.
5. El usuario solicita un archivo.

   El navegador del usuario o cualquier otro espectador obtiene los pares nombre-valor del paso 4 y los añade a la solicitud en un encabezado `Cookie`. Esta es la cookie firmada.
6. CloudFront utiliza la clave pública para validar la firma en la cookie firmada y confirmar que dicha cookie no se ha manipulado. Si la firma no es válida, se rechaza la solicitud.

   Si la firma de la cookie es válida, CloudFront examina la instrucción de la política en la cookie (o crea una si utiliza una política predefinida) para confirmar que la solicitud sigue siendo válida. Por ejemplo, si ha especificado una fecha y hora de inicio y fin de la cookie, CloudFront confirma que el usuario intenta acceder al contenido durante el periodo en el que ha decidido permitir dicho acceso.

   Si la solicitud cumple los requisitos de la instrucción de la política, CloudFront enviará el contenido del mismo modo que envía el contenido no restringido: determina si el archivo ya está en la caché de borde, reenvía la solicitud al origen en caso necesario y devuelve el archivo al usuario.

Prevención del uso indebido de cookies firmadas

Si especifica el parámetro `Domain` en un encabezado `Set-Cookie`, especifique el valor de la forma más precisa posible para reducir el acceso potencial por parte de alguien con el mismo nombre de dominio raíz. Por ejemplo, app.example.com es mejor que example.com, especialmente si no

controla example.com. Esto ayuda a impedir que alguien obtenga acceso a su contenido desde www.example.com.

Para evitar este tipo de ataques, haga lo siguiente:

- Excluya los atributos de cookies `Expires` y `Max-Age` para que el encabezado `Set-Cookie` cree una cookie de sesión. Las cookies de sesión se eliminan automáticamente cuando el usuario cierra el navegador, lo que reduce la posibilidad de alguien obtenga acceso no autorizado a su contenido.
- Incluya el atributo `Secure` para que la cookie se cifre cuando un espectador la incluya en una solicitud.
- De ser posible, utilice una política personalizada e incluya la dirección IP del espectador.
- En el atributo `CloudFront-Expires`, especifique el menor tiempo de vencimiento posible pero razonable en función de por cuánto tiempo desea que los usuarios puedan obtener acceso a su contenido.

Cuándo comprueba CloudFront la fecha y hora de vencimiento de una cookie firmada

Para determinar si una cookie firmada sigue siendo válida, CloudFront comprueba la fecha y hora de vencimiento de la cookie en el momento de la solicitud HTTP. Si un cliente comienza a descargar un archivo grande inmediatamente antes de la fecha de vencimiento, la descarga se realizará por completo incluso si se sobrepasa la hora de vencimiento durante la descarga. Si la conexión TCP se interrumpe y el cliente intenta reiniciar la descarga después de la fecha de vencimiento, la descarga fallará.

Si un cliente utiliza rangos GET para obtener un archivo en partes más pequeñas, cualquier solicitud GET que se produzca después de la fecha de vencimiento no se procesará. Para obtener más información acerca de Range GET, consulte Cómo CloudFront procesa las solicitudes parciales de un objeto (rango GET).

Código de muestra y herramientas de terceros

El código de muestra para contenido privado solo muestra cómo crear firmas para URL firmadas. Sin embargo, el proceso de creación de una firma para una cookie firmada es muy similar, así que gran parte del código de muestra es aplicable. Para obtener más información, consulte los temas siguientes:

- Crear una firma de URL con Perl

- Crear una firma de URL con PHP
- Crear una firma de URL mediante C# y .NET Framework
- Crear una firma de URL con Java

Establecimiento de cookies firmadas mediante una política predefinida

Para establecer una cookie firmada utilizando una política predefinida, complete los pasos siguientes. Para crear la firma, consulte Creación de una firma para una cookie firmada que utiliza una política predefinida.

Para establecer cookies firmadas mediante una política predefinida

1. Si utiliza. NET o Java para crear cookies firmadas y no ha reformateado la clave privada del par de claves del formato .pem predeterminado a un formato compatible con .NET o con Java, hágalo ahora. Para obtener más información, consulte Volver a formatear la clave privada (solo .NET y Java).
2. Programe su aplicación para enviar tres encabezados `Set-Cookie` a los espectadores aprobados. Necesita tres encabezados `Set-Cookie` porque cada encabezado `Set-Cookie` puede contener solo un par de nombre-valor y una cookie firmada de CloudFront requiere tres pares de nombre-valor. Los pares de nombre-valor son: `CloudFront-Expires`, `CloudFront-Signature` y `CloudFront-Key-Pair-Id`. Los valores deben estar presentes en el lector antes de que un usuario realice la primera solicitud de un archivo cuyo acceso desea controlar.

   > **Note**
   >
   > En general, recomendamos que excluya los atributos `Expires` y `Max-Age`. Al excluir los atributos, el navegador elimina la cookie cuando el usuario lo cierra, lo que reduce la posibilidad de alguien obtenga acceso no autorizado a su contenido. Para obtener más información, consulte Prevención del uso indebido de cookies firmadas.

   Los nombres de los atributos de las cookies distinguen entre mayúsculas y minúsculas.

   Los saltos de línea se incluyen únicamente para que los atributos sean más legibles.

```
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
```

(Opcional) **`Domain`**

Nombre de dominio del archivo solicitado. Si no especifica un atributo `Domain`, el valor predeterminado será el nombre de dominio de la URL; esto es aplicable solo al nombre de dominio especificado, no a subdominios. Si especifica un atributo `Domain`, también será aplicable a subdominios. Un punto al inicio del nombre de dominio (por ejemplo, `Domain=.example.com`) es opcional. Además, si no especifica un atributo `Domain`, el nombre de dominio de la URL y el valor del atributo `Domain` deberán coincidir.

Puede especificar el nombre de dominio que CloudFront ha asignado a la distribución, por ejemplo, d111111abcdef8.cloudfront.net, pero no puede especificar *.cloudfront.net para el nombre de dominio.

Si desea utilizar un nombre de dominio alternativo como example.com en las URL, debe añadir dicho nombre de dominio a su distribución independientemente de que especifique el atributo `Domain`. Para obtener más información, consulte Nombres de dominio alternativos (CNAME) en el tema Referencia de toda la configuración de distribución.

(Opcional) **`Path`**

Ruta del archivo solicitado. Si no especifica un atributo `Path`, el valor predeterminado será la ruta de la URL.

`Secure`

Requiere que el espectador cifre cookies antes de enviar una solicitud. Recomendamos que envíe el encabezado `Set-Cookie` a través de una conexión HTTPS para asegurarse de que los atributos de la cookie estén protegidos contra ataques man-in-the-middle.

`HttpOnly`

Define la forma en que el navegador (si es compatible) interactúa con el valor de la cookie. Con `HttpOnly`, JavaScript no puede acceder a los valores de las cookies. Esta precaución puede ayudar a mitigar los ataques de scripting entre sitios (XSS). Para obtener más información, consulte Using HTTP cookies.

`CloudFront-Expires`

Especifique la fecha y la hora de vencimiento en formato de tiempo Unix (en segundos) y hora universal coordinada (UTC). Por ejemplo, 1 de enero de 2026 a las 10:00 UTC pasa a ser 1767290400 en formato de tiempo Unix.

Para utilizar el tiempo de época, especifique un número entero de 64 bits para una fecha que no sea posterior a `9223372036854775807` (viernes, 11 de abril de 2262 a las 23:47:16.854 UTC).

Para obtener información acerca de UTC, consulte RFC 3339, fecha y hora en Internet: marcas temporales, https://tools.ietf.org/html/rfc3339.

`CloudFront-Signature`

Una versión de una instrucción de política JSON firmada, a la que se le ha aplicado una función hash y codificada en base64. Para obtener más información, consulte Creación de una firma para una cookie firmada que utiliza una política predefinida.

`CloudFront-Key-Pair-Id`

El ID de una clave pública de CloudFront, por ejemplo, `K2JCJMDEHXQW5F`. El ID de clave pública indica a CloudFront qué clave pública usar para validar la URL firmada. CloudFront compara la información de la firma con la información de la instrucción de política para comprobar que la URL no se ha manipulado.

Esta clave pública debe pertenecer a un grupo de claves que tiene un signatario de confianza en la distribución. Para obtener más información, consulte Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas.

En el ejemplo siguiente, se muestran los encabezados `Set-Cookie` de una cookie firmada cuando se usa el nombre de dominio asociado a la distribución en las URL de los archivos:

```
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
```

En el ejemplo siguiente, se muestran los encabezados `Set-Cookie` de una cookie firmada cuando se usa el nombre de dominio alternativo example.org en las URL de los archivos:

```
Set-Cookie: CloudFront-Expires=1426500000; Domain=example.org; Path=/images/*; Secure;
 HttpOnly
Set-Cookie: CloudFront-Signature=yXrSIgyQoeE4FBI4eMKF6ho~CA8_; Domain=example.org;
 Path=/images/*; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F; Domain=example.org; Path=/images/*;
 Secure; HttpOnly
```

Si desea utilizar un nombre de dominio alternativo como example.com en las URL, debe añadir dicho nombre de dominio a su distribución independientemente de que especifique el atributo `Domain`. Para obtener más información, consulte Nombres de dominio alternativos (CNAME) en el tema Referencia de toda la configuración de distribución.

Creación de una firma para una cookie firmada que utiliza una política predefinida

Para crear la firma para una cookie firmada que utilice una política predefinida, realice los procedimientos indicados a continuación.

Temas

- Creación de una instrucción de política para una cookie firmada que use una política predefinida
- Firma de la instrucción de política para crear una firma para una cookie firmada que utiliza una política predefinida

Creación de una instrucción de política para una cookie firmada que use una política predefinida

Al establecer una cookie firmada que use una política predefinida, el atributo `CloudFront-Signature` es una versión de una instrucción de política firmada y a la que se le ha aplicado una función hash. En el caso de cookies firmadas que utilizan una política predefinida, la instrucción

de política no se incluye en el encabezado `Set-Cookie`, a diferencia de las cookies firmadas que utilizan una política personalizada. Para crear la instrucción de política, complete los pasos siguientes.

Para crear una instrucción de política para una cookie firmada que use una política predefinida

1. Cree la instrucción de política utilizando el siguiente formato JSON y codificación de caracteres UTF-8. Incluya toda la puntuación y otros valores literalmente, tal como se especifica. Para obtener más información acerca de los parámetros `Resource` y `DateLessThan`, consulte Valores que se especifican en la instrucción de política de una política predefinida para cookies firmadas.

```
{
    "Statement": [
        {
            "Resource": "base URL or stream name",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": ending date and time in Unix time format and
 UTC
                }
            }
        }
    ]
}
```

2. Elimine todos los espacios vacíos (incluidos tabuladores y caracteres de línea nueva) de la instrucción de la política. Es posible que tenga que incluir caracteres de escape en la cadena del código de la aplicación.

Valores que se especifican en la instrucción de política de una política predefinida para cookies firmadas

Al crear una instrucción de una política predefinida, debe especificar los siguientes valores:

Recurso

La URL base, incluidas las cadenas de consulta, de haberlas; por ejemplo:

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

Puede especificar solo un valor en `Resource`.

Tenga en cuenta lo siguiente:

- Protocol (Protocolo): el valor debe comenzar con `http://` o `https://`.
- Query string parameters (Parámetros de cadena de consulta): si no tiene parámetros de cadena de consulta, omita el signo de interrogación.
- Alternate domain names (Nombres de dominio alternativos): si especifica un nombre de dominio alternativo (CNAME) en la URL, debe especificarlo al hacer referencia al archivo en la página web o aplicación. No especifique la URL de Amazon S3 para el archivo.

DateLessThan

La fecha y hora de vencimiento de la URL en formato de tiempo Unix (en segundos) y hora universal coordinada (UTC). No incluya el valor entre comillas.

Por ejemplo, 16 de marzo de 2015 a las 10:00 h UTC pasa a ser 1426500000 en formato de tiempo Unix.

Este valor debe coincidir con el valor del atributo `CloudFront-Expires` en el encabezado `Set-Cookie`. No incluya el valor entre comillas.

Para obtener más información, consulte Cuándo comprueba CloudFront la fecha y hora de vencimiento de una cookie firmada.

Ejemplo de instrucción de política para una política predefinida

Si se utiliza el siguiente ejemplo de instrucción de política en una cookie firmada, los usuarios podrán obtener acceso al archivo `https://d111111abcdef8.cloudfront.net/horizon.jpg` hasta el 16 de marzo de 2015 a las 10:00 h UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": 1426500000
                }
            }
        }
```

```
    ]
}
```

Firma de la instrucción de política para crear una firma para una cookie firmada que utiliza una política predefinida

Para crear el valor del atributo `CloudFront-Signature` en un encabezado `Set-Cookie`, aplique una función hash y firme la instrucción de política creada en Para crear una instrucción de política para una cookie firmada que use una política predefinida.

Para obtener más información y ejemplos de cómo aplicar una función hash, firmar y codificar la instrucción de política, consulte los siguientes temas:

- Comandos de Linux y OpenSSL para codificación y cifrado base64
- Ejemplos de código para la creación de una firma para una URL firmada

Para crear una firma para una cookie firmada que use una política predefinida

1. Use la función hash SHA-1 y RSA para resumir y firmar la instrucción de política creada en el procedimiento Para crear una instrucción de política para una cookie firmada que use una política predefinida. Utilice la versión de la instrucción de política que ya no incluye espacios vacíos.

   Para la clave privada requerida por la función hash, utilice una clave privada cuya clave pública esté en un grupo de claves de confianza activo para la distribución.

   > **Note**
   >
   > El método que utilice para resumir y aplicar una función hash la instrucción de política depende de su lenguaje de programación y plataforma. Para ver código de muestra, consulte Ejemplos de código para la creación de una firma para una URL firmada.

2. Elimine los espacios vacíos (incluidos tabuladores y caracteres de línea nueva) de la cadena a la que se le ha aplicado una función hash y firmada.
3. Codifique la cadena con codificación base64 de MIME. Para obtener más información, consulte la Section 6.8, Base64 Content-Transfer-Encoding de RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.

4. Sustituya caracteres no válidos en una cadena de consulta de URL por caracteres válidos. En la siguiente tabla se muestran los caracteres válidos y no válidos.

Sustituya los caracteres no válidos	Por estos caracteres válidos
+	- (guion)
=	_ (guion bajo)
/	~ (tilde)

5. Incluya el valor resultante en el encabezado `Set-Cookie` para el par nombre-valor `CloudFront-Signature`. A continuación, vuelva a Para establecer cookies firmadas mediante una política predefinida y añada el encabezado `Set-Cookie` en `CloudFront-Key-Pair-Id`.

Establecimiento de cookies firmadas mediante una política personalizada

Para establecer una cookie firmada que utiliza una política personalizada, complete los siguientes pasos.

Para establecer cookies firmadas mediante una política personalizada

1. Si utiliza. NET o Java para crear URL firmadas y no ha reformateado la clave privada del par de claves del formato .pem predeterminado a un formato compatible con .NET o con Java, hágalo ahora. Para obtener más información, consulte Volver a formatear la clave privada (solo .NET y Java).
2. Programe su aplicación para enviar tres encabezados `Set-Cookie` a los espectadores aprobados. Necesita tres encabezados `Set-Cookie` porque cada encabezado `Set-Cookie` puede contener solo un par de nombre-valor y una cookie firmada de CloudFront requiere tres pares de nombre-valor. Los pares de nombre-valor son: `CloudFront-Policy`, `CloudFront-Signature` y `CloudFront-Key-Pair-Id`. Los valores deben estar presentes en el lector antes de que un usuario realice la primera solicitud de un archivo cuyo acceso desea controlar.

> **Note**
>
> En general, recomendamos que excluya los atributos `Expires` y `Max-Age`. Al excluirlos, el navegador elimina la cookie cuando el usuario lo cierra, lo que reduce la posibilidad

de alguien obtenga acceso no autorizado a su contenido. Para obtener más información, consulte Prevención del uso indebido de cookies firmadas.

Los nombres de los atributos de las cookies distinguen entre mayúsculas y minúsculas.

Los saltos de línea se incluyen únicamente para que los atributos sean más legibles.

```
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
```

(Opcional) **`Domain`**

Nombre de dominio del archivo solicitado. Si no especifica un atributo `Domain`, el valor predeterminado será el nombre de dominio de la URL; esto es aplicable solo al nombre de dominio especificado, no a subdominios. Si especifica un atributo `Domain`, también será aplicable a subdominios. Un punto al inicio del nombre de dominio (por ejemplo, `Domain=.example.com`) es opcional. Además, si no especifica un atributo `Domain`, el nombre de dominio de la URL y el valor del atributo `Domain` deberán coincidir.

Puede especificar el nombre de dominio que CloudFront ha asignado a la distribución, por ejemplo, d111111abcdef8.cloudfront.net, pero no puede especificar *.cloudfront.net para el nombre de dominio.

Si desea utilizar un nombre de dominio alternativo como example.com en las URL, debe añadir dicho nombre de dominio a su distribución independientemente de que especifique el atributo `Domain`. Para obtener más información, consulte Nombres de dominio alternativos (CNAME) en el tema Referencia de toda la configuración de distribución.

(Opcional) **`Path`**

Ruta del archivo solicitado. Si no especifica un atributo `Path`, el valor predeterminado será la ruta de la URL.

`Secure`

Requiere que el espectador cifre cookies antes de enviar una solicitud. Recomendamos que envíe el encabezado `Set-Cookie` a través de una conexión HTTPS para asegurarse de que los atributos de la cookie estén protegidos contra ataques man-in-the-middle.

`HttpOnly`

Requiere que el espectador envíe la cookie únicamente en solicitudes de HTTP o HTTPS.

`CloudFront-Policy`

La instrucción de política en formato JSON después de haber eliminado los espacios vacíos y, a continuación, codificada con base64. Para obtener más información, consulte Creación de una firma para una cookie firmada que utiliza una política personalizada.

La instrucción de política controla el acceso que una cookie firmada concede a un usuario. Incluye los archivos a los que el usuario puede acceder, una fecha y hora de vencimiento, una fecha y hora opcionales a las que la URL se convierte en válida y una dirección IP opcional o un intervalo de direcciones IP a las que se permite acceder al archivo.

`CloudFront-Signature`

Una versión firmada, a la que se le ha aplicado una función hash y codificada en base64 de la instrucción de política JSON. Para obtener más información, consulte Creación de una firma para una cookie firmada que utiliza una política personalizada.

`CloudFront-Key-Pair-Id`

El ID de una clave pública de CloudFront, por ejemplo, `K2JCJMDEHXQW5F`. El ID de clave pública indica a CloudFront qué clave pública usar para validar la URL firmada. CloudFront compara la información de la firma con la información de la instrucción de política para comprobar que la URL no se ha manipulado.

Esta clave pública debe pertenecer a un grupo de claves que tiene un signatario de confianza en la distribución. Para obtener más información, consulte Especificación de los signatarios que pueden crear URL firmadas y cookies firmadas.

Ejemplos de encabezados **`Set-Cookie`** para políticas personalizadas

Consulte los siguientes ejemplos de pares de encabezados `Set-Cookie`.

Si desea utilizar un nombre de dominio alternativo como example.org en las URL, debe agregarlo a la distribución independientemente de que especifique el atributo `Domain`. Para obtener más información, consulte Nombres de dominio alternativos (CNAME) en el tema Referencia de toda la configuración de distribución.

Example Ejemplo 1

Puede utilizar los encabezados `Set-Cookie` de una cookie firmada cuando se utiliza el nombre de dominio asociado a la distribución en las URL de los archivos.

```
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 Ejemplo 2

Puede utilizar los encabezados `Set-Cookie` de una cookie firmada cuando se utiliza el nombre de dominio alternativo (example.org) en las URL de los archivos.

```
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 Ejemplo 3

Puede utilizar los pares de encabezados `Set-Cookie` de una solicitud firmada cuando se utiliza el nombre de dominio asociado a la distribución en las URL de los archivos.

```
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 Ejemplo 4

Puede utilizar los pares de encabezados `Set-Cookie` de una solicitud firmada cuando se utiliza un nombre de dominio alternativo (example.org) asociado a la distribución en las URL de los archivos.

```
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
```

Creación de una instrucción de política para una cookie firmada que utiliza una política personalizada

Para crear una instrucción de política para una política personalizada, complete los siguientes pasos. Para consultar varias instrucciones de políticas de ejemplo que controlan el acceso a archivos de distintas maneras, consulte Ejemplos de instrucciones de políticas para una cookie firmada que utiliza una política personalizada.

Para crear una instrucción de política para una cookie firmada que use una política personalizada

1. Cree la instrucción de política en el siguiente formato JSON.

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

Tenga en cuenta lo siguiente:

- Puede incluir una instrucción.
- Utilice la codificación de caracteres UTF-8.
- Incluya toda la puntuación y los nombres de parámetros exactamente como se especifica. No se aceptan abreviaturas de nombres de parámetros.
- El orden de los parámetros de la sección `Condition` no importa.
- Para obtener información acerca de valores para `Resource`, `DateLessThan`, `DateGreaterThan` y `IpAddress`, consulte Valores que se especifican en la instrucción de política de una política personalizada para cookies firmadas.

2. Elimine todos los espacios vacíos (incluidos tabuladores y caracteres de línea nueva) de la instrucción de la política. Es posible que tenga que incluir caracteres de escape en la cadena del código de la aplicación.
3. Codifique la instrucción de política con codificación base64 de MIME. Para obtener más información, consulte la Section 6.8, Base64 Content-Transfer-Encoding de RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.

4. Sustituya caracteres no válidos en una cadena de consulta de URL por caracteres válidos. En la siguiente tabla se muestran los caracteres válidos y no válidos.

Sustituya los caracteres no válidos	Por estos caracteres válidos
+	- (guion)
=	_ (guion bajo)
/	~ (tilde)

5. Incluya el valor resultante en el encabezado `Set-Cookie` después de `CloudFront-Policy=`.
6. Cree una firma para el encabezado `Set-Cookie` en `CloudFront-Signature` aplicando una función hash, firmando y codificando con base64 la instrucción de política. Para obtener más información, consulte Creación de una firma para una cookie firmada que utiliza una política personalizada.

Valores que se especifican en la instrucción de política de una política personalizada para cookies firmadas

Al crear una instrucción de política para una política personalizada, debe especificar los siguientes valores.

Recurso

La URL base, incluidas las cadenas de consulta, de haberlas:

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

> **Important**
>
> Si omite el parámetro `Resource`, los usuarios podrán obtener acceso a todos los archivos asociados a cualquier distribución que esté asociada al par de claves utilizado para crear la URL firmada.

Puede especificar solo un valor en `Resource`.

Tenga en cuenta lo siguiente:

- Protocol (Protocolo): el valor debe comenzar con `http://` o `https://`.
- Query string parameters (Parámetros de cadena de consulta): si no tiene parámetros de cadena de consulta, omita el signo de interrogación.
- Wildcards (Caracteres comodín): puede utilizar el carácter comodín que coincide con cero o más caracteres (*) o el carácter comodín que coincide exactamente con un carácter (?) en cualquier lugar de la cadena. Por ejemplo, el valor:

  ```
  https://d111111abcdef8.cloudfront.net/*game_download.zip*
  ```

  incluiría, por ejemplo, los siguientes archivos:

  - `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`
- Alternate domain names (Nombres de dominio alternativos): si especifica un nombre de dominio alternativo (CNAME) en la URL, debe especificarlo al hacer referencia al archivo en la página web o aplicación. No especifique la URL de Amazon S3 para el archivo.

DateLessThan

La fecha y hora de vencimiento de la URL en formato de tiempo Unix (en segundos) y hora universal coordinada (UTC). No incluya el valor entre comillas.

Por ejemplo, 16 de marzo de 2015 a las 10:00 h UTC pasa a ser 1426500000 en formato de tiempo Unix.

Para obtener más información, consulte Cuándo comprueba CloudFront la fecha y hora de vencimiento de una cookie firmada.

DateGreaterThan (opcional)

Una fecha y hora de inicio opcionales de la URL en formato de tiempo Unix (en segundos) y hora universal coordinada (UTC). Los usuarios no pueden acceder al archivo en la fecha y hora especificadas ni antes. No incluya el valor entre comillas.

IpAddress (opcional)

La dirección IP del cliente que hace la solicitud GET. Tenga en cuenta lo siguiente:

- Para permitir que cualquier dirección IP obtenga acceso al archivo, omita el parámetro `IpAddress`.
- Puede especificar una dirección IP o a un rango de direcciones IP. Por ejemplo, no puede configurar la política para permitir el acceso si la dirección IP del cliente está en uno de dos rangos separados.
- Para permitir el acceso desde una única dirección IP, especifique:

  `"Dirección IP IPv/32"`

- Debe especificar rangos de direcciones IP en formato estándar IPv4 CIDR (por ejemplo, `192.0.2.0/24`). Para obtener más información, consulte RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan, https://tools.ietf.org/html/rfc4632.

> **Important**
>
> Las direcciones IP en formato IPv6, como 2001:0db8:85a3::8a2e:0370:7334, no son compatibles.

Si está utilizando una política personalizada que incluya `IpAddress`, no habilite IPv6 para la distribución. Si desea restringir el acceso a algún contenido por dirección IP y admite solicitudes IPv6 de otro contenido, puede crear dos distribuciones. Para obtener más información, consulte Habilitación de IPv6 (solicitudes de espectadores) en el tema Referencia de toda la configuración de distribución.

Ejemplos de instrucciones de políticas para una cookie firmada que utiliza una política personalizada

En los siguientes ejemplos de instrucciones de políticas, se muestra cómo controlar el acceso a un archivo específico, a todos los archivos de un directorio o a todos los archivos asociados a un ID de par de claves. Los ejemplos también muestran cómo controlar el acceso de una dirección IP individual o a un rango de direcciones IP, y cómo impedir que los usuarios utilicen la cookie firmada después de una fecha y hora específicas.

Si copia y pega cualquiera de estos ejemplos, elimine los espacios vacíos (incluidos los tabuladores y los caracteres de línea nueva), sustituya los valores por sus propios valores e incluya un carácter de línea nueva después de la llave de cierre (}).

Para obtener más información, consulte Valores que se especifican en la instrucción de política de una política personalizada para cookies firmadas.

Temas

- Ejemplo de instrucción de política: acceso a un archivo desde un intervalo de direcciones IP
- Ejemplo de instrucción de política: acceso a todos los archivos de un directorio desde un intervalo de direcciones IP
- Ejemplo de instrucción de política: acceso a todos los archivos asociados con un ID de par de claves desde una dirección IP

Ejemplo de instrucción de política: acceso a un archivo desde un intervalo de direcciones IP

En la siguiente política personalizada de ejemplo de una cookie firmada se especifica que un usuario puede acceder al archivo `https://d111111abcdef8.cloudfront.net/game_download.zip` desde las direcciones IP incluidas en el intervalo `192.0.2.0/24` hasta el 1 de enero de 2023 a las 10:00 UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/game_download.zip",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Ejemplo de instrucción de política: acceso a todos los archivos de un directorio desde un intervalo de direcciones IP

La siguiente política personalizada de ejemplo le permite crear cookies firmadas para cualquier archivo del directorio `training`, tal y como indica el carácter comodín * del parámetro `Resource`. Los usuarios podrán obtener acceso al archivo desde una dirección IP incluida en el rango `192.0.2.0/24` hasta el 1 de enero de 2013 a las 10:00 h UTC:

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/training/*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Cada cookie firmada en la que utilice esta política tendrá una URL base que identificará un archivo específico; por ejemplo:

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Ejemplo de instrucción de política: acceso a todos los archivos asociados con un ID de par de claves desde una dirección IP

La siguiente política personalizada de ejemplo le permite establecer cookies firmadas para cualquier archivo asociado a cualquier distribución, tal y como indica el carácter comodín * del parámetro `Resource`. El usuario debe utilizar la dirección IP `192.0.2.10/32`. (El valor `192.0.2.10/32` en notación CIDR se refiere a la dirección IP individual `192.0.2.10`). Los archivos solo van a estar disponibles desde el 1 de enero de 2013 a las 10:00 h UTC hasta el 2 de enero de 2013 a las 10:00 h UTC:

```
{
    "Statement": [
```

```
        {
            "Resource": "https://*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.10/32"
                },
                "DateGreaterThan": {
                    "AWS:EpochTime": 1767290400
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767376800
                }
            }
        }
    ]
}
```

Cada cookie firmada en la que utiliza esta política incluye una URL base que identifica un archivo específico de una distribución de CloudFront específica; por ejemplo:

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

La cookie firmada también incluye un ID de par de claves que se debe asociar con un grupo de claves de confianza en la distribución (d111111abcdef8.cloudfront.net) que se especifica en la URL base.

Creación de una firma para una cookie firmada que utiliza una política personalizada

La firma de una cookie firmada que utiliza una política personalizada es una versión de la instrucción de política a la que se le ha aplicado una función hash, firmada y codificada con base64.

Para obtener más información y ejemplos de cómo resumir, aplicar una función hash y codificar la instrucción de política, consulte:

- Comandos de Linux y OpenSSL para codificación y cifrado base64
- Ejemplos de código para la creación de una firma para una URL firmada

Para crear una firma para una cookie firmada con una política personalizada

1. Use la función hash SHA-1 y RSA para resumir y firmar la instrucción de política JSON creada en el procedimiento Para crear una instrucción de política para una URL firmada que use una

política personalizada. Utilice la versión de la instrucción de política que ya no incluye espacios vacíos pero que aún no se ha codificado con base64.

Para la clave privada requerida por la función hash, utilice una clave privada cuya clave pública esté en un grupo de claves de confianza activo para la distribución.

> **Note**
>
> El método que utilice para resumir y aplicar una función hash la instrucción de política depende de su lenguaje de programación y plataforma. Para ver código de muestra, consulte Ejemplos de código para la creación de una firma para una URL firmada.

2. Elimine los espacios vacíos (incluidos tabuladores y caracteres de línea nueva) de la cadena a la que se le ha aplicado una función hash y firmada.
3. Codifique la cadena con codificación base64 de MIME. Para obtener más información, consulte la Section 6.8, Base64 Content-Transfer-Encoding de RFC 2045, MIME (Multipurpose Internet Mail Extensions) Part One: Format of Internet Message Bodies.
4. Sustituya caracteres no válidos en una cadena de consulta de URL por caracteres válidos. En la siguiente tabla se muestran los caracteres válidos y no válidos.

Sustituya los caracteres no válidos	Por estos caracteres válidos
+	- (guion)
=	_ (guion bajo)
/	~ (tilde)

5. Incluya el valor resultante en el encabezado `Set-Cookie`, en el par nombre-valor `CloudFront-Signature=`, y vuelva a Para establecer cookies firmadas mediante una política personalizada para añadir el encabezado `Set-Cookie` en `CloudFront-Key-Pair-Id`.

Create signed cookies using PHP

El siguiente ejemplo de código es similar al ejemplo de Crear una firma de URL con PHP en el sentido de que crea un enlace a un video. Sin embargo, en lugar de firmar la URL en el código, en

este ejemplo se firman las cookies con la función `create_signed_cookies()`. El reproductor del cliente utiliza las cookies para autenticar cada solicitud a la distribución de CloudFront.

Este enfoque resulta útil para transmitir contenido, como HTTP Live Streaming (HLS) o la transmisión dinámica adaptativa a través de HTTP (DASH), donde el cliente debe realizar varias solicitudes para recuperar el manifiesto, los segmentos y los activos de reproducción relacionados. Al usar cookies firmadas, el cliente puede autenticar cada solicitud sin necesidad de generar una nueva URL firmada para cada segmento.

> **Note**
>
> - Crear una firma de URL es solo una parte del proceso de entrega de contenido privado mediante cookies firmadas. Para obtener más información, consulte Uso de cookies firmadas.

Temas

- Creación de la firma RSA SHA-1
- Creación de cookies firmadas
- Código completo

En las siguientes secciones, se desglosa el ejemplo de código en partes individuales. A continuación, encontrará el ejemplo de código completo.

Creación de la firma RSA SHA-1

Este ejemplo de código hace lo siguiente:

1. La función `rsa_sha1_sign` proporciona hashes y firma la instrucción de política. Los argumentos requeridos son una instrucción de política y la clave privada que corresponde a una clave pública que está en un grupo de claves de confianza para la distribución.
2. A continuación, la función `url_safe_base64_encode` crea una versión de la firma de URL segura.

```
function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";
    $fp = fopen($private_key_filename, "r");
```

```
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);
    openssl_sign($policy, $signature, $pkeyid);
    openssl_free_key($pkeyid);
    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}
```

Creación de cookies firmadas

El siguiente código crea las cookies firmadas con los siguientes atributos de cookie: `CloudFront-Expires`, `CloudFront-Signature` y `CloudFront-Key-Pair-Id`. El código usa una política personalizada.

```
function create_signed_cookies($resource, $private_key_filename, $key_pair_id,
 $expires, $client_ip = null) {
    $policy = array(
        'Statement' => array(
            array(
                'Resource' => $resource,
                'Condition' => array(
                    'DateLessThan' => array('AWS:EpochTime' => $expires)
                )
            )
        )
    );

    if ($client_ip) {
        $policy['Statement'][0]['Condition']['IpAddress'] = array('AWS:SourceIp' =>
 $client_ip . '/32');
    }

    $policy = json_encode($policy);
    $encoded_policy = url_safe_base64_encode($policy);
```

```
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    $encoded_signature = url_safe_base64_encode($signature);

    return array(
        'CloudFront-Policy' => $encoded_policy,
        'CloudFront-Signature' => $encoded_signature,
        'CloudFront-Key-Pair-Id' => $key_pair_id
    );
}
```

Para obtener más información, consulte Establecimiento de cookies firmadas mediante una política personalizada.

Código completo

El siguiente ejemplo de código proporciona una demostración completa de la creación de cookies firmadas de CloudFront con PHP. Puede descargar el ejemplo completo desde el archivo demo-php.zip.

En el siguiente ejemplo, puede modificar el elemento `$policy Condition` para permitir los rangos de direcciones IPv4 e IPv6. Para ver un ejemplo, consulte Uso de direcciones IPv6 en políticas de IAM en la Guía del usuario de Amazon Simple Storage Service.

```
<?php

function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);
    openssl_sign($policy, $signature, $pkeyid);
    openssl_free_key($pkeyid);
    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}
```

```
function create_signed_cookies($resource, $private_key_filename, $key_pair_id,
 $expires, $client_ip = null) {
    $policy = array(
        'Statement' => array(
            array(
                'Resource' => $resource,
                'Condition' => array(
                    'DateLessThan' => array('AWS:EpochTime' => $expires)
                )
            )
        )
    );

    if ($client_ip) {
        $policy['Statement'][0]['Condition']['IpAddress'] = array('AWS:SourceIp' =>
 $client_ip . '/32');
    }

    $policy = json_encode($policy);
    $encoded_policy = url_safe_base64_encode($policy);
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    $encoded_signature = url_safe_base64_encode($signature);

    return array(
        'CloudFront-Policy' => $encoded_policy,
        'CloudFront-Signature' => $encoded_signature,
        'CloudFront-Key-Pair-Id' => $key_pair_id
    );
}



$private_key_filename = '/home/test/secure/example-priv-key.pem';
$key_pair_id = 'K2JCJMDEHXQW5F';
$base_url = 'https://d1234.cloudfront.net';

$expires = time() + 3600; // 1 hour from now

// Get the viewer real IP from the x-forward-for header as $_SERVER['REMOTE_ADDR']
 will return viewer facing IP. An alternative option is to use CloudFront-Viewer-
Address header. Note that this header is a trusted CloudFront immutable header. Example
 format: IP:PORT ("CloudFront-Viewer-Address": "1.2.3.4:12345")
$client_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
```

```
// For HLS manifest and segments (using wildcard)
$hls_resource = $base_url . '/sign/*';
$signed_cookies = create_signed_cookies($hls_resource, $private_key_filename,
 $key_pair_id, $expires, $client_ip);

// Set the cookies
$cookie_domain = parse_url($base_url, PHP_URL_HOST);
foreach ($signed_cookies as $name => $value) {
    setcookie($name, $value, $expires, '/', $cookie_domain, true, true);
}

?>

<!DOCTYPE html>
<html>
<head>
    <title>CloudFront Signed HLS Stream with Cookies</title>
</head>
<body>
    <h1>Amazon CloudFront Signed HLS Stream with Cookies</h1>
    <h2>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?> only viewable by IP
 <?php echo $client_ip; ?></h2>

    <div id='hls-video'>
        <video id="video" width="640" height="360" controls></video>
    </div>

    <script src="https://cdn.jsdelivr.net/npm/hls.js@latest"></script>
    <script>
        var video = document.getElementById('video');
        var manifestUrl = '<?php echo $base_url; ?>/sign/manifest.m3u8';

        if (Hls.isSupported()) {
            var hls = new Hls();
            hls.loadSource(manifestUrl);
            hls.attachMedia(video);
        }
        else if (video.canPlayType('application/vnd.apple.mpegurl')) {
            video.src = manifestUrl;
        }
    </script>
</body>
```

```
</html>
```

En lugar de utilizar cookies firmadas, puede utilizar URL firmadas. Para obtener más información, consulte Crear una firma de URL con PHP.

Comandos de Linux y OpenSSL para codificación y cifrado base64

Utilice los siguientes comandos de línea de comandos de Linux y OpenSSL para aplicar una función hash y firmar la instrucción de política, codificar la firma con base64 y sustituir caracteres que no sean válidos en los parámetros de cadenas de consulta de URL por caracteres válidos.

Para obtener información acerca de OpenSSL, consulte https://www.openssl.org.

```
cat policy | tr -d "\n" | tr -d " \t\n\r" | openssl sha1 -sign private_key.pem |
 openssl base64 -A | tr -- '+=/' '-_~'
```

En el comando anterior:

- `cat` lee el archivo `policy`.
- `tr -d "\n" | tr -d " \t\n\r"` elimina los espacios vacíos y el carácter de nueva línea agregados por `cat`.
- OpenSSL codifica el archivo con el hash SHA-1 y lo firma con el archivo de clave privada `private_key.pem`. La firma de clave privada puede ser RSA 2048 o ECDSA 256.
- OpenSSL codifica en base64 la instrucción de política a la que se le ha aplicado una función hash y que se ha firmado.
- `tr` sustituye los caracteres no válidos de los parámetros de cadenas de consulta de URL por caracteres válidos.

Para consultar más ejemplos de código que demuestren la creación de una firma, consulte Ejemplos de código para la creación de una firma para una URL firmada.

Ejemplos de código para la creación de una firma para una URL firmada

En esta sección se incluyen ejemplos de aplicación descargables en los que se muestra cómo crear firmas para URL firmadas. Los ejemplos están disponibles en Perl, PHP, C # y Java. Puede utilizar cualquiera de los ejemplos para crear URL firmadas. El script Perl se ejecuta en plataformas Linux y macOS. El ejemplo de PHP funcionará en cualquier servidor que ejecute PHP. El ejemplo de C # utiliza .NET Framework.

Para obtener un código de ejemplo en JavaScript (Node.js), consulte Creación de URL firmadas de Amazon CloudFront en Node.js en el blog para desarrolladores de AWS.

Para obtener un código de ejemplo en Python, consulte Generar una URL firmada para Amazon CloudFront en la Referencia de la API de AWS SDK para Python (Boto3) y este código de ejemplo en el repositorio GitHub de Boto3.

Temas

- Crear una firma de URL con Perl
- Crear una firma de URL con PHP
- Crear una firma de URL mediante C# y .NET Framework
- Crear una firma de URL con Java

Crear una firma de URL con Perl

Esta sección incluye un script Perl para plataformas Linux/Mac que puede utilizar para crear la firma para contenido privado. Para crear la firma, ejecute el script con argumentos de línea de comandos que especifiquen la URL de CloudFront, la ruta a la clave privada del signatario, el ID de la clave y una fecha de vencimiento de la URL. La herramienta también puede decodificar URL firmadas.

> **Note**
>
> Crear una firma de URL es solo una parte del proceso de entrega de contenido privado mediante una URL firmada. Para obtener más información acerca del proceso completo, consulte Uso de URL firmadas.

Temas

- Código fuente del script Perl para crear una URL firmada

Código fuente del script Perl para crear una URL firmada

El siguiente código fuente Perl puede utilizarse para crear una URL firmada para CloudFront. Los comentarios del código incluyen información acerca de los conmutadores de las líneas de comandos y las características de la herramienta.

```
#!/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;
```

Crear una firma de URL con PHP

Cualquier servidor web que ejecute PHP puede utilizar este código de ejemplo de PHP para crear instrucciones de política y firmas para distribuciones de CloudFront privadas. El ejemplo completo crea una página web que funciona con enlaces de URL firmadas que reproducen una secuencia de vídeo mediante streaming de CloudFront. Puede descargar el ejemplo completo desde el archivo demo-php.zip.

> **Notas**
>
> - Crear una firma de URL es solo una parte del proceso de entrega de contenido privado mediante una URL firmada. Para obtener más información acerca de todo el proceso, consulte Uso de URL firmadas.
> - También puede crear URL firmadas mediante la clase `UrlSigner` en AWS SDK para PHP. Para obtener más información, consulte Class UrlSigner en la Referencia de la API de AWS SDK para PHP.

Temas

- Creación de la firma RSA SHA-1
- Creación de una política predefinida
- Crear una política personalizada
- Ejemplo de código completo

En las siguientes secciones, se desglosa el ejemplo de código en partes individuales. A continuación, puede encontrar Ejemplo de código completo.

Creación de la firma RSA SHA-1

Este ejemplo de código hace lo siguiente:

- La función `rsa_sha1_sign` proporciona hashes y firma la instrucción de política. Los argumentos requeridos son una instrucción de política y la clave privada que corresponde a una clave pública que está en un grupo de claves de confianza para la distribución.
- A continuación, la función `url_safe_base64_encode` crea una versión de la firma de URL segura.

```
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);
}
```

El siguiente fragmento de código utiliza las funciones `get_canned_policy_stream_name()` y `get_custom_policy_stream_name()` para crear una política predefinida y personalizada. CloudFront utiliza las políticas para crear la URL para el streaming del video, incluida la especificación de la hora de vencimiento.

A continuación, puede utilizar una política predefinida o una política personalizada para determinar cómo administrar el acceso a su contenido. Para obtener información sobre cuál elegir, consulte la sección Decisión de utilizar políticas predefinidas o personalizadas para URL firmadas.

Creación de una política predefinida

El siguiente código de ejemplo crea una instrucción de política predefinida para la firma.

> **Note**
>
> La variable `$expires` es una marca temporal fecha/hora que debe ser un número entero, no una cadena.

```
function get_canned_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $expires) {
    // this policy is well known by CloudFront, but you still need to sign it, since it
 contains your parameters
    $canned_policy = '{"Statement":[{"Resource":"' . $video_path . '","Condition":
{"DateLessThan":{"AWS:EpochTime":'. $expires . '}}}]}';
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($canned_policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($canned_policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, null, $encoded_signature,
 $key_pair_id, $expires);
    // URL-encode the query string characters
    return $stream_name;
}
```

Para obtener más información acerca de políticas predefinidas, consulte Creación de una URL firmada mediante una política predefinida.

Crear una política personalizada

El siguiente código de ejemplo crea una instrucción de política personalizada para la firma.

```
function get_custom_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $policy) {
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    // make the signature safe to be included in a URL
```

```
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, $encoded_policy, $encoded_signature,
 $key_pair_id, null);
    // URL-encode the query string characters
    return $stream_name;
}
```

Para obtener más información acerca de políticas personalizadas, consulte Creación de una URL firmada mediante una política personalizada.

Ejemplo de código completo

El siguiente código de muestra proporciona una demostración completa de la creación de URL firmadas de CloudFront con PHP. Puede descargar el ejemplo completo desde el archivo demo-php.zip.

En el siguiente ejemplo, puede modificar el elemento `$policy` de `Condition` para permitir los rangos de direcciones IPv4 () e IPv6. Para ver un ejemplo, consulte Uso de direcciones IPv6 en políticas de IAM en la Guía del usuario de Amazon Simple Storage Service.

```
<?php

function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";

    // load the private key
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);

    // compute signature
    openssl_sign($policy, $signature, $pkeyid);

    // free the key from memory
    openssl_free_key($pkeyid);

    return $signature;
}

function url_safe_base64_encode($value) {
```

```
    $encoded = base64_encode($value);
    // replace unsafe characters +, = and / with the safe characters -, _ and ~
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}

function create_stream_name($stream, $policy, $signature, $key_pair_id, $expires) {
    $result = $stream;
    // if the stream already contains query parameters, attach the new query parameters
 to the end
    // otherwise, add the query parameters
    $separator = strpos($stream, '?') == FALSE ? '?' : '&';
    // the presence of an expires time means we're using a canned policy
    if($expires) {
        $result .= $separator . "Expires=" . $expires . "&Signature=" . $signature .
 "&Key-Pair-Id=" . $key_pair_id;
    }
    // not using a canned policy, include the policy itself in the stream name
    else {
        $result .= $separator . "Policy=" . $policy . "&Signature=" . $signature .
 "&Key-Pair-Id=" . $key_pair_id;
    }

    // new lines would break us, so remove them
    return str_replace('\n', '', $result);
}


function get_canned_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $expires) {
    // this policy is well known by CloudFront, but you still need to sign it, since it
 contains your parameters
    $canned_policy = '{"Statement":[{"Resource":"' . $video_path . '","Condition":
{"DateLessThan":{"AWS:EpochTime":'. $expires . '}}}]}';
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($canned_policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($canned_policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);
```

```
    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, null, $encoded_signature,
 $key_pair_id, $expires);
    // URL-encode the query string characters
    return $stream_name;
}

function get_custom_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $policy) {
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, $encoded_policy, $encoded_signature,
 $key_pair_id, null);
    // URL-encode the query string characters
    return $stream_name;
}


// Path to your private key.  Be very careful that this file is not accessible
// from the web!

$private_key_filename = '/home/test/secure/example-priv-key.pem';
$key_pair_id = 'K2JCJMDEHXQW5F';

// Make sure you have "Restrict viewer access" enabled on this path behaviour and using
 the above Trusted key groups (recommended).
$video_path = 'https://example.com/secure/example.mp4';

$expires = time() + 300; // 5 min from now
$canned_policy_stream_name = get_canned_policy_stream_name($video_path,
 $private_key_filename, $key_pair_id, $expires);

// Get the viewer real IP from the x-forward-for header as $_SERVER['REMOTE_ADDR']
 will return viewer facing IP. An alternative option is to use CloudFront-Viewer-
Address header. Note that this header is a trusted CloudFront immutable header. Example
 format: IP:PORT ("CloudFront-Viewer-Address": "1.2.3.4:12345")
$client_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
```

```
$policy =
'{'.
    '"Statement":['.
        '{'.
            '"Resource":"'. $video_path . '",'.
            '"Condition":{'.
                '"IpAddress":{"AWS:SourceIp":"' . $client_ip . '/32"},'.
                '"DateLessThan":{"AWS:EpochTime":' . $expires . '}'.
            '}'.
        '}'.
    ']' .
    '}';
$custom_policy_stream_name = get_custom_policy_stream_name($video_path,
 $private_key_filename, $key_pair_id, $policy);

?>

<html>

<head>
    <title>CloudFront</title>
</head>

<body>
    <h1>Amazon CloudFront</h1>
    <h2>Canned Policy</h2>
    <h3>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?></h3>
    <br />

    <div id='canned'>The canned policy video will be here: <br>

        <video width="640" height="360" autoplay muted controls>
        <source src="<?php echo $canned_policy_stream_name; ?>" type="video/mp4">
        Your browser does not support the video tag.
        </video>
    </div>

    <h2>Custom Policy</h2>
    <h3>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?> only viewable by IP
 <?php echo $client_ip; ?></h3>
    <div id='custom'>The custom policy video will be here: <br>

         <video width="640" height="360" autoplay muted controls>
         <source src="<?php echo $custom_policy_stream_name; ?>" type="video/mp4">
```

```
        Your browser does not support the video tag.
       </video>
    </div>

</body>

</html>
```

Para obtener ejemplos adicionales de firmas de URL, consulte los siguientes temas:

- Crear una firma de URL con Perl
- Crear una firma de URL mediante C# y .NET Framework
- Crear una firma de URL con Java

En lugar de utilizar URL firmadas para crear la firma, puede utilizar cookies firmadas. Para obtener más información, consulte Create signed cookies using PHP.

Crear una firma de URL mediante C# y .NET Framework

Los ejemplos de C# de esta sección implementan una aplicación de ejemplo que muestra cómo crear las firmas para distribuciones privadas de CloudFront mediante instrucciones de políticas predefinidas y personalizadas. Los ejemplos incluyen funciones de utilidad basadas en el AWS SDK para .NET que pueden resultar útiles en aplicaciones .NET.

También puede crear URL firmadas y cookies firmadas mediante SDK para .NET. En la Referencia de la API SDK para .NET, consulte los siguientes temas:

- URL firmadas: AmazonCloudFrontUrlSigner
- Cookies firmadas: AmazonCloudFrontCookieSigner

Para descargar el código, diríjase a Código de firma en C#.

> **Notas**
>
> - Las clases `AmazonCloudFrontUrlSigner` y `AmazonCloudFrontCookieSigner` se han trasladado a un paquete independiente. Para obtener más información sobre su uso, consulte CookieSigner and UrlSigner en la Guía para desarrolladores de AWS SDK para .NET (V4).

- Crear una firma de URL es solo una parte del proceso de entrega de contenido privado mediante una URL firmada. Para obtener más información, consulte Uso de URL firmadas. Para obtener más información sobre el uso de cookies firmadas, consulte Uso de cookies firmadas.

Uso de una clave RSA en .NET Framework

Para utilizar una clave RSA en .NET Framework, debe convertir el archivo.pem suministrado por AWS al formato XML que utiliza el .NET Framework.

Después de la conversión, el archivo de clave privada RSA estará en el siguiente formato:

Example Clave privada RSA en formato XML de .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>
```

Método de firma de políticas predefinidas en C#

El siguiente código C# crea una URL firmada que utiliza una política predefinida siguiendo los pasos que se indican a continuación:

- Crea una instrucción de política.
- La instrucción de política aplica la función hash mediante SHA1 y firma el resultado con RSA y la clave privada cuya clave pública correspondiente se encuentra en un grupo de claves de confianza.
- Codifica con base64 la instrucción de política a la que se le ha aplicado una función hash y firmada y sustituye caracteres especiales para que la cadena se pueda usar tranquilamente como parámetro de solicitud de URL.
- Encadena los valores.

Para ver la implementación completa, consulte el ejemplo disponible en Código de firma en C#.

> **Note**
>
> Se devuelve `keyId` al cargar una clave pública a CloudFront. Para obtener más información, consulte
>
> 6 &Key-Pair-Id.

Example: método de firma de políticas predefinidas en C#

```
public static string ToUrlSafeBase64String(byte[] bytes)
{
    return System.Convert.ToBase64String(bytes)
        .Replace('+', '-')
        .Replace('=', '_')
        .Replace('/', '~');
}
```

```
public static string CreateCannedPrivateURL(string urlString,
    string durationUnits, string durationNumber, string pathToPolicyStmnt,
    string pathToPrivateKey, string keyId)
{
    // args[] 0-thisMethod, 1-resourceUrl, 2-seconds-minutes-hours-days
    // to expiration, 3-numberOfPreviousUnits, 4-pathToPolicyStmnt,
    // 5-pathToPrivateKey, 6-keyId

    TimeSpan timeSpanInterval = GetDuration(durationUnits, durationNumber);

    // Create the policy statement.
    string strPolicy = CreatePolicyStatement(pathToPolicyStmnt,
        urlString,
        DateTime.Now,
        DateTime.Now.Add(timeSpanInterval),
        "0.0.0.0/0");
    if ("Error!" == strPolicy) return "Invalid time frame." +
        "Start time cannot be greater than end time.";

    // Copy the expiration time defined by policy statement.
    string strExpiration = CopyExpirationTimeFromPolicy(strPolicy);

    // Read the policy into a byte buffer.
    byte[] bufferPolicy = Encoding.ASCII.GetBytes(strPolicy);

    // Initialize the SHA1CryptoServiceProvider object and hash the policy data.
    using (SHA1CryptoServiceProvider
        cryptoSHA1 = new SHA1CryptoServiceProvider())
    {
        bufferPolicy = cryptoSHA1.ComputeHash(bufferPolicy);

        // Initialize the RSACryptoServiceProvider object.
        RSACryptoServiceProvider providerRSA = new RSACryptoServiceProvider();
        XmlDocument xmlPrivateKey = new XmlDocument();

        // Load your private key, which you created by converting your
        // .pem file to the XML format that the .NET framework uses.
        // Several tools are available.
        xmlPrivateKey.Load(pathToPrivateKey);

        // Format the RSACryptoServiceProvider providerRSA and
        // create the signature.
        providerRSA.FromXmlString(xmlPrivateKey.InnerXml);
        RSAPKCS1SignatureFormatter rsaFormatter =
```

```
            new RSAPKCS1SignatureFormatter(providerRSA);
        rsaFormatter.SetHashAlgorithm("SHA1");
        byte[] signedPolicyHash = rsaFormatter.CreateSignature(bufferPolicy);

        // Convert the signed policy to URL-safe base64 encoding and
        // replace unsafe characters + = / with the safe characters - _ ~
        string strSignedPolicy = ToUrlSafeBase64String(signedPolicyHash);

        // Concatenate the URL, the timestamp, the signature,
        // and the key pair ID to form the signed URL.
        return urlString +
            "?Expires=" +
            strExpiration +
            "&Signature=" +
            strSignedPolicy +
            "&Key-Pair-Id=" +
            keyId;
    }
}
```

Método de firma de políticas personalizadas en C#

El siguiente código C# crea una URL firmada que utiliza una política personalizada siguiendo los pasos que se indican a continuación:

1. Crea una instrucción de política.
2. Codifica con base64 la instrucción de política y sustituye caracteres especiales para que la cadena se pueda usar tranquilamente como parámetro de solicitud de URL.
3. La instrucción de política aplica la función hash mediante SHA1 y cifra el resultado mediante RSA y la clave privada cuya clave pública correspondiente se encuentra en un grupo de claves de confianza.
4. Codifica con base64 la instrucción de política a la que se le ha aplicado una función hash y sustituye caracteres especiales para que la cadena se pueda usar tranquilamente como parámetro de solicitud de URL.
5. Encadena los valores.

Para ver la implementación completa, consulte el ejemplo disponible en Código de firma en C#.

> **Note**
>
> Se devuelve `keyId` al cargar una clave pública a CloudFront. Para obtener más información, consulte
>
> 6 &Key-Pair-Id.

Example: método de firma de políticas personalizadas en C#

```
public static string ToUrlSafeBase64String(byte[] bytes)
{
    return System.Convert.ToBase64String(bytes)
        .Replace('+', '-')
        .Replace('=', '_')
        .Replace('/', '~');
}

public static string CreateCustomPrivateURL(string urlString,
    string durationUnits, string durationNumber, string startIntervalFromNow,
    string ipaddress, string pathToPolicyStmnt, string pathToPrivateKey,
    string keyId)
{
    // args[] 0-thisMethod, 1-resourceUrl, 2-seconds-minutes-hours-days
    // to expiration, 3-numberOfPreviousUnits, 4-starttimeFromNow,
    // 5-ip_address, 6-pathToPolicyStmt, 7-pathToPrivateKey, 8-keyId

    TimeSpan timeSpanInterval = GetDuration(durationUnits, durationNumber);
    TimeSpan timeSpanToStart = GetDurationByUnits(durationUnits,
        startIntervalFromNow);
    if (null == timeSpanToStart)
        return "Invalid duration units." +
            "Valid options: seconds, minutes, hours, or days";

    string strPolicy = CreatePolicyStatement(
        pathToPolicyStmnt, urlString, DateTime.Now.Add(timeSpanToStart),
        DateTime.Now.Add(timeSpanInterval), ipaddress);

    // Read the policy into a byte buffer.
    byte[] bufferPolicy = Encoding.ASCII.GetBytes(strPolicy);

    // Convert the policy statement to URL-safe base64 encoding and
```

```
    // replace unsafe characters + = / with the safe characters - _ ~

    string urlSafePolicy = ToUrlSafeBase64String(bufferPolicy);

    // Initialize the SHA1CryptoServiceProvider object and hash the policy data.
    byte[] bufferPolicyHash;
    using (SHA1CryptoServiceProvider cryptoSHA1 =
        new SHA1CryptoServiceProvider())
    {
        bufferPolicyHash = cryptoSHA1.ComputeHash(bufferPolicy);

        // Initialize the RSACryptoServiceProvider object.
        RSACryptoServiceProvider providerRSA = new RSACryptoServiceProvider();
        XmlDocument xmlPrivateKey = new XmlDocument();

        // Load your private key, which you created by converting your
        // .pem file to the XML format that the .NET framework uses.
        // Several tools are available.
        xmlPrivateKey.Load(pathToPrivateKey);

        // Format the RSACryptoServiceProvider providerRSA
        // and create the signature.
        providerRSA.FromXmlString(xmlPrivateKey.InnerXml);
        RSAPKCS1SignatureFormatter RSAFormatter =
            new RSAPKCS1SignatureFormatter(providerRSA);
        RSAFormatter.SetHashAlgorithm("SHA1");
        byte[] signedHash = RSAFormatter.CreateSignature(bufferPolicyHash);

        // Convert the signed policy to URL-safe base64 encoding and
        // replace unsafe characters + = / with the safe characters - _ ~
        string strSignedPolicy = ToUrlSafeBase64String(signedHash);

        return urlString +
            "?Policy=" +
            urlSafePolicy +
            "&Signature=" +
            strSignedPolicy +
            "&Key-Pair-Id=" +
            keyId;
    }
}
```

Métodos de utilidades para generar firmas

Los siguientes métodos obtienen la instrucción de política de un archivo y analizan intervalos de tiempo para generar firmas.

Example: métodos de utilidades para generar firmas

```
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();
}
```

Véase también

- Crear una firma de URL con Perl
- Crear una firma de URL con PHP
- Crear una firma de URL con Java

Crear una firma de URL con Java

Además del siguiente ejemplo de código, puede utilizar la clase de utilidad `CloudFrontUrlSigner` de AWS SDK para Java (versión 1) para crear URL firmadas de CloudFront.

Para ver más ejemplos, consulte Create signed URLs and cookies using an AWS SDK en la biblioteca de códigos de ejemplos de códigos de AWS SDK.

> **Note**
>
> La creación de una URL firmada es solo una parte del proceso de entrega de contenido privado con CloudFront. Para obtener más información acerca de todo el proceso, consulte Uso de URL firmadas.

En el ejemplo siguiente se muestra cómo crear una URL firmada de CloudFront.

Example Política de Java y métodos de cifrado de firma

```
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);

    }
}
```

Véase también:

- Crear una firma de URL con Perl
- Crear una firma de URL con PHP
- Crear una firma de URL mediante C# y .NET Framework

Restricción del acceso a un origen de AWS

Puede configurar CloudFront y algunos orígenes de AWS de forma que se obtengan los siguientes beneficios:

- Restringe el acceso al origen de AWS para que no sea accesible al público.
- Se asegura de que los espectadores (usuarios) puedan acceder al contenido en el origen de AWS solo a través de la distribución de CloudFront especificada. Esto impide que los espectadores accedan al contenido directamente desde el origen o a través de una distribución no deseada de CloudFront.

Para ello, configure CloudFront para que envíe solicitudes autenticadas al origen de AWS y configure el origen de AWS para que solo permita el acceso a las solicitudes autenticadas de CloudFront. Para obtener más información, consulte los siguientes temas para ver los tipos de orígenes de AWS compatibles.

Temas

- Restricción del acceso a un origen de AWS Elemental MediaPackage v2
- Restricción del acceso a un origen de AWS Elemental MediaStore
- Restricción del acceso a un origen de URL de función de AWS Lambda
- Restricción del acceso a un origen de Amazon S3
- Restricción del acceso con orígenes de la VPC

Restricción del acceso a un origen de AWS Elemental MediaPackage v2

CloudFront proporciona control de acceso de origen (OAC) para restringir el acceso a un origen de MediaPackage v2.

> **Note**
>
> CloudFront OAC solo admite MediaPackage v2. MediaPackage v1 no se admite.

Temas

- Creación de un nuevo OAC
- Configuración avanzada para el control de acceso de origen

Creación de un nuevo OAC

Complete los pasos que se describen en los siguientes temas para configurar un nuevo OAC en CloudFront.

Temas

- Requisitos previos
- Concesión del permiso de CloudFront para acceder al origen de MediaPackage v2
- Creación del OAC

Requisitos previos

Antes de crear y configurar el OAC, debe tener una distribución de CloudFront con un origen de MediaPackage v2. Para obtener más información, consulte Uso de un contenedor de MediaStore o un canal de MediaPackage.

Concesión del permiso de CloudFront para acceder al origen de MediaPackage v2

Antes de crear un OAC o configurarlo en una distribución de CloudFront, asegúrese de que CloudFront tiene permiso para acceder al origen de MediaPackage v2. Realice esta acción después de crear una distribución de CloudFront, pero antes de agregar el OAC al origen de MediaPackage v2 en la configuración de distribución.

Utilice una política de IAM para permitir que la entidad principal del servicio de CloudFront (`cloudfront.amazonaws.com`) acceda al origen. Utilice un elemento `Condition` en la política para permitir que CloudFront acceda al origen de MediaPackage v2 solo cuando la solicitud sea en nombre de la distribución de CloudFront que contiene el origen de MediaPackage v2. Esta es la distribución con el origen de MediaPackage v2 a la que desea agregar OAC.

Example: política de IAM que permite el acceso de solo lectura a una distribución de CloudFront con OAC habilitado

La siguiente política permite que la distribución de CloudFront (*`E1PDK09ESKHJWT`*) acceda al origen de MediaPackage v2. El origen es el ARN especificado para el elemento `Resource`.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {"Service": "cloudfront.amazonaws.com"},
            "Action": "mediapackagev2:GetObject",
            "Resource": "arn:aws:mediapackagev2:us-
east-1:123456789012:channelGroup/channel-group-name/channel/channel-name/
originEndpoint/origin_endpoint_name",
            "Condition": {
                "StringEquals": {"AWS:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT"}
            }
        }
    ]
}
```

Notas

- Si ha activado la característica MQAR y el control de acceso de origen (OAC), agregue la acción `mediapackagev2:GetHeadObject` a la política de IAM. MQAR requiere este permiso para enviar solicitudes `HEAD` al origen de MediaPackage v2. Para obtener más información acerca de MQAR, consulte Resiliencia basada en la calidad multimedia.
- Si crea una distribución que no tiene permiso para el origen de MediaPackage v2, puede elegir Copiar política en la consola de CloudFront y, a continuación, elegir Actualizar permisos de punto de conexión. Después, puede adjuntar el permiso copiado al dispositivo de punto de conexión. Para obtener más información, consulte Endpoint policy fields en la Guía del usuario de AWS Elemental MediaPackage.

Creación del OAC

Para crear un OAC, puede utilizar la Consola de administración de AWS, CloudFormation, la AWS CLI o la API de CloudFront.

Console

Creación de un OAC

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Origin access (Acceso de origen).
3. Elija Crear configuración de control.
4. En el formulario Crear nuevo OAC, haga lo siguiente:
   a. Indique un Nombre y, opcionalmente, una Descripción para el OAC.
   b. En el panel Configuración, le recomendamos que deje la predeterminada, Firmar solicitudes (recomendado). Para obtener más información, consulte the section called "Configuración avanzada para el control de acceso de origen".
5. Para Tipo de origen, elija MediaPackage V2.
6. Seleccione Crear.

> **Tip**
> Después de crear el OAC, anote el Nombre. Lo necesita en el siguiente procedimiento.

Cómo agregar un OAC a un origen de MediaPackage v2 en una distribución

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija una distribución con un origen de MediaPackage V2 a la que desee agregar el OAC y, a continuación, elija la pestaña Orígenes.
3. Seleccione el origen de MediaPackage v2 al que desea agregar el OAC y, a continuación, elija Editar.
4. Seleccione Solo HTTP para el Protocolo de origen.
5. En el menú desplegable Control de acceso de origen, elija el nombre de OAC que desee utilizar.
6. Seleccione Save changes (Guardar cambios).

La distribución comienza a implementarse en todas las ubicaciones periféricas de CloudFront. Cuando una ubicación periférica recibe la nueva configuración, firma todas las solicitudes que envía al origen de MediaPackage v2.

CloudFormation

Para crear un OAC con CloudFormation, utilice el tipo de recurso `AWS::CloudFront::OriginAccessControl`. En el siguiente ejemplo se muestra la sintaxis de plantilla de CloudFormation, en formato YAML, para crear 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
```

Para obtener más información, consulte AWS::CloudFront::OriginAccessControl en la Guía del usuario de AWS CloudFormation.

CLI

Para crear un control de acceso de origen con la AWS Command Line Interface (AWS CLI), utilice el comando aws cloudfront create-origin-access-control. Puede utilizar un archivo de entrada para proporcionar los parámetros de entrada del comando, en lugar de especificar cada parámetro individual como entrada de la línea de comandos.

Para crear un control de acceso de origen (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo llamado `origin-access-control.yaml`. Este archivo contiene todos los parámetros de entrada para el comando create-origin-access-control.

   ```
   aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
    origin-access-control.yaml
   ```

2. Abra el archivo `origin-access-control.yaml` que acaba de crear. Edite el archivo para agregar un nombre para el OAC, una descripción (opcional) y cambie `SigningBehavior` por `always`. A continuación, guarde el archivo.

Para obtener información sobre otras configuraciones de OAC, consulte the section called "Configuración avanzada para el control de acceso de origen".

3. Utilice el siguiente comando para crear el control de acceso de origen mediante los parámetros de entrada del archivo `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

Anote el valor de `Id` en la salida del comando. Lo necesita para agregar el OAC a un origen de MediaPackage v2 en una distribución de CloudFront.

Cómo adjuntar un OAC a un origen de MediaPackage v2 en una distribución existente (CLI con archivo de entrada)

1. Utilice el comando siguiente para guardar la configuración de distribución de la distribución de CloudFront a la que desea agregar el OAC. La distribución debe tener un origen de MediaPackage v2.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Abra el archivo llamado `dist-config.yaml` que acaba de crear. Edite el archivo y realice los siguientes cambios:

   - En el objeto `Origins`, agregue el ID de OAC al campo que se llama `OriginAccessControlId`.
   - Elimine el valor del campo que se llama `OriginAccessIdentity`, si existe.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución y utilizar el control de acceso de origen.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribución comienza a implementarse en todas las ubicaciones periféricas de CloudFront. Cuando una ubicación periférica recibe la nueva configuración, firma todas las solicitudes que envía al origen de MediaPackage v2.

API

Para crear un OAC con la API de CloudFront, utilice CreateOriginAccessControl. Para obtener más información sobre los campos que especifique en esta llamada a la API, consulte la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Después de crear un OAC, puede adjuntarlo a un origen de MediaPackage v2 en una distribución, mediante una de las siguientes llamadas a la API:

- Para asociarlo a una distribución existente, utilice UpdateDistribution.
- Para asociarlo a una nueva distribución, utilice CreateDistribution.

Para estas dos llamadas a la API, proporcione el ID de OAC en el campo `OriginAccessControlId`, dentro de un origen. Para obtener más información sobre los otros campos que especifique en estas llamadas a la API, consulte Referencia de toda la configuración de distribución y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Configuración avanzada para el control de acceso de origen

La característica de OAC de CloudFront incluye configuraciones avanzadas que están pensadas solo para casos de uso específicos. Utilice la configuración recomendada a menos que tenga una necesidad específica de la configuración avanzada.

El OAC contiene una configuración denominada Comportamiento de firma (en la consola) o `SigningBehavior` (en la API, CLI y CloudFormation). Esta configuración proporciona las siguientes opciones:

Firmar siempre las solicitudes de origen (configuración recomendada)

Recomendamos utilizar esta configuración, denominada Firmar solicitudes (recomendado) en la consola o `always` en la API, la CLI y CloudFormation. Con esta configuración, CloudFront siempre firma todas las solicitudes que envía al origen de MediaPackage v2.

Nunca firmar solicitudes de origen

Esta configuración se denomina No firmar solicitudes en la consola o `never` en la API, la CLI y CloudFormation. Utilice esta configuración con el fin de desactivar el OAC para todos los orígenes en todas las distribuciones que utilizan este OAC. Esto puede ahorrar tiempo y esfuerzo en comparación con la eliminación de un OAC de todos los orígenes y distribuciones que lo utilizan, uno por uno. Con esta configuración, CloudFront no firma las solicitudes que envía al origen de MediaPackage v2.

> **Warning**
>
> Para utilizar esta configuración, el origen de MediaPackage v2 debe ser de acceso público. Si utiliza esta configuración con un origen de MediaPackage v2 que no es de acceso público, CloudFront no podrá acceder al origen. El origen de MediaPackage v2 devuelve errores a CloudFront y CloudFront pasa esos errores a los lectores. Para obtener más información, consulte el ejemplo de política de MediaPackage v2 para Policies and Permissions in MediaPackage en la Guía del usuario de AWS Elemental MediaPackage.

No anular el encabezado **`Authorization`** del lector (cliente)

Esta configuración se denomina Do not override authorization header (No anular el encabezado authorization en la consola o `no-override` en la API, la CLI y CloudFormation. Utilice esta configuración cuando desee que CloudFront firme las solicitudes de origen solo cuando la solicitud del lector correspondiente no incluya un encabezado `Authorization`. Con esta configuración, CloudFront pasa el encabezado `Authorization` de la solicitud del lector cuando hay uno, pero firma la solicitud de origen (agrega su propio encabezado `Authorization`) cuando la solicitud del lector no incluye un encabezado `Authorization`.

> **Warning**
>
> Para pasar el encabezado `Authorization` de la solicitud del lector, debe agregar el encabezado `Authorization` a una política de caché para todos los comportamientos

de caché que utilizan los orígenes de MediaPackage v2 asociados con este control de acceso de origen.

Restricción del acceso a un origen de AWS Elemental MediaStore

CloudFront proporciona un control de acceso de origen (OAC) para restringir el acceso a un origen de AWS Elemental MediaStore.

Temas

- Creación de un nuevo control de acceso de origen
- Configuración avanzada para el control de acceso de origen

Creación de un nuevo control de acceso de origen

Complete los pasos que se describen en los siguientes temas para configurar un nuevo control de acceso de origen en CloudFront.

Temas

- Requisitos previos
- Concesión del permiso de CloudFront para acceder al origen de MediaStore
- Creación del control de acceso de origen

Requisitos previos

Antes de crear y configurar el control de acceso de origen (OAC), debe tener una distribución de CloudFront con un origen de MediaStore.

Concesión del permiso de CloudFront para acceder al origen de MediaStore

Antes de crear un control de acceso de origen o configurarlo en una distribución de CloudFront, asegúrese de que CloudFront tiene permiso para acceder al origen de MediaStore. Realice esta acción después de crear una distribución de CloudFront, pero antes de agregar el OAC al origen de MediaStore en la configuración de distribución.

Utilice una política de contenedor de MediaStore para permitir que la entidad principal del servicio de CloudFront (`cloudfront.amazonaws.com`) acceda al origen. Utilice un elemento `Condition` en

la política para permitir que CloudFront acceda al contenedor de MediaStore solo cuando la solicitud sea en nombre de la distribución de CloudFront que contiene el origen de MediaStore. Esta es la distribución con el origen de MediaStore al que desea agregar OAC.

A continuación, se muestran ejemplos de políticas de contenedor de MediaStore que permiten a una distribución de CloudFront acceder a un origen de MediaStore.

Example Política de contenedor de MediaStore que permite el acceso de solo lectura a una distribución de CloudFront con OAC habilitado

JSON

```
{
        "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipalReadOnly",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject"
                ],
                "Resource": "arn:aws:mediastore:us-
east-1:111122223333:container/<container name>/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

Example Política de contenedor de MediaStore que permite el acceso de lectura y escritura a una distribución de CloudFront con OAC habilitado

JSON

```
{
        "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipalReadWrite",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject",
                  "mediastore:PutObject"
                ],
                "Resource": "arn:aws:mediastore:us-
east-1:111122223333:container/container-name/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

> **Note**
>
> Para permitir el acceso de escritura, debe configurar los Allowed HTTP methods (Métodos HTTP permitidos) para incluir PUT en la configuración de comportamiento de la distribución de CloudFront.

Creación del control de acceso de origen

Para crear un OAC, puede utilizar Consola de administración de AWS, CloudFormation, AWS CLI o la API de CloudFront.

Console

Para crear un control de acceso de origen

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Origin access (Acceso de origen).
3. Elija Create control setting (Crear configuración de control).
4. En el formulario Create control setting (Crear configuración de control), haga lo siguiente:
   a. En el panel Details (Detalles), ingrese un valor para Name (Nombre) y (opcionalmente) para Description (Descripción) para el control de acceso de origen.
   b. En el panel Settings (Configuración), le recomendamos que deje la configuración predeterminada Sign requests (recommended) (Firmar solicitudes [recomendado]). Para obtener más información, consulte the section called “Configuración avanzada para el control de acceso de origen”.
5. Elija MediaStore en el menú desplegable de Origin type (Tipo de origen).
6. Seleccione Crear.

   Una vez creado el OAC, anote el valor de Name (Nombre). Lo necesita en el siguiente procedimiento.

Para agregar un control de acceso de origen a un origen de MediaStore en una distribución

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija una distribución con un origen de MediaStore a la que desee agregar el OAC y, a continuación, elija la pestaña Origins (Orígenes).
3. Seleccione el origen de MediaStore al que desea agregar el OAC y, a continuación, elija Edit (Editar).
4. Seleccione HTTPS only (Solo HTTP) para el Protocol (Protocolo) de origen.
5. En el menú desplegable Origin access control (Control de acceso de origen), elija el OAC que desee utilizar.

6. Seleccione Save changes (Guardar cambios).

La distribución comienza a implementarse en todas las ubicaciones periféricas de CloudFront. Cuando una ubicación periférica recibe la nueva configuración, firma todas las solicitudes que envía al origen de bucket de MediaStore.

CloudFormation

Para crear un control de acceso de origen (OAC) con CloudFormation, utilice el tipo de recurso `AWS::CloudFront::OriginAccessControl`. El siguiente ejemplo se muestra la sintaxis de plantilla de CloudFormation, en formato YAML, para crear un control de acceso de origen.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: mediastore
      SigningBehavior: always
      SigningProtocol: sigv4
```

Para obtener más información, consulte AWS::CloudFront::OriginAccessControl en la Guía del usuario de AWS CloudFormation.

CLI

Para crear un control de acceso de origen con la AWS Command Line Interface (AWS CLI), utilice el comando aws cloudfront create-origin-access-control. Puede utilizar un archivo de entrada para proporcionar los parámetros de entrada del comando, en lugar de especificar cada parámetro individual como entrada de la línea de comandos.

Para crear un control de acceso de origen (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo llamado `origin-access-control.yaml`. Este archivo contiene todos los parámetros de entrada para el comando create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Abra el archivo `origin-access-control.yaml` que acaba de crear. Edite el archivo para agregar un nombre para el OAC, una descripción (opcional) y cambie `SigningBehavior` por `always`. A continuación, guarde el archivo.

   Para obtener información sobre otras configuraciones de OAC, consulte the section called "Configuración avanzada para el control de acceso de origen".

3. Utilice el siguiente comando para crear el control de acceso de origen mediante los parámetros de entrada del archivo `origin-access-control.yaml`.

   ```
   aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
   access-control.yaml
   ```

   Anote el valor de `Id` en la salida del comando. Lo necesita para agregar el OAC a un origen de MediaStore en una distribución de CloudFront.

Para adjuntar un OAC a un origen de MediaStore en una distribución existente (CLI con archivo de entrada)

1. Utilice el comando siguiente para guardar la configuración de distribución de la distribución de CloudFront a la que desea agregar el OAC. La distribución debe tener un origen de MediaStore.

   ```
   aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
   output yaml > dist-config.yaml
   ```

2. Abra el archivo llamado `dist-config.yaml` que acaba de crear. Edite el archivo y realice los siguientes cambios:

   - En el objeto `Origins`, agregue el ID de OAC al campo que se llama `OriginAccessControlId`.
   - Elimine el valor del campo que se llama `OriginAccessIdentity`, si existe.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución y utilizar el control de acceso de origen.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribución comienza a implementarse en todas las ubicaciones periféricas de CloudFront. Cuando una ubicación periférica recibe la nueva configuración, firma todas las solicitudes que envía al origen de MediaStore.

API

Para crear un control de acceso de origen con la API de CloudFront, utilice CreateOriginAccessControl. Para obtener más información sobre los campos que especifique en esta llamada a la API, consulte la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Después de crear un control de acceso de origen, puede adjuntarlo a un origen de MediaStore en una distribución, mediante una de las siguientes llamadas a la API:

- Para asociarlo a una distribución existente, utilice UpdateDistribution.
- Para asociarlo a una nueva distribución, utilice CreateDistribution.

Para estas dos llamadas a la API, proporcione el ID de control de acceso de origen en el campo `OriginAccessControlId`, dentro de un origen. Para obtener más información sobre los otros campos que especifique en estas llamadas a la API, consulte Referencia de toda la configuración de distribución y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Configuración avanzada para el control de acceso de origen

La característica de control de acceso de origen de CloudFront incluye configuraciones avanzadas que están pensadas solo para casos de uso específicos. Utilice la configuración recomendada a menos que tenga una necesidad específica de la configuración avanzada.

El control de acceso de origen contiene una configuración denominada Signing behavior (Comportamiento de firma) (en la consola) o `SigningBehavior` (en la API, CLI y CloudFormation). Esta configuración proporciona las siguientes opciones:

Firmar siempre las solicitudes de origen (configuración recomendada)

Recomendamos utilizar esta configuración, denominada Firmar solicitudes (recomendado) en la consola o `always` en la API, la CLI y CloudFormation. Con esta configuración, CloudFront siempre firma todas las solicitudes que envía al origen de MediaStore.

Nunca firmar solicitudes de origen

Esta configuración se denomina Do not sign requests (No firmar solicitudes) en la consola o `never` en la API, la CLI y CloudFormation. Utilice esta configuración para desactivar el control de acceso de origen para todos los orígenes en todas las distribuciones que utilizan este control de acceso de origen. Esto puede ahorrar tiempo y esfuerzo en comparación con la eliminación de un control de acceso de origen de todos los orígenes y distribuciones que lo utilizan, uno por uno. Con esta configuración, CloudFront no firma las solicitudes que envía al origen de MediaStore.

> **Warning**
>
> Para utilizar esta configuración, el origen de MediaStore debe ser de acceso público. Si utiliza esta configuración con un origen de MediaStore que no es de acceso público, CloudFront no podrá acceder al origen. El origen de MediaStore devuelve errores a CloudFront y CloudFront pasa esos errores a los lectores. Para obtener más información, consulte el ejemplo de política de contenedores de MediaStore para el acceso público de lectura a través de HTTPS.

No anular el encabezado **`Authorization`** del lector (cliente)

Esta configuración se denomina Do not override authorization header (No anular el encabezado authorization en la consola o `no-override` en la API, la CLI y CloudFormation. Utilice esta configuración cuando desee que CloudFront firme las solicitudes de origen solo cuando la solicitud del lector correspondiente no incluya un encabezado `Authorization`. Con esta configuración, CloudFront pasa el encabezado `Authorization` de la solicitud del lector cuando hay uno, pero firma la solicitud de origen (agrega su propio encabezado `Authorization`) cuando la solicitud del lector no incluye un encabezado `Authorization`.

> **Warning**
>
> Para pasar el encabezado `Authorization` de la solicitud del lector, debe agregar el encabezado `Authorization` a una política de caché para todos los comportamientos de caché que utilizan los orígenes de MediaStore asociados con este control de acceso de origen.

Restricción del acceso a un origen de URL de función de AWS Lambda

CloudFront proporciona un control de acceso de origen (OAC) para restringir el acceso a un origen de URL de función de Lambda.

Temas

- Creación de un nuevo OAC
- Configuración avanzada para el control de acceso de origen
- Código de plantilla de ejemplo

Creación de un nuevo OAC

Complete los pasos que se describen en los siguientes temas para configurar un nuevo OAC en CloudFront.

> **Important**
>
> Si utiliza los métodos `PUT` o `POST` con la URL de función de Lambda, los usuarios deben calcular el SHA256 del cuerpo e incluir el valor del hash de carga útil del cuerpo de la solicitud en el encabezado `x-amz-content-sha256` al enviar la solicitud a CloudFront. Lambda no admite las cargas sin firmar.

Temas

- Requisitos previos
- Concesión de permiso de CloudFront para acceder a la URL de función de Lambda
- Creación del OAC

Requisitos previos

Antes de crear y configurar OAC, debe tener una distribución de CloudFront con una URL de función de Lambda como el origen. Para usar OAC, debe especificar `AWS_IAM` como valor para el parámetro `AuthType`. Para obtener más información, consulte Uso de una URL de función de Lambda.

Concesión de permiso de CloudFront para acceder a la URL de función de Lambda

Antes de crear un OAC o configurarlo en una distribución de CloudFront, asegúrese de que CloudFront tiene permiso para acceder a la URL de función de Lambda. Realice esta acción después de crear una distribución de CloudFront, pero antes de agregar el OAC a la URL de función de Lambda en la configuración de distribución.

> **Note**
>
> Para actualizar la política de IAM para la URL de función de Lambda, debe usar la AWS Command Line Interface (AWS CLI). En este momento, no se admite la edición de la política de IAM en la consola de Lambda.

El siguiente comando de la AWS CLI concede a la entidad principal de servicio de CloudFront (`cloudfront.amazonaws.com`) acceso a la URL de función de Lambda. El elemento `Condition` en la política permite que CloudFront acceda a Lambda solo cuando la solicitud sea en nombre de la distribución de CloudFront que contiene la URL de función de Lambda. Esta es la distribución con el origen de URL de función de Lambda a la que desea agregar OAC.

Example: comando de la AWS CLI para actualizar una política con el fin de permitir el acceso de solo lectura a una distribución de CloudFront con OAC habilitado

Los siguientes comandos de la AWS CLI permiten que la distribución de CloudFront (*`E1PDK09ESKHJWT`*) acceda a su *`FUNCTION_URL_NAME`* de Lambda.

```
aws lambda add-permission \
--statement-id "AllowCloudFrontServicePrincipal" \
--action "lambda:InvokeFunctionUrl" \
--principal "cloudfront.amazonaws.com" \
--source-arn "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT" \
--function-name FUNCTION_URL_NAME
```

```
aws lambda add-permission \
--statement-id "AllowCloudFrontServicePrincipalInvokeFunction" \
--action "lambda:InvokeFunction" \
--principal "cloudfront.amazonaws.com" \
--source-arn "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT" \
--function-name FUNCTION_URL_NAME
```

> **Note**
>
> Si crea una distribución y no tiene permiso para la URL de función de Lambda, puede elegir el comando de copia de la CLI en la consola de CloudFront y, a continuación, introducir este comando desde el terminal de la línea de comandos. Para obtener más información, consulte Concesión de acceso a las funciones a los Servicios de AWS en la Guía para desarrolladores de AWS Lambda.

Creación del OAC

Para crear un OAC, puede utilizar la Consola de administración de AWS, CloudFormation, la AWS CLI o la API de CloudFront.

Console

Creación de un OAC

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Origin access (Acceso de origen).
3. Elija Crear configuración de control.
4. En el formulario Crear nuevo OAC, haga lo siguiente:
   a. Indique un Nombre y, opcionalmente, una Descripción para el OAC.
   b. En el panel Configuración, le recomendamos que deje la predeterminada, Firmar solicitudes (recomendado). Para obtener más información, consulte the section called “Configuración avanzada para el control de acceso de origen”.
5. En Tipo de origen, elija Lambda.
6. Seleccione Crear.

> **Tip**
>
> Después de crear el OAC, anote el Nombre. Lo necesita en el siguiente procedimiento.

Cómo agregar un control de acceso de origen a la URL de una función de Lambda en una distribución

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija una distribución con una URL de función de Lambda a la que desee agregar el OAC y, a continuación, elija la pestaña Orígenes.
3. Seleccione la URL de función de Lambda a la que desea agregar el OAC y, a continuación, elija Editar.
4. Seleccione Solo HTTP para el Protocolo de origen.
5. En el menú desplegable Control de acceso de origen, elija el nombre de OAC que desee utilizar.
6. Seleccione Save changes (Guardar cambios).

La distribución comienza a implementarse en todas las ubicaciones periféricas de CloudFront. Cuando una ubicación periférica recibe la nueva configuración, firma todas las solicitudes que envía a la URL de función de Lambda.

CloudFormation

Para crear un OAC con CloudFormation, utilice el tipo de recurso `AWS::CloudFront::OriginAccessControl`. En el siguiente ejemplo se muestra la sintaxis de plantilla de CloudFormation, en formato YAML, para crear 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
```

Para obtener más información, consulte AWS::CloudFront::OriginAccessControl en la Guía del usuario de AWS CloudFormation.

CLI

Para crear un control de acceso de origen con la AWS Command Line Interface (AWS CLI), utilice el comando aws cloudfront create-origin-access-control. Puede utilizar un archivo de entrada para proporcionar los parámetros de entrada del comando, en lugar de especificar cada parámetro individual como entrada de la línea de comandos.

Para crear un control de acceso de origen (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo llamado `origin-access-control.yaml`. Este archivo contiene todos los parámetros de entrada para el comando create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Abra el archivo `origin-access-control.yaml` que acaba de crear. Edite el archivo para agregar un nombre para el OAC, una descripción (opcional) y cambie `SigningBehavior` por `always`. A continuación, guarde el archivo.

   Para obtener información sobre otras configuraciones de OAC, consulte the section called "Configuración avanzada para el control de acceso de origen".

3. Utilice el siguiente comando para crear el control de acceso de origen mediante los parámetros de entrada del archivo `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

   Anote el valor de `Id` en la salida del comando. Se necesita para agregar el OAC a una URL de función de Lambda en una distribución de CloudFront.

Cómo adjuntar un OAC a una URL de función de Lambda en una distribución existente (CLI con archivo de entrada)

1. Utilice el comando siguiente para guardar la configuración de distribución de la distribución de CloudFront a la que desea agregar el OAC. La distribución debe tener una URL de función de Lambda como el origen.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Abra el archivo llamado `dist-config.yaml` que acaba de crear. Edite el archivo y realice los siguientes cambios:

   - En el objeto `Origins`, agregue el ID de OAC al campo que se llama `OriginAccessControlId`.
   - Elimine el valor del campo que se llama `OriginAccessIdentity`, si existe.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución y utilizar el control de acceso de origen.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribución comienza a implementarse en todas las ubicaciones periféricas de CloudFront. Cuando una ubicación periférica recibe la nueva configuración, firma todas las solicitudes que envía a la URL de función de Lambda.

API

Para crear un OAC con la API de CloudFront, utilice CreateOriginAccessControl. Para obtener más información sobre los campos que especifique en esta llamada a la API, consulte la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Después de crear un OAC, puede adjuntarlo a una URL de función de Lambda en una distribución, mediante una de las siguientes llamadas a la API:

- Para asociarlo a una distribución existente, utilice UpdateDistribution.
- Para asociarlo a una nueva distribución, utilice CreateDistribution.

Para estas dos llamadas a la API, proporcione el ID de OAC en el campo `OriginAccessControlId`, dentro de un origen. Para obtener más información sobre los otros campos que especifique en estas llamadas a la API, la documentación de referencia de la API para AWS SDK u otro cliente de la API.

Configuración avanzada para el control de acceso de origen

La característica de OAC de CloudFront incluye configuraciones avanzadas que están pensadas solo para casos de uso específicos. Utilice la configuración recomendada a menos que tenga una necesidad específica de la configuración avanzada.

El OAC contiene una configuración denominada Comportamiento de firma (en la consola) o `SigningBehavior` (en la API, CLI y CloudFormation). Esta configuración proporciona las siguientes opciones:

Firmar siempre las solicitudes de origen (configuración recomendada)

Recomendamos utilizar esta configuración, denominada Firmar solicitudes (recomendado) en la consola o `always` en la API, la CLI y CloudFormation. Con esta configuración, CloudFront siempre firma todas las solicitudes que envía a la URL de función de Lambda.

Nunca firmar solicitudes de origen

Esta configuración se denomina No firmar solicitudes en la consola o `never` en la API, la CLI y CloudFormation. Utilice esta configuración con el fin de desactivar el OAC para todos los orígenes en todas las distribuciones que utilizan este OAC. Esto puede ahorrar tiempo y esfuerzo en comparación con la eliminación de un OAC de todos los orígenes y distribuciones que lo utilizan, uno por uno. Con esta configuración, CloudFront no ninguna solicitud que envía a la URL de función de Lambda.

> **Warning**
>
> Para utilizar esta configuración, la URL de función de Lambda debe ser de acceso público. Si utiliza esta configuración con una URL de función de Lambda que no es de acceso público, CloudFront no podrá acceder al origen. La URL de función de Lambda devuelve errores a CloudFront y CloudFront pasa esos errores a los lectores. Para obtener más información, consulte Modelo de seguridad y autenticación para URL de funciones de Lambda en la Guía del usuario de AWS Lambda.

No anular el encabezado **`Authorization`** del lector (cliente)

Esta configuración se denomina Do not override authorization header (No anular el encabezado authorization en la consola o `no-override` en la API, la CLI y CloudFormation. Utilice esta configuración cuando desee que CloudFront firme las solicitudes de origen solo cuando la solicitud del lector correspondiente no incluya un encabezado `Authorization`. Con esta configuración, CloudFront pasa el encabezado `Authorization` de la solicitud del lector cuando hay uno, pero firma la solicitud de origen (agrega su propio encabezado `Authorization`) cuando la solicitud del lector no incluye un encabezado `Authorization`.

> **Warning**
>
> - Si usa esta configuración, debe especificar la firma de Signature Version 4 para la URL de la función de Lambda en lugar del nombre o CNAME de la distribución de CloudFront. Cuando CloudFront reenvíe el encabezado `Authorization` de la solicitud del lector a la URL de la función de Lambda, Lambda validará la firma con respecto al host del dominio de la URL de Lambda. Si la firma no se basa en el dominio de la URL de Lambda, el host de la firma no coincidirá con el host utilizado por el origen de la URL de Lambda. Esto significa que la solicitud producirá un error, lo que provocará un error de validación de firma.
> - Para pasar el encabezado `Authorization` de la solicitud del lector, debe agregar el encabezado `Authorization` a una política de caché para todos los comportamientos de caché que utilizan las URL de función de Lambda asociadas con este control de acceso de origen.

Código de plantilla de ejemplo

Si el origen de CloudFront es la URL de una función de Lambda asociada a un OAC, puede utilizar el siguiente script de Python para cargar archivos en la función de Lambda con el método `POST`.

Este código asume que configuró el OAC con el comportamiento de firma predeterminado establecido en Firmar siempre las solicitudes de origen y que no seleccionó la configuración No anular el encabezado authorization.

Esta configuración permite al OAC administrar correctamente la autorización de SigV4 con Lambda mediante el nombre de host de Lambda. La carga útil se firma mediante SigV4 desde la identidad de IAM autorizada para la URL de la función de Lambda, que se designa como tipo `IAM_AUTH`.

La plantilla muestra cómo administrar los valores hash de la carga útil firmados en el encabezado x-amz-content-sha256 de las solicitudes `POST` del lado del cliente. En concreto, esta plantilla está diseñada para administrar las cargas útiles de datos de los formularios. La plantilla permite cargar archivos de forma segura a una URL de la función de Lambda a través de CloudFront y utiliza mecanismos de autenticación de AWS para garantizar que solo las solicitudes autorizadas puedan acceder a la función de Lambda.

El código incluye las siguientes funcionalidades:

- Cumple con el requisito de incluir el hash de carga útil en el encabezado x-amz-content-sha256.
- Utiliza la autenticación SigV4 para un acceso seguro de Servicio de AWS.
- Admite la carga de archivos mediante el uso de datos de formularios multiparte
- Incluye la gestión de errores para las excepciones de las solicitudes.

```
import boto3
from botocore.auth import SigV4Auth
from botocore.awsrequest import AWSRequest
import requests
import hashlib
import os


def calculate_body_hash(body):
    return hashlib.sha256(body).hexdigest()
```

```
def sign_request(request, credentials, region, service):
    sigv4 = SigV4Auth(credentials, service, region)
    sigv4.add_auth(request)


def upload_file_to_lambda(cloudfront_url, file_path, region):
    # AWS credentials
    session = boto3.Session()
    credentials = session.get_credentials()

    # Prepare the multipart form-data
    boundary = "------------------------boundary"

    # Read file content
    with open(file_path, 'rb') as file:
        file_content = file.read()

    # Get the filename from the path
    filename = os.path.basename(file_path)

    # Prepare the multipart body
    body = (
        f'--{boundary}\r\n'
        f'Content-Disposition: form-data; name="file"; filename="{filename}"\r\n'
        f'Content-Type: application/octet-stream\r\n\r\n'
    ).encode('utf-8')
    body += file_content
    body += f'\r\n--{boundary}--\r\n'.encode('utf-8')

    # Calculate SHA256 hash of the entire body
    body_hash = calculate_body_hash(body)

    # Prepare headers
    headers = {
        'Content-Type': f'multipart/form-data; boundary={boundary}',
        'x-amz-content-sha256': body_hash
    }

    # Create the request
    request = AWSRequest(
        method='POST',
        url=cloudfront_url,
```

```
        data=body,
        headers=headers
    )

    # Sign the request
    sign_request(request, credentials, region, 'lambda')

    # Get the signed headers
    signed_headers = dict(request.headers)

    # Print request headers before sending
    print("Request Headers:")
    for header, value in signed_headers.items():
        print(f"{header}: {value}")

    try:
        # Send POST request with signed headers
        response = requests.post(
            cloudfront_url,
            data=body,
            headers=signed_headers
        )

        # Print response status and content
        print(f"\nStatus code: {response.status_code}")
        print("Response:", response.text)

        # Print response headers
        print("\nResponse Headers:")
        for header, value in response.headers.items():
            print(f"{header}: {value}")

    except requests.exceptions.RequestException as e:
        print(f"An error occurred: {e}")


# Usage
cloudfront_url = "https://d111111abcdef8.cloudfront.net"
file_path = r"filepath"
region = "us-east-1"  # example: "us-west-2"

upload_file_to_lambda(cloudfront_url, file_path, region)
```

Restricción del acceso a un origen de Amazon S3

CloudFront proporciona dos formas de enviar solicitudes autenticadas a un origen de Amazon S3: control de acceso de origen (OAC) e identidad de acceso de origen (OAI). OAC lo ayuda a proteger los orígenes, como en el caso de Amazon S3.

Le recomendamos que utilice OAC en su lugar porque es compatible con las siguientes características:

- Todos los buckets de Amazon S3 en todas las Regiones de AWS, incluidas las regiones opcionales lanzadas después de diciembre de 2022
- Cifrado del servidor con AWS KMS de Amazon S3 (SSE-KMS)
- Solicitudes dinámicas (`PUT` y `DELETE`) en Amazon S3

OAI no es compatible con estas características o requiere soluciones alternativas adicionales en esos escenarios. Si ya utiliza OAI y desea migrar, consulte the section called “Migración de la identidad de acceso de origen (OAI) al control de acceso de origen (OAC)”.

> **Notas**
>
> - Si utiliza CloudFront OAC con orígenes de buckets de Amazon S3, debe establecer Propiedad de objetos de Amazon S3 como Aplicada al propietario del bucket, que es el valor predeterminado para los nuevos buckets de Amazon S3. Si necesita ACL, utilice la configuración Preferida del propietario del bucket para mantener el control de los objetos cargados mediante CloudFront.
> - Si su origen es un bucket de Amazon S3 configurado como punto de conexión de sitio web, debe configurarlo con CloudFront como un origen personalizado. Esto significa que no puede utilizar OAC (nila OAI). OAC no admite el redireccionamiento de origen mediante Lambda@Edge.

En los temas siguientes se describe cómo utilizar la OAC con un origen de Amazon S3.

Temas

- the section called “Creación de un nuevo control de acceso de origen”
- the section called “Eliminación de una distribución con un OAC adjunto a un bucket de S3”

- the section called “Migración de la identidad de acceso de origen (OAI) al control de acceso de origen (OAC)”
- the section called “Configuración avanzada para el control de acceso de origen”

Creación de un nuevo control de acceso de origen

Complete los pasos que se describen en los siguientes temas para configurar un nuevo control de acceso de origen en CloudFront.

Temas

- Requisitos previos
- Concesión de permiso de CloudFront para acceder al bucket de S3
- Creación del control de acceso de origen

Requisitos previos

Antes de crear y configurar el control de acceso de origen (OAC), debe tener una distribución de CloudFront con un bucket de origen de Amazon S3. Este origen debe ser un bucket S3 normal, no un bucket configurado como punto de conexión de sitio web. Para obtener más información sobre la configuración de una distribución de CloudFront con un origen de bucket de S3, consulte the section called “Introducción a una distribución estándar”.

> **Important**
>
> Cuando utiliza OAC para proteger el origen de Amazon S3, la comunicación entre CloudFront y Amazon S3 es siempre a través de HTTPS, pero solo cuando elige firmar siempre las solicitudes. Debe elegir Firmar solicitudes (recomendado) en la consola o especificar `always` en la API de CloudFront, AWS CLI o CloudFormation.
> Si, en su lugar, elige la opción No firmar solicitudes o No invalidar el encabezado de autorización, CloudFront utiliza el protocolo de conexión que especificó en las siguientes políticas:
>
> - Política de protocolo para lectores
> - Política de protocolo de origen (solo orígenes personalizados)

Por ejemplo, si elige No invalidar el encabezado de autorización y desea utilizar HTTPS entre CloudFront y el origen de Amazon S3, utilice Redirigir HTTP a HTTPS o Solo HTTPS para la política de protocolo del lector.

Concesión de permiso de CloudFront para acceder al bucket de S3

Antes de crear un control de acceso de origen (OAC) o configurarlo en una distribución de CloudFront, asegúrese de que CloudFront tiene permiso para acceder al origen del bucket de S3. Realice esta acción después de crear una distribución de CloudFront, pero antes de agregar el OAC al origen de S3 en la configuración de distribución.

Utilice una política de bucket de S3 para permitir a la entidad principal de servicio de CloudFront (`cloudfront.amazonaws.com`) acceder al bucket. Utilice un elemento `Condition` en la política para permitir que CloudFront acceda al bucket solo cuando la solicitud sea en nombre de la distribución de CloudFront que contiene el origen de S3. Esta es la distribución con el origen de S3 al que desea agregar OAC.

Para obtener información sobre cómo agregar o modificar una política de bucket, consulte Agregar una política de bucket mediante la consola de Amazon S3 en la Guía del usuario de Amazon S3.

A continuación, se muestran ejemplos de políticas de bucket de S3 que permiten a una distribución de CloudFront con OAC habilitado el acceso a un origen de S3.

Example Política de bucket de S3 que permite el acceso de solo lectura a una distribución de CloudFront con OAC habilitado

JSON

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

```
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
        }
      }
    }
  ]
}
```

Example Política de bucket de S3 que permite el acceso de lectura y escritura a una distribución de CloudFront con OAC habilitado

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipalReadWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID>"
        }
      }
    }
  ]
}
```

SSE-KMS

Si los objetos del origen de bucket de S3 están cifrados mediante el cifrado del servidor con AWS Key Management Service (SSE-KMS), debe asegurarse de que la distribución de CloudFront tiene permiso para utilizar la clave de AWS KMS. Para conceder permiso de distribución de CloudFront para utilizar la clave de KMS, agregue una declaración a la política de claves de KMS. Para obtener información sobre cómo modificar una política de claves, consulte Modificación de una política de claves en la Guía del desarrollador de AWS Key Management Service.

Example Instrucción de política de claves de KMS

El siguiente ejemplo muestra una declaración de política de AWS KMS que permite a la distribución de CloudFront con OAC acceder a una clave de KMS para SSE-KMS.

```
{
    "Sid": "AllowCloudFrontServicePrincipalSSE-KMS",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "cloudfront.amazonaws.com"
        ]
     },
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
            "StringEquals": {
                "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
            }
        }
}
```

Creación del control de acceso de origen

Para crear un control de acceso de origen (OAC), puede utilizar la Consola de administración de AWS, CloudFormation, la AWS CLI o la API de CloudFront.

Console

Para crear un control de acceso de origen

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Origin access (Acceso de origen).
3. Elija Create control setting (Crear configuración de control).
4. En el formulario Create control setting (Crear configuración de control), haga lo siguiente:
   a. En el panel Details (Detalles), ingrese un valor para Name (Nombre) y (opcionalmente) para Description (Descripción) para el control de acceso de origen.
   b. En el panel Settings (Configuración), le recomendamos que deje la configuración predeterminada Sign requests (recommended) (Firmar solicitudes [recomendado]). Para obtener más información, consulte the section called “Configuración avanzada para el control de acceso de origen”.
5. Elija S3 en el menú desplegable de Origin type (Tipo de origen).
6. Seleccione Crear.

   Una vez creado el OAC, anote el valor de Name (Nombre). Lo necesita en el siguiente procedimiento.

Para agregar un control de acceso de origen a un origen de S3 en una distribución

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija una distribución con un origen de S3 a la que desee agregar el OAC y, a continuación, elija la pestaña Origins (Orígenes).
3. Seleccione el origen de S3 al que desea agregar el OAC y, a continuación, elija Edit (Editar).
4. En la sección Acceso de origen, elija (Configuración del control de acceso de origen (recomendado).
5. En el menú desplegable Origin access control (Control de acceso de origen), elija el OAC que desee utilizar.
6. Seleccione Save changes (Guardar cambios).

La distribución comienza a implementarse en todas las ubicaciones periféricas de CloudFront. Cuando una ubicación periférica recibe la nueva configuración, firma todas las solicitudes que envía al origen de bucket de S3.

CloudFormation

Para crear un control de acceso de origen (OAC) con CloudFormation, utilice el tipo de recurso `AWS::CloudFront::OriginAccessControl`. El siguiente ejemplo se muestra la sintaxis de plantilla de CloudFormation, en formato YAML, para crear un control de acceso de origen.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: s3
      SigningBehavior: always
      SigningProtocol: sigv4
```

Para obtener más información, consulte AWS::CloudFront::OriginAccessControl en la Guía del usuario de AWS CloudFormation.

CLI

Para crear un control de acceso de origen con la AWS Command Line Interface (AWS CLI), utilice el comando aws cloudfront create-origin-access-control. Puede utilizar un archivo de entrada para proporcionar los parámetros de entrada del comando, en lugar de especificar cada parámetro individual como entrada de la línea de comandos.

Para crear un control de acceso de origen (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo llamado `origin-access-control.yaml`. Este archivo contiene todos los parámetros de entrada para el comando create-origin-access-control.

   ```
   aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
    origin-access-control.yaml
   ```

2. Abra el archivo `origin-access-control.yaml` que acaba de crear. Edite el archivo para agregar un nombre para el OAC, una descripción (opcional) y cambie `SigningBehavior` por `always`. A continuación, guarde el archivo.

Para obtener información sobre otras configuraciones de OAC, consulte the section called "Configuración avanzada para el control de acceso de origen".

3. Utilice el siguiente comando para crear el control de acceso de origen mediante los parámetros de entrada del archivo `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

Anote el valor de `Id` en la salida del comando. Lo necesita para agregar el OAC a un origen de bucket de S3 en una distribución de CloudFront.

Para adjuntar un OAC a un origen de bucket de S3 en una distribución existente (CLI con archivo de entrada)

1. Utilice el comando siguiente para guardar la configuración de distribución de la distribución de CloudFront a la que desea agregar el OAC. La distribución debe tener un origen de bucket de S3.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Abra el archivo llamado `dist-config.yaml` que acaba de crear. Edite el archivo y realice los siguientes cambios:

   - En el objeto `Origins`, agregue el ID de OAC al campo que se llama `OriginAccessControlId`.
   - Elimine el valor del campo que se llama `OriginAccessIdentity`, si existe.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución y utilizar el control de acceso de origen.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribución comienza a implementarse en todas las ubicaciones periféricas de CloudFront. Cuando una ubicación periférica recibe la nueva configuración, firma todas las solicitudes que envía al origen de bucket de S3.

API

Para crear un control de acceso de origen con la API de CloudFront, utilice CreateOriginAccessControl. Para obtener más información sobre los campos que especifique en esta llamada a la API, consulte la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Después de crear un control de acceso de origen, puede adjuntarlo a un origen de bucket de S3 en una distribución, mediante una de las siguientes llamadas a la API:

- Para asociarlo a una distribución existente, utilice UpdateDistribution.
- Para asociarlo a una nueva distribución, utilice CreateDistribution.

Para estas dos llamadas a la API, proporcione el ID de control de acceso de origen en el campo `OriginAccessControlId`, dentro de un origen. Para obtener más información sobre los otros campos que especifique en estas llamadas a la API, consulte Referencia de toda la configuración de distribución y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Eliminación de una distribución con un OAC adjunto a un bucket de S3

Si necesita eliminar una distribución con un OAC adjunto a un bucket de S3, debe eliminarla antes de eliminar el origen del bucket de S3. También puede incluir la región en el nombre de dominio de origen. Si no es posible, puede eliminar el OAC de la distribución mediante el cambio a público antes de la eliminación. Para obtener más información, consulte Eliminar una distribución.

Migración de la identidad de acceso de origen (OAI) al control de acceso de origen (OAC)

Para migrar de una identidad de acceso de origen (OAI) heredada a un control de acceso de origen (OAC), actualice primero el origen del bucket de S3 para permitir que OAI y la distribución con OAC

habilitado accedan al contenido del bucket. De este modo se garantiza que CloudFront nunca pierda el acceso al bucket durante la transición. Para permitir que OAI y la distribución con OAC habilitado accedan a un bucket de S3, actualice la política de bucket para incluir dos declaraciones, una para cada tipo de entidad principal.

El siguiente ejemplo de política de bucket de S3 permite que una OAI y una distribución con OAC habilitado accedan a un origen de S3.

Example Política de bucket de S3 que permite el acceso de solo lectura para una OAI y una distribución de CloudFront con OAC habilitado

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipalReadOnly",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
                }
            }
        },
        {
            "Sid": "AllowLegacyOAIReadOnly",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
```

```
}
```

Después de actualizar la política de buckets del origen de S3 para permitir el acceso tanto a OAI como a OAC, puede actualizar la configuración de la distribución para utilizar OAC en lugar de OAI. Para obtener más información, consulte the section called “Creación de un nuevo control de acceso de origen”.

Una vez implementada por completo la distribución, puede eliminar la declaración de la política de buckets que permite el acceso a la OAI. Para obtener más información, consulte the section called “Concesión de permiso de CloudFront para acceder al bucket de S3”.

Configuración avanzada para el control de acceso de origen

La característica de control de acceso de origen de CloudFront incluye configuraciones avanzadas que están pensadas solo para casos de uso específicos. Utilice la configuración recomendada a menos que tenga una necesidad específica de la configuración avanzada.

El control de acceso de origen contiene una configuración denominada Signing behavior (Comportamiento de firma) (en la consola) o `SigningBehavior` (en la API, CLI y CloudFormation). Esta configuración proporciona las siguientes opciones:

Firmar siempre las solicitudes de origen (configuración recomendada)

Recomendamos utilizar esta configuración, denominada Sign requests (recommended) (Firmar solicitudes [recomendado]) en la consola o `always` en la API, la CLI y CloudFormation. Con esta configuración, CloudFront siempre firma todas las solicitudes que envía al origen de bucket de S3.

Nunca firmar solicitudes de origen

Esta configuración se denomina Do not sign requests (No firmar solicitudes) en la consola o `never` en la API, la CLI y CloudFormation. Utilice esta configuración para desactivar el control de acceso de origen para todos los orígenes en todas las distribuciones que utilizan este control de acceso de origen. Esto puede ahorrar tiempo y esfuerzo en comparación con la eliminación de un control de acceso de origen de todos los orígenes y distribuciones que lo utilizan, uno por uno. Con esta configuración, CloudFront no firma las solicitudes que envía al origen de bucket de S3.

> **Warning**
>
> Para utilizar esta configuración, el origen de bucket de S3 debe ser de acceso público. Si utiliza esta configuración con un origen de bucket de S3 que no es de acceso público, CloudFront no podrá acceder al origen. El origen de bucket de S3 devuelve errores a CloudFront y CloudFront pasa esos errores a los lectores.

No anular el encabezado **`Authorization`** del lector (cliente)

Esta configuración se denomina Do not override authorization header (No anular el encabezado authorization en la consola o `no-override` en la API, la CLI y CloudFormation. Utilice esta configuración cuando desee que CloudFront firme las solicitudes de origen solo cuando la solicitud del lector correspondiente no incluya un encabezado `Authorization`. Con esta configuración, CloudFront pasa el encabezado `Authorization` de la solicitud del lector cuando hay uno, pero firma la solicitud de origen (agrega su propio encabezado `Authorization`) cuando la solicitud del lector no incluye un encabezado `Authorization`.

> **Warning**
>
> Para pasar el encabezado `Authorization` de la solicitud del lector, debe agregar el encabezado `Authorization` a una política de caché para todos los comportamientos de caché que utilizan los orígenes de buckets de S3 asociados con este control de acceso de origen.

Uso de una identidad de acceso de origen (heredado, no recomendado)

Descripción de la identidad de acceso de origen

La identidad de acceso de origen (OAI) de CloudFront proporciona una funcionalidad similar a la del control de acceso de origen (OAC), pero no funciona en todos los escenarios. En concreto, OAI no admite:

- Buckets de Amazon S3 en todas las Regiones de AWS, incluidas las regiones opcionales
- Cifrado del servidor con AWS KMS de Amazon S3 (SSE-KMS)
- Solicitudes dinámicas (`PUT`, `POST` o `DELETE`) en Amazon S3
- Regiones de AWS nuevas lanzadas después de enero de 2023

> **Tip**
>
> Le recomendamos que utilice OAC en su lugar. Para configurar OAC, consulte Creación de un nuevo control de acceso de origen. Para obtener información acerca de cómo migrar de OAI a OAC, consulte the section called “Migración de la identidad de acceso de origen (OAI) al control de acceso de origen (OAC)”.

Concesión de un permiso de identidad de acceso de origen para leer archivos en el bucket de Amazon S3

Cuando crea una OAI o agrega una a una distribución con la consola de CloudFront, puede actualizar automáticamente la política de bucket de Amazon S3 para conceder a la OAI permiso de acceso al bucket. Como alternativa, puede elegir crear o actualizar manualmente la política del bucket. Sea cual sea el método que utilice, debe revisar los permisos para asegurarse de que:

- La OAI de CloudFront puede acceder a los archivos del bucket en nombre de los lectores que los soliciten a través de CloudFront.
- Los lectores no pueden utilizar las URL de Amazon S3 para acceder a los archivos fuera de CloudFront.

> **Important**
>
> Si configura CloudFront para que acepte y reenvíe todos los métodos HTTP compatibles con CloudFront, asegúrese de conceder a la OAI de CloudFront los permisos deseados. Por ejemplo, si configura CloudFront para aceptar y reenviar solicitudes que utilizan el método `DELETE`, configure la política de bucket para que gestionen las solicitudes `DELETE` de forma adecuada para que los lectores solo puedan eliminar archivos que desee que eliminen.

Uso de políticas de buckets de Amazon S3

Puede conceder a la OAI de CloudFront acceso a los archivos de un bucket de Amazon S3 mediante la creación o actualización de la política de bucket de las siguientes maneras:

- Mediante la pestaña Permissions (Permisos) del bucket de Amazon S3 en la consola de Amazon S3.
- Mediante PutBucketPolicy en la API de Amazon S3.

- Mediante la consola de CloudFront. Cuando agrega una OAI a la configuración de origen en la consola de CloudFront, puede elegir Yes, update the bucket policy (Sí, actualizar política de bucket) para indicar a CloudFront que actualice la política del bucket en su nombre.

Si actualiza la política del bucket manualmente, asegúrese de:

- Especificar la OAI correcta como `Principal` en la política.
- Conceder a la OAI los permisos que necesita para obtener acceso a los objetos en nombre de los lectores.

Para obtener más información, consulte las siguientes secciones.

Cómo especificar una OAI como **`Principal`** en una política de bucket

Para especificar una OAI como `Principal` en una política de bucket de Amazon S3, utilice el nombre de recurso de Amazon (ARN) de la OAI, que incluye el ID de la OAI. Por ejemplo:

```
"Principal": {
    "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <origin
 access identity ID>"
}
```

Busque el ID de OAI en la consola de CloudFront, en Seguridad, Acceso de origen, Identidades (heredado). Como alternativa, utilice ListCloudFrontOriginAccessIdentities en la API de CloudFront.

Conceda permisos a una OAI

Para conceder a la OAI permisos para acceder a los objetos del bucket de Amazon S3, utilice acciones de la política relacionadas con operaciones específicas de la API de Amazon S3. Por ejemplo, la acción `s3:GetObject` permite a la OAI leer objetos del bucket. Para obtener más información, consulte los ejemplos de la siguiente sección o consulte acciones de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Ejemplos de políticas de bucket de Amazon S3

En los siguientes ejemplos se muestran las políticas de buckets de Amazon S3 que permiten a la OAI de CloudFront acceder a un bucket de S3.

Busque el ID de OAI en la consola de CloudFront, en Seguridad, Acceso de origen, Identidades (heredado). Como alternativa, utilice ListCloudFrontOriginAccessIdentities en la API de CloudFront.

Example Política de bucket de Amazon S3 que concede acceso de lectura a la OAI

El siguiente ejemplo permite a la OAI leer objetos del bucket especificado (`s3:GetObject`).

JSON

```
{
    "Version":"2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

Example Política de bucket de Amazon S3 que concede acceso de lectura y escritura a la OAI

El siguiente ejemplo permite a la OAI leer y escribir objetos en el bucket (`s3:GetObject` y `s3:PutObject`) especificado. Esto permite a los lectores cargar archivos en el bucket de Amazon S3 a través de CloudFront.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
```

```
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

Uso de ACL de objetos de Amazon S3 (no recomendado)

> **Important**
>
> Recomendamos el uso de las políticas de bucket de Amazon S3 para conceder a una OAI acceso a un bucket de S3. Puede utilizar listas de control de acceso (ACL) como se describe en esta sección, pero no lo recomendamos.
> Amazon S3 recomienda configurar Propiedad de objetos de S3 como propietario del bucket forzado, lo que significa que las ACL están desactivadas para el bucket y los objetos que contiene. Al aplicar esta configuración para Propiedad de objetos, debe utilizar políticas de bucket para dar acceso a la OAI (consulte la sección anterior).
> La sección siguiente es solo para casos de uso heredados que requieren ACL.

Puede conceder a una OAI de CloudFront acceso a los archivos de un bucket de Amazon S3 creando o actualizando la ACL de archivos de las siguientes maneras:

- Mediante la pestaña Permissions (Permisos) del objeto de Amazon S3 en la consola de Amazon S3.
- Mediante PutObjectAcl en la API de Amazon S3.

Cuando concede acceso a una OAI mediante una ACL, debe especificar la OAI mediante el ID de usuario canónico de Amazon S3. En la consola de CloudFront, puede encontrar este ID en Seguridad, Acceso de origen, Identidades (heredado). Si utiliza la API de CloudFront, use el valor del elemento `S3CanonicalUserId` devuelto al crear la OAI o llame a ListCloudFrontOriginAccessIdentities en la API de CloudFront.

Uso de una identidad de acceso de origen en las regiones de Amazon S3 que solo admiten la autenticación de Signature Version 4

Las regiones de Amazon S3 más recientes requieren que utilice Signature Version 4 para solicitudes autenticadas. (Para ver las versiones de firma admitidas en cada región de Amazon S3, consulte Puntos de conexión y cuotas de Amazon Simple Storage Service en la Referencia general de AWS). Si utiliza una identidad de acceso de origen y si su bucket se encuentra en una de las regiones que requiere firma versión 4, tenga en cuenta lo siguiente:

- Las solicitudes `DELETE`, `GET`, `HEAD`, `OPTIONS` y `PATCH` se admiten sin cualificación.
- `POST`Las solicitudes no están admitidas.

Restricción del acceso con orígenes de la VPC

Puede utilizar CloudFront para entregar contenido de las aplicaciones que se alojan en las subredes privadas de la nube privada virtual (VPC). Puede usar equilibradores de carga de aplicación, equilibradores de carga de red e instancias de EC2 en subredes privadas como orígenes de la VPC.

A continuación, se indican algunos de los motivos por los que es posible que desee utilizar Orígenes de la VPC:

- Seguridad: Orígenes de la VPC se ha diseñado para mejorar el estado de seguridad de su aplicación porque coloca sus equilibradores de carga e instancias de EC2 en subredes privadas, lo que convierte a CloudFront en el único punto de entrada. Las solicitudes de los usuarios van de CloudFront a los orígenes de la VPC a través de una conexión privada y segura, lo que proporciona seguridad adicional a las aplicaciones.
- Administración: Orígenes de la VPC reduce la sobrecarga operativa necesaria para una conectividad segura entre CloudFront y los orígenes. Puede trasladar sus orígenes a subredes privadas sin acceso público y no tiene que implementar listas de control de acceso (ACL) ni otros mecanismos para restringir el acceso a sus orígenes. De esta forma, no tiene que invertir en un trabajo de desarrollo indiferenciado para proteger sus aplicaciones web con CloudFront.
- Escalabilidad y rendimiento: orígenes de la VPC le ayuda a proteger sus aplicaciones web, lo que le permite dedicar tiempo a centrarse en el crecimiento de sus aplicaciones empresariales fundamentales y, al mismo tiempo, mejorar la seguridad y mantener el alto rendimiento y la escalabilidad global con CloudFront. Orígenes de la VPC optimiza la administración de la seguridad y reduce la complejidad operativa para que pueda usar CloudFront como punto de entrada único para sus aplicaciones.

> **Tip**
>
> CloudFront permite compartir los orígenes de las VPC compartidos en Cuentas de AWS, estén o no en la organización. Puede compartir los orígenes de la VPC desde la consola de CloudFront o usar AWS Resource Access Manager (AWS RAM). Para obtener más información, consulte Trabajo con recursos compartidos en CloudFront.

Requisitos previos

Antes de crear un origen de la VPC para la distribución de CloudFront, debe completar los siguientes pasos:

- Cree una nube privada virtual (VPC) en Amazon VPC.
  - La VPC debe estar en una de las Regiones de AWS que admiten orígenes de la VPC. Para obtener más información, consulte Regiones de AWS admitidas para Orígenes de la VPC.
  - Las ACL de red asociadas a las subredes de la VPC se aplican al tráfico de salida (saliente) cuando la conservación de la dirección IP del cliente está habilitada en el origen de la VPC. Sin embargo, para permitir que el tráfico salga a través del origen de la VPC debe configurar la ACL como una regla de entrada y de salida.

    Por ejemplo, para permitir que los clientes de TCP y UDP que utilizan un puerto de origen efímero se conecten al punto de conexión a través del origen de la VPC, asocie la subred del punto de conexión a una ACL de red que permita el tráfico saliente destinado a un puerto TCP o UDP efímero (rango de puertos 1024-65535, destino 0.0.0.0/0). Además, cree una regla de entrada coincidente (rango de puertos 1024-65535, fuente 0.0.0.0/0).

  Para obtener información sobre la creación de una VPC, consulte Creación de una VPC y otros recursos de la VPC en la Guía del usuario de Amazon VPC.
- En la VPC, incluya lo siguiente:
  - Puerta de enlace de Internet: debe agregar una puerta de enlace de Internet a la VPC que tiene los recursos de origen de la VPC. La puerta de enlace de Internet es necesaria para indicar que la VPC pueda recibir tráfico de Internet. La puerta de enlace de Internet no se usa para enrutar el tráfico a los orígenes dentro de la subred y no es necesario actualizar las políticas de enrutamiento.
  - Subred privada con al menos una dirección IPv4 disponible: CloudFront se dirige a la subred mediante una interfaz de red elástica (ENI) administrada por un servicio que CloudFront crea

después de definir el recurso de origen de la VPC con CloudFront. Debe tener al menos una dirección IPv4 disponible en su subred privada para que el proceso de creación de la ENI se lleve a cabo correctamente. La dirección IPv4 puede ser privada y no conlleva ningún coste adicional.

> **Note**
>
> No se admiten subredes solo de IPv6.

- En la subred privada, lance un equilibrador de carga de aplicación, un equilibrador de carga de red o una instancia de EC2 para utilizarlos como origen.
  - El recurso que lance debe estar completamente implementado y en estado Activo antes de poder usarlo para un origen de la VPC.
  - Los equilibradores de carga de puerta de enlace, los equilibradores de carga de red de doble pila y los equilibradores de carga de red con oyentes de TLS no se pueden agregar como orígenes.
  - Para que se utilice como un origen de la VPC, un equilibrador de carga de red debe tener un grupo de seguridad asociado.
  - Actualice los grupos de seguridad de los orígenes privados de la VPC para permitir explícitamente la lista de prefijos administrada por CloudFront. Para obtener más información, consulte Utilizar la lista de prefijos administrados de CloudFront.

    > **Note**
    >
    > CloudFront-VPCOrigins-Service-SG es un nombre reservado de AWS para los grupos de seguridad que se utilizan para los orígenes de las VPC. Debe especificar un nombre diferente para el grupo de seguridad. Para obtener más información, consulte Creación de un grupo de seguridad.

    - Una vez creado el origen de la VPC, se puede restringir aún más el grupo de seguridad para permitir solo el tráfico de sus orígenes de la VPC. Para ello, actualice el origen de tráfico permitido de la lista de prefijos administrados al grupo de seguridad de CloudFront.

> **Note**
>
> Los desencadenadores de tráfico de WebSockets, gRPC, solicitudes de origen y respuestas de origen con Lambda@Edge en CloudFront no se admiten en los orígenes de VPC. Para obtener más información, consulte Trabajo con solicitudes y respuestas en la documentación de Lambda@Edge.

Creación de un origen de la VPC (nueva distribución)

El siguiente procedimiento muestra cómo crear un origen de la VPC para la nueva distribución de CloudFront en la consola de CloudFront. También puede usar las operaciones de la API CreateVpcOrigin y CreateDistribution con la AWS CLI o un SDK de AWS.

Para crear un origen de la VPC para una nueva distribución de CloudFront

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Orígenes de la VPC, Crear origen de la VPC.
3. Rellene los campos obligatorios. En ARN de origen, seleccione el ARN del equilibrador de carga de aplicación, equilibrador de carga de red o la instancia de EC2. Si no ve el ARN, puede copiar el ARN de recurso específico y pegarlo aquí.
4. Elija Crear origen de la VPC.
5. Espere a que el estado del origen de la VPC cambie a Implementado. Este proceso puede tardar hasta 15 minutos.
6. Elija Distribuciones, Crear distribución.
7. En Dominio de origen, seleccione su recurso de orígenes de la VPC en la lista desplegable.

   Si el origen la VPC es una instancia de EC2, copie y pegue el nombre DNS de IP privada de la instancia en el campo Dominio de origen.
8. Termine de crear su distribución. Para obtener más información, consulte Creación de una distribución de CloudFront en la consola.

Creación de un origen de la VPC (distribución existente)

El siguiente procedimiento muestra cómo crear un origen de la VPC para una distribución de CloudFront existente en la consola de CloudFront, lo que ayuda a garantizar una disponibilidad

continua de sus aplicaciones. También puede usar las operaciones de la API CreateVpcOrigin y UpdateDistributionWithStagingConfig con la AWS CLI o un SDK de AWS.

Si lo desea, puede agregar el origen de la VPC a la distribución existente sin crear una distribución provisional.

Para crear un origen de la VPC para una distribución existente de CloudFront

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Orígenes de la VPC, Crear origen de la VPC.
3. Rellene los campos obligatorios. En ARN de origen, seleccione el ARN del equilibrador de carga de aplicación, equilibrador de carga de red o la instancia de EC2. Si no ve el ARN, puede copiar el ARN de recurso específico y pegarlo aquí.
4. Elija Crear origen de la VPC.
5. Espere a que el estado del origen de la VPC cambie a Implementado. Este proceso puede tardar hasta 15 minutos.
6. En el panel de navegación, elija Distribuciones.
7. Elija el ID de su distribución.
8. En la pestaña General, en Implementación continua, elija Crear distribución provisional. Para obtener más información, consulte Uso de la implementación continua de CloudFront para probar de forma segura los cambios en la configuración de la CDN.
9. Siga los pasos del asistente Crear distribución provisional para crear una distribución provisional. Incluya los pasos siguientes:
   - En Orígenes, seleccione Crear origen.
   - En Dominio de origen, seleccione su recurso de orígenes de la VPC en el menú desplegable.

     Si el origen la VPC es una instancia de EC2, copie y pegue el nombre DNS de IP privada de la instancia en el campo Dominio de origen.
   - Elija Crear origen.
10. En la distribución provisional, pruebe el origen de la VPC.
11. Promueva la configuración de la distribución provisional a su distribución principal. Para obtener más información, consulte Promoción de una configuración de distribución provisional.
12. Elimine el acceso público al origen de la VPC haciendo la subred privada. Una vez hecho esto, el origen de la VPC no se podrá detectar en Internet, pero CloudFront seguirá teniendo acceso

privado a él. Para obtener más información, consulte Asociación o desvinculación de una subred y una tabla de enrutamiento en la Guía del usuario de Amazon VPC.

Actualización de un origen de la VPC

El siguiente procedimiento muestra cómo actualizar un origen de la VPC para la distribución de CloudFront en la consola de CloudFront. También puede usar las operaciones de la API UpdateDistribution y UpdateVpcOrigin con la AWS CLI o un SDK de AWS.

Para actualizar un origen de la VPC de una distribución existente de CloudFront

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Distribuciones.
3. Elija el ID de su distribución.
4. Elija la pestaña Comportamientos.
5. Asegúrese de que el origen de la VPC no sea el origen predeterminado del comportamiento de la caché.
6. Elija la pestaña Orígenes.
7. Seleccione el origen de la VPC que va a actualizar y elija Eliminar. Esto desvincula el origen de la VPC de la distribución. Repita los pasos 2 a 7 para desvincular el origen de la VPC de cualquier otra distribución.
8. Elija Orígenes de la VPC.
9. Seleccione el origen de la VPC y elija Editar.
10. Realice las actualizaciones y elija Actualizar origen de la VPC.
11. Espere a que el estado del origen de la VPC cambie a Implementado. Este proceso puede tardar hasta 15 minutos.
12. En el panel de navegación, elija Distribuciones.
13. Elija el ID de su distribución.
14. Elija la pestaña Orígenes.
15. Elija Crear origen.
16. En Dominio de origen, seleccione su recurso de orígenes de la VPC en el menú desplegable.

    Si el origen la VPC es una instancia de EC2, copie y pegue el nombre DNS de IP privada de la instancia en el campo Dominio de origen.

17. Elija Crear origen. Esto vuelve a asociar el origen de la VPC a su distribución. Repita los pasos 12 a 17 para asociar el origen de la VPC actualizada a cualquier otra distribución.

Regiones de AWS admitidas para Orígenes de la VPC

Actualmente, los orígenes de la VPC se admiten en las siguientes Regiones de AWS comerciales. Se indican las excepciones a la zona de disponibilidad (AZ).

Nombre de la región	Región
Este de EE. UU. (Ohio)	`us-east-2`
Este de EE. UU. (Norte de Virginia)	`us-east-1 (except AZ use1-az3)`
Oeste de EE. UU. (Norte de California)	`us-west-1 (except AZ usw1-az2)`
Oeste de EE. UU. (Oregón)	`us-west-2`
África (Ciudad del Cabo)	`af-south-1`
Asia-Pacífico (Hong Kong)	`ap-east-1`
Asia-Pacífico (Mumbai)	`ap-south-1`
Asia-Pacífico (Hyderabad)	`ap-south-2`
Asia-Pacífico (Yakarta)	`ap-southeast-3`
Asia-Pacífico (Melbourne)	`ap-southeast-4`
Asia-Pacífico (Osaka)	`ap-northeast-3`
Asia-Pacífico (Singapur)	`ap-southeast-1`
Asia-Pacífico (Sídney)	`ap-southeast-2`
Asia-Pacífico (Tokio)	`ap-northeast-1 (except AZ apne1-az3)`

Nombre de la región	Región
Asia-Pacífico (Seúl)	`ap-northeast-2 (except AZ apne2-az1)`
Asia-Pacífico (Tailandia)	`ap-southeast-7`
Asia-Pacífico (Malasia)	`ap-southeast-5`
Asia-Pacífico (Taipéi)	`ap-east-2`
Canadá (centro)	`ca-central-1 (except AZ cac1-az3)`
Oeste de Canadá (Calgary)	`ca-west-1`
Europa (Fráncfort)	`eu-central-1`
Europa (Irlanda)	`eu-west-1`
Europa (Londres)	`eu-west-2`
Europa (Milán)	`eu-south-1`
Europa (París)	`eu-west-3`
Europa (España)	`eu-south-2`
Europa (Estocolmo)	`eu-north-1`
Europa (Zúrich)	`eu-central-2`
Israel (Tel Aviv)	`il-central-1`
Medio Oriente (Baréin)	`me-south-1`
Medio Oriente (EAU)	`me-central-1`
América del Sur (São Paulo)	`sa-east-1`
México (centro)	`mx-central-1`

Restricción del acceso a Application Load Balancer

Puede utilizar equilibradores de carga de aplicaciones internos y orientados a Internet con Amazon CloudFront. Puede usar equilibradores de carga de aplicaciones internos dentro de subredes privadas con CloudFront mediante orígenes de la VPC. Los orígenes de VPC de CloudFront le permiten ofrecer contenido de aplicaciones alojadas en subredes de VPC privadas sin exponerlas a Internet pública. Para obtener más información, consulte Restricción del acceso con orígenes de la VPC.

Si utiliza un equilibrador de carga de aplicaciones orientado a Internet con CloudFront, puede usar las siguientes mitigaciones de seguridad para evitar que los usuarios accedan directamente a un equilibrador de carga de aplicaciones y permitir el acceso solo a través de CloudFront.

1. Configure CloudFront para agregar un encabezado HTTP personalizado a las solicitudes que envía al balanceador de carga de aplicaciones.
2. Configure el balanceador de carga de aplicaciones para que solo reenvíe solicitudes que contengan el encabezado HTTP personalizado.
3. Requiera HTTPS para mejorar la seguridad de esta solución.

CloudFront también puede ayudar a reducir la latencia e incluso absorber algunos ataques de denegación de servicio distribuido (DDoS).

Si el caso de uso requiere un acceso dual a las aplicaciones web desde CloudFront y el equilibrador de carga de aplicaciones directamente a través de Internet, considere dividir las API de la aplicación web de la siguiente manera:

- API que deben pasar a través de CloudFront. En este caso, considere la posibilidad de utilizar un equilibrador de carga de aplicaciones privado independiente como origen.
- API que requieren acceso a través del equilibrador de carga de aplicaciones. En este caso, se omite CloudFront.

Para una aplicación web u otro contenido que proporciona un equilibrador de carga de aplicación expuesto a Internet en Elastic Load Balancing, CloudFront puede almacenar en caché objetos y proporcionárselos directamente a los usuarios (espectadores), lo que reduce la carga en el equilibrador de carga de aplicación. Un equilibrador de carga expuesto a Internet tiene un nombre de DNS que se puede resolver públicamente y direcciona las solicitudes de los clientes a través de Internet hasta los destinos.

Para obtener más información, consulte los siguientes temas. Después de completar estos pasos, los usuarios solo pueden acceder a su balanceador de carga de aplicaciones a través de CloudFront.

Temas

- Configuración de CloudFront para agregar un encabezado HTTP personalizado a solicitudes
- Configuración de un equilibrador de carga de aplicaciones para que solo reenvíe solicitudes que contengan un encabezado específico
- (Opcional) Mejore la seguridad de esta solución
- (Opcional) Limitación del acceso al origen mediante la lista de prefijos administrados por AWS para CloudFront

Configuración de CloudFront para agregar un encabezado HTTP personalizado a solicitudes

Puede configurar CloudFront para agregar un encabezado HTTP personalizado a las solicitudes que envía a su origen (en este caso, un balanceador de carga de aplicaciones).

> **Important**
>
> Este caso de uso se basa en mantener el nombre del encabezado personalizado y el valor en secreto. Si el nombre y el valor del encabezado no son secretos, otros clientes HTTP podrían incluirlos en las solicitudes que envían directamente al balanceador de carga de aplicaciones. Esto puede hacer que el balanceador de carga de aplicaciones se comporte como si las solicitudes vinieran de CloudFront cuando no lo hacen. Para evitar esto, mantenga el nombre del encabezado personalizado y el valor en secreto.

Puede configurar CloudFront para agregar un encabezado HTTP personalizado a las solicitudes de origen con la consola de CloudFront, CloudFormation o la API de CloudFront.

Para agregar un encabezado HTTP personalizado (consola de CloudFront)

En la consola de CloudFront, utilice la configuración Origin Custom Headers (Encabezados personalizados de origen) Origin Settings (Configuración de origen). Introduzca el Nombre del encabezado y el Valor.

> **Note**
>
> En producción, use nombres de encabezado y valores generados aleatoriamente. Trate los nombres y valores de los encabezados como credenciales seguras, como nombres de usuario y contraseñas.

Puede editar la configuración Origin Custom Headers (Encabezados personalizados de origen) cuando crea o edita un origen para una distribución existente de CloudFront y crea una distribución nueva. Para obtener más información, consulte Actualizar una distribución y Creación de una distribución.

Para agregar un encabezado HTTP personalizado (CloudFormation)

En una plantilla de CloudFormation, utilice la propiedad `OriginCustomHeaders`, como se muestra en el siguiente ejemplo.

> **Note**
>
> El nombre del encabezado y el valor de este ejemplo son solo para demostración. En producción, use valores generados aleatoriamente. Trate el nombre y el valor del encabezado como una credencial segura, como un nombre de usuario y una contraseña.

```
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'
```

Para obtener más información, consulte las propiedades Origen y OriginCustomHeader en la Guía del usuario de AWS CloudFormation.

Para agregar un encabezado HTTP personalizado (API de CloudFront)

En la API de CloudFront, utilice el `CustomHeaders` objeto interior `Origin`. Para obtener más información, consulte CreateDistribution and UpdateDistribution en la Referencia de la API de Amazon CloudFront y la documentación del SDK u otro cliente de API.

Hay algunos nombres de encabezados que no se pueden especificar como encabezados personalizados de origen. Para obtener más información, consulte Encabezados personalizados que CloudFront no puede agregar a solicitudes de origen.

Configuración de un equilibrador de carga de aplicaciones para que solo reenvíe solicitudes que contengan un encabezado específico

Después de configurar CloudFront para agregar un encabezado HTTP personalizado a las solicitudes que envía al balanceador de carga de aplicaciones (consulte la sección anterior), puede configurar el balanceador de carga para que solo reenvíe solicitudes que contengan este encabezado personalizado. Para ello, agregue una nueva regla y modifique la regla predeterminada en el agente de escucha del balanceador de carga.

Requisitos previos

Para utilizar los siguientes procedimientos, necesita un balanceador de carga de aplicaciones con al menos un agente de escucha. Si aún no ha creado uno, consulte Crear un balanceador de carga de aplicaciones en la Guía del usuario de balanceadores de carga de aplicaciones.

Los siguientes procedimientos modifican un agente de escucha HTTPS. Puede utilizar el mismo proceso para modificar un agente de escucha HTTP.

Para actualizar las reglas en un agente de escucha del balanceador de carga de aplicaciones

1. Agregue una nueva regla. Siga las instrucciones de Agregar una regla, con las siguientes modificaciones:
   - Agregue la regla al equilibrador de carga que es el origen de la distribución de CloudFront.
   - Para Agregar condición, elija Encabezado Http. Especifique el nombre del encabezado HTTP y el valor que agregó como encabezado personalizado de origen en CloudFront.
   - Para Agregar acción, elija Reenviar a. Elija el grupo de destino al que desea reenviar las solicitudes.
2. Edite la regla predeterminada en el oyente del equilibrador de carga. Siga las instrucciones de Editar una regla, con las siguientes modificaciones:
   - Edite la regla predeterminada del equilibrador de carga que es el origen de la distribución de CloudFront.
   - Elimine la acción predeterminada y, a continuación, en Agregar acción, elija Devolver respuesta fija.
   - En Response code (Código de respuesta), escriba **`403`**.
   - En Response body (Cuerpo de respuesta), escriba **`Access denied`**.

Después de completar estos pasos, el oyente del equilibrador de carga tiene dos reglas. Una regla reenvía las solicitudes que contienen el encabezado HTTP (solicitudes que provienen de CloudFront). La otra regla envía una respuesta fija a todas las demás solicitudes (solicitudes que no provienen de CloudFront).

Puede verificar que la solución funcione si envía una solicitud a su distribución de CloudFront y una a su balanceador de carga de aplicaciones. La solicitud a CloudFront devuelve su aplicación web o contenido y la que se envía directamente al balanceador de carga de aplicaciones devuelve una respuesta `403` con el mensaje de texto sin formato `Access denied`.

(Opcional) Mejore la seguridad de esta solución

Para mejorar la seguridad de esta solución, puede configurar su distribución de CloudFront para que utilice siempre HTTPS cuando envíe solicitudes a su balanceador de carga de aplicaciones. Recuerde, esta solución solo funciona si mantiene el nombre del encabezado personalizado y el valor en secreto. El uso de HTTPS puede ayudar a evitar que un espía descubra el nombre y el

valor del encabezado. También recomendamos cambiar periódicamente el nombre y el valor del encabezado.

Usar HTTPS para solicitudes de origen

Para configurar CloudFront a fin de que utilice HTTPS para solicitudes de origen, establezca la configuración Origin Protocol Policy (Política de protocolo de origen) en HTTPS Only (Solo HTTPS). Esta configuración está disponible en la consola de CloudFront, CloudFormation y la API de CloudFront. Para obtener más información, consulte Protocolo (solo orígenes personalizados).

Lo siguiente también se aplica al configurar CloudFront con el fin de que utilice HTTPS para solicitudes de origen:

- Debe configurar CloudFront para que reenvíe el encabezado `Host` al origen con la política de solicitud de origen. Puede utilizar la política de solicitud de origen administrada por AllViewer.
- Asegúrese de que el Equilibrador de carga de aplicación dispone de un oyente HTTPS (como se muestra en la sección anterior). Para obtener más información, consulte Crear un agente de escucha HTTPS en la Guía del usuario de balanceadores de carga de aplicaciones. Utilizar un oyente HTTPS requiere disponer de un certificado SSL/TLS que coincida con el nombre de dominio enrutado al Equilibrador de carga de aplicación.
- Los certificados SSL/TLS para CloudFront solo se pueden solicitar (o importar) en la Región de AWS de `us-east-1` en AWS Certificate Manager (ACM). Como CloudFront es un servicio global, distribuye automáticamente el certificado de la región de `us-east-1` a todas las regiones asociadas a la distribución de CloudFront.
  - Por ejemplo, si tiene un Equilibrador de carga de aplicación (ALB) en la región de `ap-southeast-2`, debe configurar certificados SSL/TLS tanto en la región de `ap-southeast-2` (para utilizar HTTPS entre CloudFront y el origen de ALB) como en la región de `us-east-1` (para utilizar HTTPS entre los lectores y CloudFront). Ambos certificados deben coincidir con el nombre de dominio que se enruta al Equilibrador de carga de aplicación. Para obtener más información, consulte Región de AWS para AWS Certificate Manager.
- Si los usuarios finales (también conocidos como lectoreso clientes) de su aplicación web pueden usar HTTPS, también puede configurar CloudFront para que prefiera (o incluso requiera) conexiones HTTPS de los usuarios finales. Para ello, utilice la configuración Viewer Protocol Policy (Política de protocolo del lector). Puede configurarla para redirigir a los usuarios finales de HTTP a HTTPS o rechazar las solicitudes que utilizan HTTP. Esta configuración está disponible en la consola de CloudFront, CloudFormation y la API de CloudFront. Para obtener más información, consulte Política de protocolo para lectores.

Cambiar el nombre y el valor del encabezado

Además de usar HTTPS, también recomendamos cambiar el nombre y el valor del encabezado periódicamente. Los pasos de alto nivel para hacerlo son los siguientes:

1. Configure CloudFront para agregar un encabezado HTTP personalizado adicional a las solicitudes que envía al balanceador de carga de aplicaciones.
2. Actualice la regla del agente de escucha del balanceador de carga de aplicaciones para reenviar solicitudes que contengan este encabezado HTTP personalizado adicional.
3. Configure CloudFront para dejar de agregar el encabezado HTTP personalizado original a las solicitudes que envía al balanceador de carga de aplicaciones.
4. Actualice la regla del agente de escucha del balanceador de carga de aplicaciones para detener el reenvío de solicitudes que contengan el encabezado HTTP personalizado original.

Para obtener más información sobre cómo realizar estos pasos, consulte las secciones anteriores.

(Opcional) Limitación del acceso al origen mediante la lista de prefijos administrados por AWS para CloudFront

Para restringir aún más el acceso al Equilibrador de carga de aplicación, puede configurar el grupo de seguridad asociado a él para que solo acepte tráfico de CloudFront cuando el servicio utilice una lista de prefijos administrados por AWS. Esto evita que el tráfico que no se origina en CloudFront llegue al Equilibrador de carga de aplicación en la capa de red (capa 3) o en la capa de transporte (capa 4).

Para obtener más información, consulte la entrada de blog Limit access to your origins using the AWS-managed prefix list for Amazon CloudFront.

Restricción de la distribución geográfica de su contenido

Puede utilizar restricciones geográficas, a veces conocidas como bloqueo geográfico, para evitar que los usuarios de ubicaciones geográficas específicas accedan al contenido que distribuye a través de una distribución de Amazon CloudFront. Para utilizar las restricciones geográficas, tiene dos opciones:

- Use la característica de restricciones geográficas de CloudFront. Utilice esta opción para restringir el acceso a todos los archivos asociados a una distribución y según el país.

- Utilice un servicio de geolocalización de terceros. Utilice esta opción para restringir el acceso a un subconjunto de los archivos asociados a una distribución o para restringirlo a un nivel más detallado que por país.

Temas

- Uso de restricciones geográficas de CloudFront
- Uso de un servicio de geolocalización de terceros

Uso de restricciones geográficas de CloudFront

Cuando un usuario solicita el contenido, CloudFront normalmente lo ofrece independientemente de dónde se encuentra el usuario. Si necesita impedir que usuarios de países específicos accedan al contenido, puede usar la característica de restricciones geográficas de CloudFront para realizar una de las siguientes acciones:

- Conceda permiso a sus usuarios para que accedan a su contenido solo si se encuentran en uno de los países aprobados en la lista de permitidos.
- Evite que los usuarios accedan al contenido si se encuentran en uno de los países prohibidos de la lista de denegación.

Por ejemplo, si una solicitud proviene de un país donde no tiene autorización para distribuir su contenido, puede utilizar las restricciones geográficas de CloudFront para bloquear la solicitud.

> **Note**
>
> CloudFront determina la ubicación de los usuarios mediante una base de datos de terceros. La precisión del mapeo entre direcciones IP y países varía en función de la región. Según pruebas recientes, la precisión global es del 99,8 %. Si CloudFront no puede determinar la ubicación de un usuario, CloudFront ofrece el contenido que el usuario ha solicitado.

Así es como funcionan las restricciones geográficas:

1. Supongamos que tiene derechos para distribuir su contenido únicamente en Liechtenstein. Se actualiza la distribución de CloudFront para agregar una lista de permitidos que contiene solo

Liechtenstein. (También puede agregar una lista de denegación que contenga todos los países excepto Liechtenstein).

2. Un usuario en Mónaco solicita el contenido y DNS dirige la solicitud a una ubicación periférica de CloudFront en Milán, Italia.
3. La ubicación periférica en Milán revisa su distribución y determina que el usuario en Mónaco no tiene permiso para descargar su contenido.
4. CloudFront devuelve un código de estado HTTP `403 (Forbidden)` al usuario.

Si lo desea, puede configurar CloudFront para devolver un mensaje de error personalizado al usuario y puede especificar el tiempo durante el cual desea que CloudFront almacene en caché la respuesta de error del archivo solicitado. El valor de predeterminado es de 10 segundos. Para obtener más información, consulte Creación de una página de error personalizada para códigos de estado HTTP específicos.

Las restricciones geográficas se aplican a la totalidad de la distribución. Si necesita aplicar una restricción a parte del contenido y una restricción diferente (o ningún tipo de restricción) a otra parte del contenido, debe crear distribuciones de CloudFront independientes o utilizar un servicio de geolocalización de terceros.

Si habilita los registros estándar (registros de acceso) de CloudFront, puede identificar las solicitudes que CloudFront rechazó al buscar las entradas de registro cuyo valor de `sc-status` (el código de estado HTTP) sea `403`. Sin embargo, si solo utiliza los registros estándar, no puede distinguir entre una solicitud que CloudFront rechazó en función de la ubicación del usuario y las que CloudFront rechazó porque el usuario no tenía permiso de acceso al archivo debido a otro motivo. Si tiene un servicio de geolocalización de terceros como Digital Element o MaxMind, puede identificar la ubicación de las solicitudes en función de la dirección IP en la columna `c-ip` (IP del cliente) de los registros de acceso. Para obtener más información sobre los registros estándar de CloudFront, consulte Registros de acceso (registros estándar).

En el siguiente procedimiento se explica cómo utilizar la consola de CloudFront para agregar restricciones geográficas a una distribución existente. Para obtener más información acerca de cómo crear una distribución, consulte Creación de una distribución.

Para agregar restricciones geográficas a la distribución web (consola) de CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.

2. En el panel de navegación, elija Distribuciones y, a continuación, elija la distribución que desea actualizar.
3. Elija la pestaña Seguridad y, a continuación, Restricciones geográficas.
4. Elija Edit (Edición de).
5. Seleccione Allow list (Lista de permitidos) para crear una lista de países permitidos o Block list (Lista de bloqueados) para crear una lista de países bloqueados.
6. Agregue los países deseados a la lista y, a continuación, elija Save changes (Guardar cambios).

Uso de un servicio de geolocalización de terceros

La característica de restricciones geográficas de CloudFront le permite controlar la distribución de su contenido en el nivel de país para todos los archivos que esté distribuyendo con una determinada distribución web. Si tiene un caso de uso de restricciones geográficas en el que las restricciones no se ajustan a los límites del país o si quiere restringir el acceso solo a algunos de los archivos que está sirviendo por una distribución determinada, puede combinar CloudFront con un servicio de geolocalización de terceros. Esto le proporciona control sobre su contenido en función no solo del país, sino también de la ciudad, código postal o incluso la latitud y la longitud.

Cuando utiliza un servicio de geolocalización de terceros, le recomendamos utilizar direcciones URL firmadas de CloudFront, que le permiten especificar una fecha y hora de vencimiento a partir de la cual la URL deja de ser válida. Además, le recomendamos utilizar un bucket de Amazon S3 como origen porque eso le permite utilizar un control de acceso de origen de CloudFront para evitar que los usuarios obtengan acceso al contenido directamente desde el origen. Para obtener más información acerca de las URL firmadas y controles de acceso de origen, consulte Distribución de contenido privado con URL firmadas y cookies firmadas.

Los siguientes pasos explican cómo controlar el acceso a sus archivos mediante un servicio de geolocalización de terceros.

Para utilizar un servicio de geolocalización de terceros para restringir el acceso a los archivos de una distribución de CloudFront

1. Obtenga una cuenta con un servicio de geolocalización.
2. Cargue su contenido a un bucket de Amazon S3.
3. Configure Amazon CloudFront y Amazon S3 para que sirvan contenido privado. Para obtener más información, consulte Distribución de contenido privado con URL firmadas y cookies firmadas.

4. Escriba su aplicación web para que haga lo siguiente:

   - Enviar la dirección IP de cada solicitud de usuario al servicio de geolocalización.
   - Evalúe el valor de devolución del servicio de geolocalización para determinar si el usuario se encuentra en una ubicación donde desea que CloudFront distribuya el contenido.
   - Si desea distribuir el contenido a la ubicación del usuario, genere una URL firmada para el contenido de CloudFront. Si no desea distribuir contenido a esa ubicación, devuelva el código de estado HTTP `403 (Forbidden)` al usuario. Otra opción es configurar CloudFront para que devuelva un mensaje de error personalizado. Para obtener más información, consulte the section called “Creación de una página de error personalizada para códigos de estado HTTP específicos”.

   Para obtener más información, consulte la documentación del servicio de geolocalización que está utilizando.

Puede utilizar una variable de servidor web para obtener las direcciones IP de los usuarios que visitan su sitio web. Sin embargo, tenga en cuenta lo siguiente:

- Si su servidor web no está conectado a Internet a través de un equilibrador de carga, puede utilizar una variable de servidor web para obtener la dirección IP remota. Sin embargo, esta dirección IP no siempre es la del usuario. También puede ser la dirección IP de un servidor proxy, dependiendo de cómo esté el usuario conectado a Internet.
- Si su servidor web está conectado a Internet a través de un balanceador de carga, una variable de servidor web podría contener la dirección IP del balanceador de carga en lugar de la dirección IP del usuario. En esta configuración, le recomendamos utilizar la última dirección IP del encabezado HTTP `X-Forwarded-For`. Este encabezado normalmente contiene más de una dirección IP, la mayoría de los cuales son de proxis o balanceadores de carga. La última dirección IP de la lista tiene más posibilidades de asociarse a la ubicación geográfica del usuario.

Si su servidor web no está conectado a un equilibrador de carga, le recomendamos que utilice variables de servidor web en lugar del encabezado `X-Forwarded-For` para evitar la suplantación de direcciones IP.

Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial

Con Amazon CloudFront, puede aplicar conexiones integrales seguras a los servidores de origen mediante HTTPS. El cifrado en el nivel de campo añade una capa de seguridad adicional que le permite proteger datos específicos durante su procesamiento en el sistema de forma que solo determinadas aplicaciones puedan verlos.

El cifrado en el nivel de campo le permite facilitar a sus usuarios que carguen de manera segura información sensible a los servidores web. La información confidencial proporcionada por los usuarios se cifra en el borde, cerca del usuario y permanece cifrada en toda la pila de la aplicación. Este cifrado garantiza que solo las aplicaciones que necesitan los datos y que tienen las credenciales para descifrarlos puedan hacerlo.

Para utilizar cifrado en el nivel de campo, cuando configure la distribución de CloudFront, especifique el conjunto de campos de las solicitudes POST que desea cifrar y la clave pública que se va a usar para cifrarlos. Puede cifrar hasta 10 campos de datos en cada solicitud. (No puede cifrar todos los datos de una solicitud mediante el cifrado en el nivel de campo, debe especificar campos individuales).

Cuando la solicitud HTTPS con el cifrado en el nivel de campo se reenvía al origen y se transfiere por toda la aplicación o subsistema de origen, la información confidencial sigue estando cifrada, lo que reduce el riesgo de una infracción de los datos o una pérdida accidental de la información confidencial. Los componentes que necesitan obtener acceso a la información confidencial por motivos empresariales, como un sistema de procesamiento de pagos que necesita tener acceso a un número de tarjeta de crédito, pueden utilizar la clave privada apropiada para descifrar los datos y obtener acceso a ellos.

> **Note**
>
> Para utilizar el cifrado en el nivel de campo, el origen debe admitir la codificación fragmentada.

El cifrado en el nivel de campo de CloudFront utiliza cifrado asimétrico, también denominado cifrado de clave pública. Se proporciona una clave pública a CloudFront y toda la información confidencial especificada se cifra automáticamente. La clave proporcionada a CloudFront no se puede utilizar para descifrar los valores cifrados; esto solo puede hacerlo la clave privada.

Temas

- Información general del cifrado en el nivel de campo
- Configuración del cifrado en el nivel de campo
- Descifrado de campos de datos en el origen

Información general del cifrado en el nivel de campo

Los siguientes pasos proporcionan información general sobre la configuración del cifrado en el nivel de campo. Para conocer los pasos específicos, consulte Configuración del cifrado en el nivel de campo.

1. Obtener un par clave pública-clave privada. Debe obtener y agregar la clave pública antes de empezar a configurar el cifrado en el nivel de campo en CloudFront.
2. Crear un perfil de cifrado en el nivel de campo. Los perfiles de cifrado en el nivel de campo que se crean en CloudFront, definen los campos que se deben cifrar.
3. Crear una configuración de cifrado en el nivel de campo. Una configuración especifica los perfiles que se van a utilizar en función del tipo de contenido de la solicitud o de un argumento de consulta para cifrar campos de datos específicos. También puede elegir las opciones de comportamiento de reenvío de solicitudes que desee para diferentes escenarios. Por ejemplo: puede establecer el comportamiento para cuando el nombre del perfil especificado por el argumento de consulta en una URL de solicitud no exista en CloudFront.
4. Enlazar a un comportamiento de la caché. Enlace la configuración a un comportamiento de la caché de una distribución para especificar cuándo CloudFront debería cifrar los datos.

Configuración del cifrado en el nivel de campo

Siga estos pasos para empezar a utilizar el cifrado en el nivel de campo. Para obtener información sobre las cuotas (antes denominadas límites) en el cifrado en el nivel de campo, consulte Cuotas.

- Paso 1: Crear un par de claves RSA
- Paso 2: Agregar la clave pública a CloudFront
- Paso 3: Crear un perfil para el cifrado en el nivel de campo
- Paso 4: Crear una configuración
- Paso 5: Agregar una configuración a un comportamiento de la caché

Paso 1: Crear un par de claves RSA

Para comenzar, debe crear un par de claves RSA que incluya una clave pública y una clave privada. La clave pública permite a CloudFront cifrar datos y la clave privada permite que los componentes del origen descifren los campos que se han cifrado. Puede utilizar OpenSSL u otra herramienta para crear un par de claves. El tamaño de la clave debe ser de 2 048 bits.

Por ejemplo, si utiliza OpenSSL, puede ejecutar el siguiente comando para generar un par de claves con una longitud de 2048 bits y guardarlo en el archivo `private_key.pem`:

```
openssl genrsa -out private_key.pem 2048
```

El archivo resultante contiene tanto la clave pública como la privada. Para extraer la clave pública de dicho archivo, ejecute el siguiente comando:

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

El archivo de clave pública (`public_key.pem`) contiene el valor de clave cifrada que se pega en el paso siguiente.

Paso 2: Agregar la clave pública a CloudFront

Después de obtener el par de claves RSA, agregue la clave pública a CloudFront.

Para agregar la clave pública a CloudFront (consola)

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Clave pública.
3. Elija Add public key (Agregar clave pública).
4. En Key name (Nombre de la clave), escriba un nombre único para la clave. El nombre no puede tener espacios y solo puede incluir caracteres alfanuméricos, guiones bajos (_) y guiones (-). El número máximo de caracteres es 128.
5. En Key value (valor de clave), pegue el valor de clave codificado de la clave pública, incluidas las líneas `-----BEGIN PUBLIC KEY-----` y `-----END PUBLIC KEY-----`.
6. En Comment (Comentario), añada un comentario opcional. Por ejemplo, podría incluir la fecha de vencimiento de la clave pública.
7. Elija Add (Añadir).

Puede agregar más claves para utilizar con CloudFront repitiendo los pasos del procedimiento.

Paso 3: Crear un perfil para el cifrado en el nivel de campo

Después de añadir al menos una clave pública a CloudFront, cree un perfil que indique a este los campos que desea cifrar.

Para crear un perfil para el cifrado en el nivel de campo (consola)

1. En el panel de navegación, elija Field-level encryption (Cifrado en el nivel de campo).
2. Elija Create profile (Crear perfil).
3. Rellene los siguientes campos:

   Profile name (Nombre de perfil)

   Escriba un nombre único para el perfil. El nombre no puede tener espacios y solo puede incluir caracteres alfanuméricos, guiones bajos (_) y guiones (-). El número máximo de caracteres es 128.

   Public key name (Nombre de clave pública)

   En la lista desplegable, elija el nombre de la clave pública que ha agregado a CloudFront en el paso 2. CloudFront utiliza la clave para cifrar los campos especificados en este perfil.

   Provider name (Nombre de proveedor)

   Escriba una frase para ayudar a identificar la clave, como el proveedor del que ha obtenido el par de claves. Necesita esta información, junto con la clave privada, cuando las aplicaciones descifran los campos de datos. El nombre del proveedor no puede tener espacios y solo puede incluir caracteres alfanuméricos, dos puntos (:), guiones bajos (_) y guiones (-). El número máximo de caracteres es 128.

   Field name pattern to match (Patrón de coincidencia de nombres de campo)

   Escriba los nombres de los campos de datos o los patrones que identifican los nombres de los campos de datos de la solicitud que desea que CloudFront cifre. Elija la opción + para añadir todos los campos que desea cifrar con esta clave.

   Para el patrón de nombre de campo, puede escribir el nombre completo del campo de datos, como DateOfBirth, o solo la primera parte del nombre con un carácter comodín (*), como CreditCard*. El patrón de nombre de campo solo puede incluir caracteres alfanuméricos, corchetes ([y]), puntos (.), guiones bajos (_) y guiones (-), además del carácter comodín opcional (*).

   Asegúrese de que no utiliza caracteres solapados para diferentes patrones de nombre de campo. Por ejemplo, si tiene el patrón de nombre de campo ABC*, no puede añadir otro patrón de nombre de campo que sea AB*. Además, los nombres de los campos distinguen

entre mayúsculas y minúsculas, y que el número máximo de caracteres que puede utilizar es de 128.

Comentario

(Opcional) Escriba un comentario sobre este perfil. El número máximo de caracteres que puede utilizar es 128.

4. Tras rellenar los campos, elija Create profile (Crear perfil).
5. Si desea añadir más perfiles, elija Add profile (Añadir perfil).

Paso 4: Crear una configuración

Después de crear uno o varios perfiles de cifrado en el nivel de campo, cree una configuración que especifique el tipo de contenido de la solicitud que incluya los datos que se van a cifrar, el perfil que se va a utilizar para el cifrado y otras opciones que especifiquen cómo desea que CloudFront gestione el cifrado.

Por ejemplo, si CloudFront no puede cifrar los datos, puede especificar si CloudFront debería bloquear o reenviar una solicitud al origen en los siguientes casos:

- Cuando el tipo de contenido de una solicitud no está en una configuración: si no ha agregado un tipo de contenido a una configuración, puede especificar si CloudFront debería reenviar la solicitud con ese tipo de contenido al origen sin cifrar los campos de datos o bloquear la solicitud y devolver un error.

> **Note**
>
> Si agrega un tipo de contenido a una configuración pero no ha especificado el perfil con el que utilizarlo, CloudFront siempre reenvía las solicitudes con ese tipo de contenido al origen.

- Cuando se desconoce el nombre de perfil proporcionado en un argumento de consulta: si especifica el argumento de consulta de `fle-profile` con un nombre de perfil que no existe para la distribución, puede especificar si CloudFront debería enviar la solicitud al origen sin cifrar los campos de datos o bloquear la solicitud y devolver un error.

En una configuración, también puede especificar si al proporcionar un perfil como un argumento de consulta en una URL se anula el perfil que ha mapeado al tipo de contenido de esa consulta.

De forma predeterminada, CloudFront utiliza el perfil que ha mapeado a un tipo de contenido, si especifica uno. Esto le permite tener un perfil que se utiliza de forma predeterminada, pero también optar por aplicar un perfil diferente en determinadas solicitudes.

Así, por ejemplo, puede especificar (en la configuración) **`SampleProfile`** como el perfil de argumento de consulta que se va a utilizar. A continuación, puede utilizar la URL `https://d1234.cloudfront.net?fle-profile=SampleProfile` en lugar de `https://d1234.cloudfront.net`, para que CloudFront utilice **`SampleProfile`** para esta solicitud y no el perfil que ha configurado para el tipo de contenido de la solicitud.

Puede crear hasta 10 configuraciones para una única cuenta y, a continuación, asociar una de ellas al comportamiento de la caché de cualquier distribución para la cuenta.

Para crear una configuración para el cifrado en el nivel de campo (consola)

1. En la página Field-level encryption (Cifrado en el nivel de campo), elija Create configuration (Crear configuración).

   Nota: para poder ver la opción para crear una configuración, debe haber creado al menos un perfil.

2. Rellene los siguientes campos para especificar el perfil que se va a usar. (Algunos campos no se pueden cambiar).

   Content type (no se puede cambiar)

   El tipo del contenido está establecido en `application/x-www-form-urlencoded` y no se puede cambiar.

   Default profile ID (opcional)

   En la lista desplegable, elija el perfil al que desea mapear al tipo de contenido en el campo Content type (Tipo de contenido).

   Content format (no se puede cambiar)

   El formato del contenido está establecido en `URLencoded` y no se puede cambiar.

3. Si desea cambiar el comportamiento predeterminado de CloudFront para las siguientes opciones, seleccione la casilla de verificación correspondiente.

Forward request to origin when request's content type is not configured (Reenviar solicitud al origen cuando el tipo de contenido de la solicitud no está configurado)

Seleccione la casilla si desea permitir que la solicitud vaya al origen si no ha especificado el perfil que se va a utilizar para el tipo de contenido de la solicitud.

Override the profile for a content type with a provided query argument (Invalidar el perfil de un tipo de contenido con un argumento de consulta proporcionado)

Seleccione la casilla si desea permitir que un perfil proporcionado en un argumento de consulta anule el perfil que ha especificado para un tipo de contenido.

4. Si selecciona la casilla para permitir que un argumento de consulta anule el perfil predeterminado, debe rellenar los siguientes campos adicionales para la configuración. Puede crear hasta cinco de estos mapeos de argumentos de consulta para su uso con las consultas.

   Query argument (Argumento de consulta)

   Escriba el valor que desea incluir en las URL para el argumento de consulta `fle-profile`. Este valor indica a CloudFront que debe utilizar el ID de perfil (que especificará en el campo siguiente) asociado con este argumento de consulta para el cifrado en el nivel de campo de esta consulta.

   El número máximo de caracteres que puede utilizar es 128. El valor no puede incluir espacios, y solo se pueden utilizar caracteres alfanuméricos además de los siguientes caracteres: guion (-), punto (.), guion bajo (_), asterisco (*), signo más (+), porcentaje (%).

   Profile ID (ID de perfil)

   En la lista desplegable, elija el perfil que desea asociar al valor que ha especificado para Query argument (Argumento de consulta).

   Forward request to origin when the profile specified in a query argument does not exist (Reenviar solicitud al origen cuando el perfil especificado en una consulta no exista)

   Seleccione la casilla de verificación si desea permitir que la solicitud vaya al origen si el perfil especificado en un argumento de consulta no está definido en CloudFront.

Paso 5: Agregar una configuración a un comportamiento de la caché

Para utilizar el cifrado en el nivel de campo, enlace una configuración a un comportamiento de la caché de una distribución añadiendo el ID de configuración como un valor de dicha distribución.

> **Important**
>
> Para vincular una configuración de cifrado en el nivel de campo a un comportamiento de la caché, la distribución debe configurarse para que siempre use HTTPS y acepte las solicitudes HTTP `POST` y `PUT` de los espectadores. Es decir, se debe cumplir lo siguiente:
>
> - La Viewer Protocol Policy (política del protocolo del espectador) del comportamiento de la caché debe establecerse en Redirect HTTP to HTTPS (Redireccionamiento de HTTP a HTTPS) o HTTPS Only (solo HTTPS). (En CloudFormation o en la API de CloudFront, `ViewerProtocolPolicy` debe establecerse en `redirect-to-https` o `https-only`).
> - Los métodos HTTP permitidos del comportamiento de la caché deben establecerse en GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. (En CloudFormation o en la API de CloudFront, `AllowedMethods` se debe configurar en `GET`, `HEAD`, `OPTIONS`, `PUT`, `POST`, `PATCH`, `DELETE`. Estos se pueden especificar en cualquier orden).
> - La Origin Protocol Policy (política del protocolo de origen) de la configuración de origen debe establecerse en Match Viewer (coincidir con espectador) o HTTPS Only (solo HTTPS). (En CloudFormation o en la API de CloudFront, `OriginProtocolPolicy` debe establecerse en `match-viewer` o `https-only`).

Para obtener más información, consulte Referencia de toda la configuración de distribución.

Descifrado de campos de datos en el origen

CloudFront cifra los campos de datos mediante AWS Encryption SDK. Los datos permanecen cifrados en toda la pila de aplicaciones y únicamente pueden tener acceso a ellos las aplicaciones que dispongan de las credenciales para descifrarlos.

Tras el cifrado, el texto cifrado se codifica en base64. Cuando las aplicaciones descifran el texto en el origen, primero deben descodificar el texto cifrado y, a continuación, utilizar el SDK de cifrado de AWS para descifrar los datos.

El siguiente código de ejemplo ilustra cómo las aplicaciones pueden descifrar datos en el origen. Tenga en cuenta lo siguiente:

- Para simplificar el ejemplo, esta muestra carga claves públicas y privadas (en formato DER) desde archivos que se encuentran en el directorio de trabajo. En la práctica, debería almacenar la clave privada en una ubicación segura sin conexión, como un módulo de seguridad de hardware sin conexión, y distribuir la clave pública a su equipo de desarrollo.
- CloudFront utiliza información específica al cifrar los datos y se debería utilizar el mismo conjunto de parámetros en el origen para descifrarlos. Entre los parámetros que CloudFront utiliza al inicializar la clave maestra se incluyen los siguientes:
  - PROVIDER_NAME: este valor se especificó al crear un perfil de cifrado en el nivel de campo. Utilice aquí el mismo valor.
  - KEY_NAME: el nombre para la clave pública se creó al cargarla en CloudFront y, a continuación, se especificó el nombre de la clave en el perfil. Utilice aquí el mismo valor.
  - ALGORITHM: CloudFront utiliza `RSA/ECB/OAEPWithSHA-256AndMGF1Padding` como algoritmo para cifrar, por lo que debe usar el mismo algoritmo para descifrar los datos.
- Si ejecuta el siguiente programa de muestra con texto cifrado como entrada, los datos descifrados se muestran en la consola. Para obtener más información, consulte el código de ejemplo de Java del SDK de cifrado de AWS.

Código de muestra

```
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 bajo demanda y streaming de video en directo con CloudFront

Puede utilizar CloudFront para distribuir vídeo bajo demanda (VOD) o streaming de vídeo en directo con cualquier origen HTTP. Una manera de configurar flujos de trabajo de video en la nube consiste en utilizar CloudFront junto con AWSMedia Services.

Temas

- Acerca del streaming de vídeo
- Distribución de vídeo bajo demanda con CloudFront
- Distribución de video en streaming con CloudFront y los servicios multimedia de AWS
- Resiliencia basada en la calidad multimedia

Acerca del streaming de vídeo

Debe utilizar un codificador para empaquetar el contenido de vídeo para que CloudFront pueda distribuirlo. El proceso de empaquetado crea segmentos que contienen el contenido de audio, vídeo y subtítulos. También genera archivos de manifiesto, que describen en un orden específico qué segmentos hay que reproducir y cuándo. Los formatos comunes de los paquetes son MPEG DASH, HLS de Apple, Microsoft Smooth Streaming y CMAF.

Streaming de VOD

En el streaming de vídeo bajo demanda (VOD), el contenido de vídeo se almacena en un servidor y los espectadores pueden verlo en cualquier momento. Para crear un recurso que los espectadores puedan transmitir en streaming, utilice un codificador, como AWS Elemental MediaConvert, con el fin de formatear y empaquetar los archivos multimedia.

Un vez que el vídeo esté empaquetado en los formatos adecuados, puede almacenarlo en un servidor o en un bucket de Amazon S3 y, a continuación, distribuirlo con CloudFront a medida que lo soliciten los lectores.

Streaming de vídeo en directo

Para la transmisión en streaming de vídeo en directo, el contenido de vídeo se transmite en tiempo real a medida que ocurren los eventos en directo, o bien se configura como un canal en vivo ininterrumpido (24 horas al día, 7 días a la semana). Para crear salidas en directo para su

retransmisión y para su transmisión en streaming, utilice un codificador como AWS Elemental MediaLive para comprimir el vídeo y formatearlo para los dispositivos de visualización.

Una codificado el vídeo, puede almacenarlo en AWS Elemental MediaStore o convertirlo a distintos formatos de distribución mediante AWS Elemental MediaPackage. Con estos orígenes, puede configurar una distribución de CloudFront para distribuir el contenido. Si desea conocer los pasos específicos y obtener orientación para crear distribuciones que funcionen con estos servicios, consulte Distribución de vídeo utilizando AWS Elemental MediaStore como origen y Distribución de vídeo en directo formateado con AWS Elemental MediaPackage.

Wowza y Unified Streaming también proporcionan herramientas que puede utilizar para transmitir vídeo en streaming con CloudFront. Para obtener más información acerca de cómo utilizar Wowza con CloudFront, consulte el artículo sobre cómo llevar su licencia de Wowza Streaming Engine a streaming HTTP en directo con CloudFront en el sitio web de documentación de Wowza. Para obtener información sobre el uso de Unified Streaming con CloudFront para la transmisión en streaming de VOD, consulte CloudFront en el sitio web de documentación de Unified Streaming.

Distribución de vídeo bajo demanda con CloudFront

Para distribuir en streaming vídeo bajo demanda (VOD) con CloudFront, utilice los siguientes servicios:

- Amazon S3 para almacenar el contenido en su formato original y para almacenar el vídeo transcodificado.
- Un codificador (como AWS Elemental MediaConvert) para transcodificar el vídeo a los formatos de streaming.
- CloudFront para distribuir el vídeo transcodificado a los lectores. Para Microsoft Smooth Streaming, consulte Configuración de vídeo bajo demanda para Microsoft Smooth Streaming.

Para crear una solución VOD con CloudFront

1. Cargue su contenido a un bucket de Amazon S3. Para obtener más información sobre cómo trabajar con Amazon S3, consulte la Guía del usuario de Amazon Simple Storage Service.
2. Transcodifique su contenido mediante un trabajo de MediaConvert. El trabajo convierte el vídeo a los formatos requeridos por los reproductores que utilizan los espectadores. También puede utilizar el trabajo para crear recursos con diferentes resoluciones y velocidades de bits.

Estos activos se utilizan para la transmisión en streaming a velocidad de bits adaptable (ABR), que ajusta la calidad de visualización en función del ancho de banda disponible del lector. MediaConvert almacena el vídeo transcodificado en un bucket de S3.

3. Distribuya su contenido convertido mediante una distribución de CloudFront. Los espectadores pueden ver el contenido en cualquier dispositivo y en cualquier momento.

Configuración de vídeo bajo demanda para Microsoft Smooth Streaming

Dispone de las siguientes opciones para usar CloudFront con el fin de distribuir contenido de vídeo bajo demanda (VOD) que ha transcodificado al formato Microsoft Smooth Streaming:

- Especifique un servidor web que ejecute Microsoft IIS y sea compatible con Smooth Streaming como origen de la distribución.
- Habilite Smooth Streaming en los comportamientos de la caché de una distribución de CloudFront. Debido a que puede utilizar varios comportamientos de la caché en una distribución, puede utilizar una distribución para archivos multimedia de Smooth Streaming y también para otros contenidos.

> **Important**
>
> Si especifica un servidor web que ejecuta Microsoft IIS como origen, no habilite Smooth Streaming en los comportamientos de caché de la distribución de CloudFront. CloudFront no puede usar un servidor Microsoft IIS como origen si habilita Smooth Streaming como comportamiento de la caché.

Si habilita Smooth Streaming en un comportamiento de la caché (es decir, no tiene un servidor que ejecute Microsoft IIS), tenga en cuenta lo siguiente:

- Podrá seguir distribuyendo otro contenido mediante el mismo comportamiento de la caché si el contenido coincide con el valor de Path Pattern (Patrón de ruta) del comportamiento.
- CloudFront puede utilizar un bucket de Amazon S3 o un origen personalizado para los archivos multimedia de Smooth Streaming. CloudFront no puede utilizar un servidor Microsoft IIS como origen si habilita Smooth Streaming para el comportamiento de la caché.
- No puede invalidar archivos multimedia en formato Smooth Streaming. Si desea actualizar los archivos antes de que caduquen, debe cambiarles el nombre. Para obtener más información, consulte Agregación, eliminación o sustitución de contenido que distribuye CloudFront.

Para obtener más información acerca de los clientes de Smooth Streaming, consulte Smooth Streaming en el sitio web de documentación de Microsoft.

Para utilizar CloudFront con el fin de distribuir archivos de Smooth Streaming cuando el origen no es un servidor web de Microsoft IIS

1. Transcodifique los archivos multimedia en formato MP4 fragmentado de Smooth Streaming.
2. Aplique alguna de las siguientes acciones:
   - Si está utilizando la consola de CloudFront: al crear o actualizar una distribución, habilite Smooth Streaming en uno o varios de los comportamientos de la caché de la distribución.
   - Si está utilizando la API de CloudFront: agregue el elemento `SmoothStreaming` al tipo complejo `DistributionConfig` para uno o más de los comportamientos de la caché de la distribución.
3. Cargue los archivos de Smooth Streaming en su origen.
4. Cree un archivo `clientaccesspolicy.xml` o `crossdomainpolicy.xml` y añádalo a una ubicación accesible en la raíz de su distribución, por ejemplo, `https://d111111abcdef8.cloudfront.net/clientaccesspolicy.xml`. A continuación se muestra un ejemplo de política:

   ```
   <?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>
   ```

   Para obtener más información, consulte la sección sobre cómo hacer que un servicio esté disponible en los límites del dominio en el sitio web de Microsoft Developer Network.
5. Para los enlaces de la aplicación (por ejemplo, un reproductor multimedia), especifique la dirección URL del archivo multimedia en el formato siguiente:

```
https://d111111abcdef8.cloudfront.net/video/presentation.ism/Manifest
```

Distribución de video en streaming con CloudFront y los servicios multimedia de AWS

Para utilizar AWS Media Services con CloudFront y distribuir contenido en directo a un público global, siga las indicaciones de esta sección.

Use AWS Elemental MediaLive para codificar las transmisiones en streaming de vídeo en directo en tiempo real. Para codificar una transmisión en streaming de vídeo de gran tamaño, MediaLive la comprime en versiones más pequeñas (la codifica) que se pueden distribuir a los lectores.

Después de comprimir una transmisión en streaming de vídeo en directo, puede utilizar cualquiera de las dos opciones principales siguientes para preparar y distribuir el contenido:

- Convierta el contenido a los formatos requeridos y, a continuación, distribúyalo: si necesita contenido en varios formatos, use AWS Elemental MediaPackage para empaquetar el contenido para diferentes tipos de dispositivos. Al empaquetar el contenido, también puede implementar funciones adicionales y añadir la administración de derechos digitales (DRM) para evitar el uso no autorizado del contenido. Para obtener instrucciones paso a paso sobre el uso de CloudFront para servir contenido formateado por MediaPackage formateó, consulte Distribución de vídeo en directo formateado con AWS Elemental MediaPackage.
- Almacene y distribuya el contenido mediante un origen escalable: si MediaLive ha codificado el contenido en los formatos requeridos por todos los dispositivos que utilizan los espectadores, utilice un origen altamente escalable, como AWS Elemental MediaStore para distribuir el contenido. Para obtener instrucciones paso a paso sobre el uso de CloudFront para servir contenido almacenado en un contenedor de MediaStore, consulte Distribución de vídeo utilizando AWS Elemental MediaStore como origen.

Una vez que haya configurado el origen mediante una de estas opciones, ya puede distribuir streaming de vídeo en directo a los lectores con CloudFront.

> **Tip**
>
> Puede obtener información sobre una solución de AWS que implementa automáticamente servicios para crear una experiencia de visualización en tiempo real de alta disponibilidad.

Si desea ver los pasos para implementar automáticamente esta solución, consulte Implementación automatizada de streaming en directo.

Temas

- Distribución de vídeo utilizando AWS Elemental MediaStore como origen
- Distribución de vídeo en directo formateado con AWS Elemental MediaPackage
- Distribución de contenido de video bajo demanda con AWS Elemental MediaPackage

Distribución de vídeo utilizando AWS Elemental MediaStore como origen

Si almacena vídeo en un contenedor de AWS Elemental MediaStore, puede crear una distribución de CloudFront para distribuir el contenido.

Para empezar, conceda a CloudFront acceso a su contenedor de MediaStore. A continuación, cree una distribución de CloudFront y configúrela para que funcione con MediaStore.

Para distribuir contenido desde un contenedor de AWS Elemental MediaStore

1. Siga el procedimiento que se describe en Cómo permitir que Amazon CloudFront acceda a un contenedor de AWS Elemental MediaStore y, a continuación, vuelva a estos pasos para crear la distribución.
2. Cree una distribución con la siguiente configuración:
   a. Dominio de origen: el punto de conexión de datos que se ha asignado al contenedor de MediaStore. En la lista desplegable, elija el contenedor de MediaStore del vídeo en directo.
   b. Ruta de origen: la estructura de carpetas en el contenedor de MediaStore donde se almacenan sus objetos. Para obtener más información, consulte the section called “Ruta de origen”.
   c. Agregar encabezado personalizado: agregue nombres de encabezado y valores si desea que CloudFront agregue encabezados personalizados cuando reenvía solicitudes a su origen.
   d. Política de protocolo de visualización: elija Redirigir HTTP a HTTPS. Para obtener más información, consulte the section called “Política de protocolo para lectores”.
   e. Política de caché y política de solicitud de origen

- En Política de caché, elija Crear política y, a continuación, cree una política de caché adecuada a sus necesidades de caché y a la duración de los segmentos. Después de crear la política, actualice la lista de políticas de caché y, a continuación, elija la política que acaba de crear.
- En Política de solicitud de origen, elija CORS-CustomOrigin de la lista desplegable.

Para el resto de la configuración, puede establecer valores específicos en función de otros requisitos técnicos o de las necesidades de su empresa. Para ver una lista de todas las opciones de las distribuciones e información sobre su configuración, consulte the section called "Toda la configuración de distribución".

3. Para los enlaces de su aplicación (por ejemplo, un reproductor multimedia), especifique el nombre del archivo multimedia en el mismo formato que utiliza para otros objetos que distribuye con CloudFront.

Distribución de vídeo en directo formateado con AWS Elemental MediaPackage

Si ha utilizado AWS Elemental MediaPackage para dar formato a una transmisión en streaming en directo, puede crear una distribución de CloudFront y configurar los comportamientos de la caché para distribuir la transmisión en streaming en directo. En el siguiente proceso, se presupone que ya ha creado un canal y que ha agregado puntos de enlace para el vídeo en directo mediante MediaPackage.

Para crear una distribución de CloudFront para MediaPackage manualmente, siga estos pasos:

Paso 1: Cree y configure una distribución de CloudFront

Realice el procedimiento siguiente para configurar una distribución de CloudFront para el canal de vídeo en directo que ha creado con MediaPackage.

Para crear una distribución para el canal de vídeo en directo

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Crear distribución.
3. Elija la configuración de la distribución, incluido lo siguiente:

Dominio de origen

El origen donde están el canal de vídeo en directo y los puntos de enlace de MediaPackage. Elija el campo de texto y, a continuación, en la lista desplegable, elija el dominio de origen de MediaPackage para su vídeo en directo. Puede mapear un dominio a varios puntos de enlace de origen.

Si ha creado el dominio de origen con otra cuenta de AWS, escriba el valor de la URL de origen en el campo. El origen debe ser una URL HTTPS.

Por ejemplo, para un punto de conexión de HLS como `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, el dominio de origen es `3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com`.

Para obtener más información, consulte the section called “Dominio de origen”.

Ruta de origen

Ruta de acceso al punto de enlace de MediaPackage desde el que se distribuye el contenido.

Para obtener más información sobre el funcionamiento de una ruta de origen, consulte the section called “Ruta de origen”.

> **Important**
>
> La ruta comodín `*` es necesaria para enrutar a alguna parte de la distribución de CloudFront. Para evitar que las solicitudes que no coincidan con una ruta explícita se dirijan al origen real, cree un origen “ficticio” para esa ruta comodín.

Example: Creación de un origen ”ficticio”

En el siguiente ejemplo, los puntos de conexión `abc123` y `def456` enrutan al origen “real”, pero las solicitudes de contenido de vídeo de cualquier otro punto de conexión se dirigen a `mediapackage.us-west-2.amazonaws.com` sin el subdominio adecuado, lo que provoca un error HTTP `404`.

Puntos de conexión de MediaPackage:

```
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
```

Origen A de CloudFront:

```
Domain: 3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com
Path: None
```

Origen B de CloudFront:

```
Domain: mediapackage.us-west-2.amazonaws.com
Path: None
```

Comportamiento de caché de CloudFront:

```
1. Path: /out/v1/abc123/* forward to Origin A
2. Path: /out/v1/def456/* forward to Origin A
3. Path: * forward to Origin B
```

Para el resto de la configuración de la distribución, establezca valores específicos en función de otros requisitos técnicos o de las necesidades de su empresa. Para ver una lista de todas las opciones de las distribuciones e información sobre su configuración, consulte the section called "Toda la configuración de distribución".

Cuando termine de elegir la otra configuración de distribución, elija Crear distribución.

4. Elija la distribución que acaba de crear y, a continuación, elija la pestaña Comportamientos.
5. Elija el comportamiento de caché predeterminado y, a continuación, elija Editar. Especifique la configuración correcta de comportamiento de la caché para el canal que ha elegido como origen. Más adelante, añadirá uno o varios orígenes adicionales y editará la configuración de comportamiento de la caché para ellos.
6. Vaya a la página Distribuciones de CloudFront.
7. Espere hasta que el valor de la columna Última modificación de su distribución haya cambiado de Implementando a una fecha y hora, lo que indica que CloudFront ha creado su distribución.

Paso 2: Agregar orígenes para los dominios de sus puntos de conexión de MediaPackage

Repita aquí los pasos para agregar cada uno de los puntos de conexión de canal de MediaPackage a su distribución, teniendo en cuenta la necesidad de crear un origen “ficticio”.

Para añadir otros puntos de enlace como orígenes

1. En la consola de CloudFront, elija la distribución que creó para su canal.
2. Elija Orígenes y, a continuación, elija Crear origen.
3. En Nombre de dominio de origen, en la lista desplegable, elija un punto de conexión de MediaPackage para el canal.
4. Para el resto de la configuración, establezca los valores en función de otros requisitos técnicos o de las necesidades de su empresa. Para obtener más información, consulte the section called “Configuración de origen”.
5. Elija Crear origen.

Paso 3: Configurar los comportamientos de la caché para todos los puntos de enlace

Es necesario configurar los comportamientos de la caché de cada punto de enlace para añadir patrones de ruta que dirijan correctamente las solicitudes. Los patrones de ruta que especifique dependerán del formato de video que distribuya. El siguiente procedimiento incluye la información del patrón de ruta que se utilizará para los formatos Apple HLS, CMAF, DASH y Microsoft Smooth Streaming.

Normalmente, se configuran dos comportamientos de la caché para cada punto de enlace:

- El manifiesto principal, que es el índice de los archivos.
- Los segmentos, que son los archivos del contenido de vídeo.

Para crear un comportamiento de la caché para un punto de enlace

1. En la consola de CloudFront, elija la distribución que creó para su canal.
2. Elija Comportamientos y, a continuación, elija Crear comportamiento.
3. Para Patrón de ruta, utilice un GUID de `OriginEndpoint` de MediaPackage específico como prefijo de ruta.

Patrones de ruta

Para un punto de conexión HLS
como `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, cree los dos comportamientos de caché siguientes:

- Para manifiestos principales y secundarios, use `/out/v1/abc123/*.m3u8`.
- Para los segmentos de contenido, use `/out/v1/abc123/*.ts`.

Para un punto de conexión CMAF
como `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, cree los dos comportamientos de caché siguientes:

- Para manifiestos principales y secundarios, use `/out/v1/abc123/*.m3u8`.
- Para los segmentos de contenido, use `/out/v1/abc123/*.mp4`.

Para un punto de conexión DASH
como `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.mpd`, cree los dos comportamientos de caché siguientes:

- Para el manifiesto principal, use `/out/v1/abc123/*.mpd`.
- Para los segmentos de contenido, use `/out/v1/abc123/*.mp4`.

Para un punto de conexión de Microsoft Smooth Streaming
como `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.ism`, solo se sirve un manifiesto, por lo que solo se crea un comportamiento de caché: `out/v1/abc123/index.ism/*`.

4. Para cada comportamiento de la caché, especifique las siguientes opciones:

Política de protocolo para lectores

Elija Redireccionamiento de HTTP a HTTPS.

Política de caché y política de solicitud de origen

En Política de caché, elija Crear política. Para su nueva política de caché, especifique la siguiente configuración:

Tiempo de vida mínimo

Establézcalo en 5 segundos o menos, para ayudar a evitar la distribución de contenido obsoleto.

Cadenas de consulta

En Cadenas de consulta (en Configuración de la clave de caché), elija Incluir cadenas de consulta especificadas. Para Permitir, agregue los siguientes valores escribiéndolos y eligiendo Agregar elemento:

- Agregue `m` como parámetro de cadena de consulta que desea que CloudFront utilice como base para el almacenamiento en caché. La respuesta de MediaPackage siempre incluye la etiqueta `?m=###` para capturar la hora de modificación del punto de enlace. Si el contenido ya se encuentra en la memoria caché con un valor diferente para esta etiqueta, CloudFront solicita un nuevo manifiesto en lugar de distribuir la versión en caché.
- Si utiliza la funcionalidad de visualización en diferido de MediaPackage, especifique `start` y `end` como parámetros adicionales de la cadena de consulta en el comportamiento de la caché para las solicitudes de manifiesto (`*.m3u8`, `*.mpd` e `index.ism/*`). De esta forma, el contenido que se distribuye es específico del periodo de tiempo solicitado en la solicitud de manifiesto. Para obtener más información acerca de la visualización en diferido y cómo dar formato a los parámetros de solicitud de inicio y finalización del contenido, consulte Visualización en diferido en la Guía del usuario de AWS Elemental MediaPackage.
- Si está utilizando la característica de filtrado de manifiestos de MediaPackage, especifique `aws.manifestfilter` como parámetro adicional de cadena de consulta para la política de caché que use con el comportamiento de caché para las solicitudes de manifiesto (`*.m3u8`, `*.mpd` e `index.ism/*`). Esto configura la distribución para reenviar la cadena de consulta `aws.manifestfilter` a su origen de MediaPackage, lo que es necesario para que funcione la característica de filtrado de manifiestos. Para obtener más información, consulte Filtrado de manifiestos en la Guía del usuario de AWS Elemental MediaPackage.
- Si utiliza HLS de baja latencia (LL-HLS), especifique `_HLS_msn` y `_HLS_part` como parámetros adicionales de cadena de consulta para la política de caché que utiliza con el comportamiento de caché para solicitudes de manifiesto (`*.m3u8`). Esto configura su distribución para reenviar las cadenas de consulta `_HLS_msn` y `_HLS_part` a su origen de MediaPackage, lo cual es necesario para que funcione la característica de solicitud de listas de reproducción de bloqueo LL-HLS.

5. Seleccione Crear.

6. Después de crear la política de caché, vuelva al flujo de trabajo de creación del comportamiento de caché. Actualice la lista de políticas de caché y elija la política que acaba de crear.
7. Elija Crear comportamiento.
8. Si su punto de conexión no es un punto de conexión de Microsoft Smooth Streaming, repita estos pasos para crear un segundo comportamiento de caché.

Paso 4: Habilitar la autorización CDN de MediaPackage basada en encabezados

Recomendamos habilitar la Autorización CDN de MediaPackage basada en encabezados entre los puntos de conexión de MediaPackage y la distribución de CloudFront. Para obtener más información, consulte Habilitar la autorización CDN en MediaPackage en la Guía del usuario de AWS Elemental MediaPackage.

Paso 5: Utilizar CloudFront para servir el canal de transmisión en directo

Después de crear la distribución, agregar los orígenes, crear los comportamientos de caché y habilitar la autorización CDN basada en encabezados, puede servir el canal de transmisión en directo mediante CloudFront. CloudFront enruta las solicitudes de los lectores a los puntos de enlace correctos de MediaPackage en función de los ajustes configurados para los comportamientos de la caché.

Para los enlaces de la aplicación (por ejemplo, un reproductor multimedia), especifique la dirección URL del archivo multimedia en el formato estándar de las URL de CloudFront. Para obtener más información, consulte the section called “Personalización de URL de archivo”.

Distribución de contenido de video bajo demanda con AWS Elemental MediaPackage

Si origina el contenido de video bajo demanda (VOD) desde un origen de AWS Elemental MediaPackage, puede crear una distribución de CloudFront y configurar comportamientos de caché optimizados para distribuir el contenido de VOD a los espectadores. El siguiente proceso supone que ya ha creado un grupo de empaquetado con una configuración de empaquetado e ingerido un activo con MediaPackage.

Para crear una distribución de CloudFront para MediaPackage manualmente, siga estos pasos:

Paso 1: Cree y configure una distribución de CloudFront

Realice el procedimiento siguiente para configurar una distribución de CloudFront para el grupo de empaquetado que ha creado con MediaPackage.

Para crear una distribución para su contenido de VOD

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija Crear distribución.
3. Elija la configuración de la distribución, incluido lo siguiente:

   Dominio de origen

   El origen de su grupo de empaquetado de MediaPackage. Escriba el valor de la URL de origen en el campo de texto. El origen debe ser una URL HTTPS.

   Por ejemplo, para un punto de conexión de HLS como `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, el dominio de origen es `3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com`.

   Para obtener más información, consulte the section called “Dominio de origen”.

   Ruta de origen

   Ruta de acceso desde el que se distribuye el contenido.

   Para obtener más información sobre el funcionamiento de una ruta de origen, consulte the section called “Ruta de origen”.

   > **Important**
   >
   > La ruta comodín `*` es necesaria para enrutar a alguna parte de la distribución de CloudFront. Para evitar que las solicitudes que no coincidan con una ruta explícita se dirijan al origen real, cree un origen “ficticio” para esa ruta comodín.

Example: Creación de un origen ”ficticio”

En el siguiente ejemplo, las configuraciones de empaquetado `def456` y `321xyz` dirigen al origen “real”, pero las solicitudes de contenido de video de cualquier otro contenido de video se dirigen a `mediapackage-vod.us-west-2.amazonaws.com` sin el subdominio adecuado, lo que provoca un error HTTP `404`.

URL del contenido de MediaPackage para un solo activo para un grupo de empaquetado con dos configuraciones de empaquetado:

```
https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/
abc123/def456/ghi789/index.m3u8
https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/
abc123/321xyz/654uvw/index.m3u8
```

Origen A de CloudFront:

```
Domain: 3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com
Path: None
```

Origen B de CloudFront:

```
Domain: mediapackage-vod.us-west-2.amazonaws.com
Path: None
```

Comportamiento de caché de CloudFront:

```
1. Path: /out/v1/*/def456/* forward to Origin A
2. Path: /out/v1/*/321xyz/* forward to Origin A
3. Path: * forward to Origin B
```

Para el resto de la configuración de la distribución, establezca valores específicos en función de otros requisitos técnicos o de las necesidades de su empresa. Para ver una lista de todas las opciones de las distribuciones e información sobre su configuración, consulte the section called “Toda la configuración de distribución”.

Cuando termine de elegir la otra configuración de distribución, elija Crear distribución.

4. Elija la distribución que acaba de crear y, a continuación, elija la pestaña Comportamientos.
5. Elija el comportamiento de caché predeterminado y, a continuación, elija Editar. Especifique la configuración correcta de comportamiento de la caché para la configuración de empaquetado que ha elegido como origen. Más adelante, añadirá uno o varios orígenes adicionales y editará la configuración de comportamiento de la caché para ellos.
6. Vaya a la página Distribuciones de CloudFront.
7. Espere hasta que el valor de la columna Última modificación de su distribución haya cambiado de Implementando a una fecha y hora, lo que indica que CloudFront ha creado su distribución.

Paso 2: Adición de orígenes para los dominios de sus grupos de empaquetado de MediaPackage

Repita aquí los pasos para agregar cada uno de los grupos de empaquetado de MediaPackage a su distribución, teniendo en cuenta la necesidad de crear un origen “ficticio”.

Para agregar otros grupos de empaquetado como orígenes

1. En la consola de CloudFront, elija la distribución que creó para su canal.
2. Elija Orígenes y, a continuación, elija Crear origen.
3. En Dominio de origen, escriba la URL del grupo de empaquetado de MediaPackage.
4. Para el resto de la configuración, establezca los valores en función de otros requisitos técnicos o de las necesidades de su empresa. Para obtener más información, consulte the section called “Configuración de origen”.
5. Elija Crear origen.

Paso 3: Configuración de los comportamientos de la caché para todas las configuraciones de empaquetado

Es necesario configurar los comportamientos de la caché de cada configuración de empaquetado para añadir patrones de ruta que dirijan correctamente las solicitudes. Los patrones de ruta que especifique dependerán del formato de video que distribuya. El siguiente procedimiento incluye la información del patrón de ruta que se utilizará para los formatos Apple HLS, CMAF, DASH y Microsoft Smooth Streaming.

Normalmente, se configuran varios comportamientos de la caché para cada configuración de empaquetado:

- El manifiesto principal, que es el índice de los archivos.

- Los segmentos, que son los archivos del contenido de vídeo. Un formato puede usar más de una extensión para el contenido, según la configuración. Se necesita un comportamiento de caché para cada extensión.

Para crear un comportamiento de la caché para una configuración de empaquetado

1. En la consola de CloudFront, elija la distribución que creó para su canal.
2. Elija Comportamientos y, a continuación, elija Crear comportamiento.
3. En Patrón de ruta, utilice un GUID de configuración de empaquetado VOD de MediaPackage específico como prefijo de ruta. Este es el segundo GUID de una ruta VOD de MediaPackage.

   Patrones de ruta

   Para contenido HLS como `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, cree los comportamientos de caché siguientes:

   - Para manifiestos principales y secundarios, use `/out/v1/*/def456/*.m3u8`.
   - Para los segmentos de contenido, use `/out/v1/*/def456/*.ts` y repita para todas las extensiones de segmento necesarias.

   Para contenido CMAF como `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, cree los comportamientos de caché siguientes:

   - Para manifiestos principales y secundarios, use `/out/v1/*/def456/*.m3u8`.
   - Para los segmentos de contenido, use `/out/v1/*/def456/*.mp4` y repita para todas las extensiones de segmento necesarias.

   Para contenido DASH como `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.mpd`, cree los comportamientos de caché siguientes:

   - Para el manifiesto principal, use `/out/v1/*/def456/*.mpd`.
   - Para los segmentos de contenido, use `/out/v1/*/def456/*.mp4`.

   Para un punto de conexión de Microsoft Smooth Streaming como `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.ism/Manifest`,

solo se sirve un manifiesto, por lo que solo se crea un comportamiento de caché: `out/v1/*/def456/*/index.ism/*`.

4. Para cada comportamiento de la caché, especifique las siguientes opciones:

   Política de protocolo para lectores

   Elija Redireccionamiento de HTTP a HTTPS.

   Política de caché y política de solicitud de origen

   En Política de caché, elija Crear política. Para su nueva política de caché, especifique la siguiente configuración:

   Tiempo de vida mínimo

   Establézcalo en 5 segundos o menos, para ayudar a evitar la distribución de contenido obsoleto.

   Cadenas de consulta

   En Cadenas de consulta (en Configuración de la clave de caché), elija Incluir cadenas de consulta especificadas. Para Permitir, agregue los siguientes valores escribiéndolos y eligiendo Agregar elemento:

   - Si está utilizando la característica de filtrado de manifiestos de MediaPackage, especifique `aws.manifestfilter` como parámetro adicional de cadena de consulta para la política de caché que use con el comportamiento de caché para las solicitudes de manifiesto (`*.m3u8`, `*.mpd` e `index.ism/*`). Esto configura la distribución para reenviar la cadena de consulta `aws.manifestfilter` a su origen de MediaPackage, lo que es necesario para que funcione la característica de filtrado de manifiestos. Para obtener más información, consulte Filtrado de manifiestos en la Guía del usuario de AWS Elemental MediaPackage.

5. Seleccione Crear.
6. Después de crear la política de caché, vuelva al flujo de trabajo de creación del comportamiento de caché. Actualice la lista de políticas de caché y elija la política que acaba de crear.
7. Elija Crear comportamiento.
8. Si su punto de conexión no es un punto de conexión de Microsoft Smooth Streaming, repita estos pasos para crear un segundo comportamiento de caché.

Paso 4: Habilitar la autorización CDN de MediaPackage basada en encabezados

Recomendamos habilitar la Autorización CDN de MediaPackage basada en encabezados entre el contenido VOD de MediaPackage y la distribución de CloudFront. Para obtener más información, consulte Habilitar la autorización CDN en MediaPackage en la Guía del usuario de AWS Elemental MediaPackage.

Paso 5: Uso de CloudFront para distribuir contenido VOD

Después de crear la distribución, agregar los orígenes, crear los comportamientos de caché y habilitar la autorización CDN basada en encabezados, puede distribuir el contenido VOD mediante CloudFront. CloudFront dirige las solicitudes de los espectadores al contenido VOD correcto de MediaPackage en función de los ajustes configurados para los comportamientos de la caché.

Para los enlaces de la aplicación (por ejemplo, un reproductor multimedia), especifique la dirección URL del archivo multimedia en el formato estándar de las URL de CloudFront. Para obtener más información, consulte the section called “Personalización de URL de archivo”.

Resiliencia basada en la calidad multimedia

La resiliencia basada en la calidad multimedia (MQAR) es una capacidad integrada entre Amazon CloudFront y los servicios multimedia de AWS. MQAR ofrece una selección automática del origen entre regiones en función de la puntuación de confianza de calidad multimedia (MQCS). AWS Elemental MediaLive sintetiza MQCS en función de parámetros que afectan a la experiencia de calidad multimedia percibida por los espectadores. Puede configurar CloudFront y los servicios multimedia de AWS Media Services para que transmitan sus eventos en streaming en directo con alta resiliencia mediante varias opciones que puede especificar en los criterios de conmutación por error del grupo de origen de CloudFront.

Al activar la característica MQAR para su distribución, autoriza a CloudFront a seleccionar automáticamente el origen que se considere que tiene la puntuación de calidad más alta.

La puntuación de calidad representa los problemas de calidad del streaming de contenido multimedia percibidos desde sus orígenes, como fotogramas negros, fotogramas congelados o perdidos, o fotogramas repetidos. Por ejemplo, si sus orígenes de AWS Elemental MediaPackage v2 se implementan en dos Regiones de AWS diferentes y una obtiene una puntuación de calidad multimedia más alta que la otra, CloudFront cambiará automáticamente al origen con la puntuación más alta.

Para ello, CloudFront hace lo siguiente:

1. CloudFront reenvía una solicitud `GET` al origen principal de MediaPackage y, al mismo tiempo, inicia una solicitud `HEAD` al origen de MediaPackage secundario. CloudFront recibe la puntuación de calidad multimedia en los encabezados de respuesta de cada origen.
2. A continuación, CloudFront realiza un seguimiento de la puntuación de cada origen y utiliza esta información para determinar el origen con la puntuación más alta cuando llega una nueva solicitud.

La puntuación de calidad multimedia de sus orígenes puede cambiar en tiempo real. CloudFront lo determina consumiendo los cambios de MQCS y cambia de origen para garantizar que los espectadores vean el contenido multimedia de mayor calidad. Para obtener más información, consulte Leveraging media quality scores with MediaPackage en la Guía del usuario de AWS Elemental MediaPackage V2.

MQAR ayuda a CloudFront a determinar, lo antes posible, si existe un problema que podría afectar a los clientes. Por ejemplo, problemas como la conexión de red, el procesamiento del video, las pérdidas o caídas del audio o los problemas de velocidad del codificador pueden afectar a la puntuación de calidad multimedia de los espectadores.

MQAR permite cambiar de un origen a otro sin problemas, lo que le permite implementar un flujo de trabajo de entrega multimedia integral y resiliente entre regiones en AWS y ofrecer contenido de calidad a sus espectadores.

> **Note**
>
> Actualmente, esta característica solo admite los orígenes de MediaPackage v2.

Para habilitar esta característica en su distribución, complete los siguientes pasos:

1. Si aún no lo ha hecho, cree sus orígenes de MediaPackage v2 y habilite esta característica en la configuración de su punto de conexión. Para una implementación entre regiones, cree un canal secundario en una Región de AWS diferente con la misma configuración. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS Elemental MediaPackage V2:
   - Create a channel and endpoint
   - Enable the media quality score

2. Para utilizar sus orígenes de MediaPackage v2 en CloudFront, cree o actualice una distribución de CloudFront. Consulte Creación de una distribución y Actualizar una distribución.
3. Cree un grupo de origen y seleccione sus dos orígenes como principal y secundario. En su grupo de origen, active la opción Puntuación de calidad multimedia. Para obtener más información, consulte Creación de un grupo de origen.
4. En el comportamiento de la caché de su distribución, seleccione el grupo de origen que creó. Se recomienda que el comportamiento de la caché coincida con el patrón de la ruta del canal.

Si CloudFront determina que ambos orígenes de MediaPackage v2 tienen la misma puntuación, reenvía la solicitud al origen principal tal como aparece en el grupo de origen. Si el origen seleccionado inicialmente responde con un código de error que coincide con los criterios de conmutación por error que especificó en el grupo de origen, CloudFront vuelve a intentar enviar la solicitud al origen alternativo del grupo de origen, independientemente de su puntuación de calidad multimedia.

Notas

- CloudFront realiza un seguimiento de la puntuación de calidad de cada comportamiento de la caché que utiliza un grupo de origen habilitado para la puntuación de calidad multimedia. Si se utiliza el mismo grupo de origen para varios canales que emiten una puntuación de calidad multimedia, cree un comportamiento de caché diferente para el patrón de ruta de cada canal a fin de evitar mezclar las puntuaciones. Para obtener más información sobre las cuotas de grupos de origen, consulte Cuotas generales de distribuciones.
- Actualmente, MQAR no está disponible cuando utiliza una función de Lambda@Edge en desencadenadores orientados al origen (solicitud de origen y respuesta de origen) que están asociados al comportamiento de la caché de su distribución. Para obtener más información, consulte Configuración del comportamiento de la caché.
- Si ha activado la característica MQAR y el control de acceso de origen (OAC), agregue la acción `mediapackagev2:GetHeadObject` a la política de IAM. MQAR requiere este permiso para enviar solicitudes `HEAD` al origen de MediaPackage v2. Para obtener más información sobre OAC, consulte Restricción del acceso a un origen de AWS Elemental MediaPackage v2.

Campos de registro de MQAR

CloudFront proporciona los siguientes campos en los registros de acceso en tiempo real para reflejar la puntuación de calidad y el origen seleccionado. Puede habilitar estos campos en los registros en tiempo real de CloudFront:

- `r-host`
- `sr-reason`
- `x-edge-mqcs`

Para obtener más información, consulte Campos 65-67.

Personalización en la periferia con funciones

Con Amazon CloudFront, puede escribir su propio código para personalizar la forma en que sus distribuciones de CloudFront procesan las solicitudes y respuestas HTTP. El código se ejecuta cerca de los lectores (usuarios) para minimizar la latencia y no es necesario administrar servidores u otra infraestructura. Puede escribir código para manipular las solicitudes y respuestas que atraviesan CloudFront, realizar autenticación y autorización básicas, generar respuestas HTTP en el borde y mucho más.

El código que escribe y asocia a su distribución de CloudFront se denomina función de borde. CloudFront ofrece dos formas de escribir y administrar funciones de borde:

CloudFront Functions

Puede escribir funciones ligeras en JavaScript para personalizaciones de CDN sensibles a la latencia a gran escala. El entorno de tiempo de ejecución de CloudFront Functions ofrece tiempos de arranque de submilisegundos, se escala inmediatamente para gestionar millones de solicitudes por segundo y es altamente seguro. CloudFront Functions es una característica nativa de CloudFront, lo que significa que puede compilar, probar e implementar su código completamente dentro de CloudFront.

Lambda@Edge

Lambda@Edge: es una extensión de AWS Lambda que ofrece computación potente y flexible para funciones complejas y lógica completa de aplicaciones más cerca de sus lectores y es altamente segura. Las funciones de Lambda@Edge se ejecutan en un entorno de tiempo de ejecución Node.js o Python. Usted publica las funciones en una sola Región de AWS y, cuando asocia la función a una distribución de CloudFront, Lambda@Edge replica el código en todo el mundo de forma automática.

Si ejecuta AWS WAF en CloudFront, puede usar encabezados AWS WAF incrustados para CloudFront Functions y Lambda @Edge. Esto funciona para solicitudes y respuestas de lectores y de origen.

Temas

- Diferencias entre CloudFront Functions y Lambda@Edge
- Personalización en la periferia con CloudFront Functions
- Personalización con funciones de conexión de CloudFront

- Personalización en la periferia con Lambda@Edge
- Restricciones en funciones de borde

Diferencias entre CloudFront Functions y Lambda@Edge

CloudFront Functions y Lambda@Edge proporcionan una forma de ejecutar código en respuesta a eventos de CloudFront.

CloudFront Functions es ideal para funciones ligeras y de corta duración para los siguientes casos de uso:

- Normalización de la clave de caché: transforme los atributos de la solicitud HTTP (encabezados, cadenas de consulta, cookies o hasta la ruta de la URL) para crear una clave de caché óptima, lo que puede mejorar la tasa de aciertos de la caché.
- Manipulación de encabezados: inserte, modifique o elimine encabezados HTTP en la solicitud o la respuesta. Por ejemplo, puede agregar un encabezado `True-Client-IP` a cada solicitud.
- Redireccionamientos o reescrituras de URL: redirija a los lectores a otras páginas en función de la información de la solicitud o puede redirigir todas las solicitudes de una ruta a otra.
- Autorización de solicitudes: valide los tokens de autorización con hash, como los tokens web JSON (JWT) mediante la inspección de los encabezados de autorización u otros metadatos de solicitud.

Para empezar a utilizar CloudFront Functions, consulte Personalización en la periferia con CloudFront Functions.

Lambda@Edge es ideal para los siguientes casos de uso:

- Funciones que tardan varios milisegundos o más en completarse
- Funciones que requieren CPU o memoria ajustable
- Funciones que dependen de bibliotecas de terceros (incluido el SDK de AWS, para la integración con otros Servicios de AWS)
- Funciones que requieren acceso a la red para utilizar servicios externos para el procesamiento
- Funciones que requieren acceso al sistema de archivos o acceso al cuerpo de las solicitudes HTTP

Para comenzar con Lambda@Edge, consulte Personalización en la periferia con Lambda@Edge.

Para ayudarle a elegir la opción para su caso de uso, utilice la siguiente tabla con el fin de entender las diferencias entre CloudFront Functions y Lambda@Edge. Para obtener información sobre las diferencias que se aplican a los métodos auxiliares para la modificación del origen, consulte Elección entre CloudFront Functions y Lambda@Edge.

	CloudFront Functions	Lambda@Edge
Lenguajes de programación	JavaScript (compatible con ECMAScript 5.1)	Node.js y Python
Orígenes de eventos	• Solicitud del lector • Respuesta del lector	• Solicitud del lector • Respuesta del lector • Solicitud del origen • Respuesta del origen
Admite Amazon CloudFront KeyValueStore	Sí CloudFront KeyValueStore solo admite JavaScript runtime 2.0	No
Escalado	Hasta millones de solicitudes por segundo	Hasta 10 000 solicitudes por segundo por región
Duración de función	Submilisegundo	Hasta 30 segundos (solicitud del lector y respuesta del lector) Hasta 30 segundos (solicitud de origen y respuesta de origen)
Tamaño de memoria de función máxima	2 MB	128 MB (solicitud del lector y respuesta del lector) 10 240 MB (10 GB) (solicitud de origen y respuesta de origen)

	CloudFront Functions	Lambda@Edge
		Para obtener más información, consulte Cuotas de Lambda@Edge.
Tamaño máximo del código de función y bibliotecas incluidas	10 KB	50 MB (solicitud del espectador y respuesta del espectador) 50 MB (solicitud de origen y respuesta de origen)
Acceso a la red	No	Sí
Acceso al sistema de archivos	No	Sí
Acceso al cuerpo de solicitud	No	Sí
Acceso a datos de geolocalización y dispositivos	Sí	No (solicitud del lector y respuesta del lector) Sí (solicitud de origen y respuesta de origen)
Se puede compilar y probar completamente dentro de CloudFront	Sí	No
Registro y métricas de funciones	Sí	Sí

Personalización en la periferia con CloudFront Functions

Con CloudFront Functions, puede escribir funciones ligeras en JavaScript para personalizaciones de CDN sensibles a la latencia a gran escala. Sus funciones pueden manipular las solicitudes y respuestas que atraviesan CloudFront, realizar autenticaciones y autorizaciones básicas, generar respuestas HTTP en el borde y mucho más. El entorno de tiempo de ejecución de CloudFront Functions ofrece tiempos de arranque de submilisegundos, se escala inmediatamente para gestionar millones de solicitudes por segundo y es altamente seguro. CloudFront Functions es una

característica nativa de CloudFront, lo que significa que puede compilar, probar e implementar su código completamente dentro de CloudFront.

Cuando asocia una distribución de CloudFront con una función de CloudFront, CloudFront intercepta solicitudes y respuestas en ubicaciones de borde de CloudFront y ejecuta la función. Puede invocar CloudFront Functions cuando se producen los siguientes eventos:

- Cuando CloudFront reciba una solicitud de un espectador (solicitud del espectador)
- Antes de que CloudFront devuelva la respuesta al espectador (respuesta al espectador)
- Durante el establecimiento de la conexión de TLS (solicitud de conexión): actualmente disponible para conexiones de TLS mutuas (mTLS)

Para obtener más información sobre CloudFront Functions, consulte los siguientes temas:

Temas

- Tutorial: creación de una función simple con CloudFront Functions
- Tutorial: creación de una función de CloudFront que incluya pares clave-valor
- Escritura de código de función
- Creación de funciones
- Prueba de funciones
- Actualización de funciones
- Publicación de funciones
- Asociación de funciones con distribuciones
- Amazon CloudFront KeyValueStore

Tutorial: creación de una función simple con CloudFront Functions

En este tutorial se muestra cómo familiarizarse con CloudFront Functions. Puede crear una función simple que redirige el lector a una URL diferente y también devuelve un encabezado de respuesta personalizado.

Contenido

- Requisitos previos
- Creación de la función
- Verificación de la función

Requisitos previos

Para utilizar CloudFront Functions, necesita una distribución de CloudFront. Si no dispone de una, consulte Introducción a una distribución estándar de CloudFront.

Creación de la función

Puede utilizar la consola de CloudFront para crear una función simple que redirige el lector a una URL diferente y también devuelve un encabezado de respuesta personalizado.

Creación de una función de CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, seleccione Funciones y, a continuación, Crear una función.
3. En la página Crear función, en Nombre, introduzca un nombre de función como *MyFunctionName*.
4. (Opcional) En Descripción, escriba una descripción de la función, como **Simple test function**.
5. Para Tiempo de ejecución, mantenga la versión de JavaScript seleccionada de forma predeterminada.
6. Elija Crear función.
7. Copie el siguiente código de función. Este código de función redirige al lector a una URL diferente y también devuelve un encabezado de respuesta personalizado.

```
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. En Código de función, pegue el código en el editor de código para reemplazar el código predeterminado.
9. Elija Guardar cambios.
10. (Opcional) Puede probar la función antes de publicarla. En este tutorial no se describe cómo probar una función. Para obtener más información, consulte Prueba de funciones.
11. Elija la pestaña Publicar y, a continuación, la función Publicar. Debe publicar la función para poder asociarla a la distribución de CloudFront.
12. A continuación, puede asociar la función a un comportamiento de distribución o caché. En la página *MyFunctionName*, elija la pestaña Publicar.

    > **Warning**
    >
    > En los pasos siguientes, seleccione un comportamiento de distribución o caché que se use para las pruebas. No asocie esta función de prueba a un comportamiento de distribución o caché que se use en producción.

13. Elija Add association.
14. En el cuadro de diálogo Asociar, elija un comportamiento de distribución o caché. En Tipo de evento, mantenga el valor predeterminado.
15. Elija Add association.

    También verá la distribución asociada en la tabla Distribuciones asociadas.
16. Espere unos minutos para que la distribución asociada termine de implementarse. Para comprobar el estado de la distribución, selecciónela en la tabla Distribuciones asociadas y elija Ver distribución.

    Cuando el estado de la distribución es Implementada, está lista para verificar el funcionamiento de la función.

Verificación de la función

Tras implementar la función, puede comprobar que funciona para su distribución.

Verificación de la función

1. En el navegador web, vaya al nombre de dominio de la distribución (por ejemplo, `https://d111111abcdef8.cloudfront.net`).

La función devuelve un redireccionamiento al navegador, por lo que el navegador se dirige automáticamente a `https://aws.amazon.com/cloudfront/`.

2. En una ventana de línea de comandos, puede usar una herramienta como curl para enviar una solicitud al nombre de dominio de su distribución.

```
curl -v https://d111111abcdef8.cloudfront.net/
```

En la respuesta, verá la respuesta de redireccionamiento (`302 Found`) y los encabezados de respuesta personalizados que agregó la función. La respuesta podría tener un aspecto similar al siguiente.

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: creación de una función de CloudFront que incluya pares clave-valor

En este tutorial, se muestra cómo incluir pares clave-valor con una función de CloudFront. Los valores y las claves forman parte de un par clave-valor. Debe incluir el nombre (del par clave-valor) en el código de la función. Cuando se ejecute la función, CloudFront reemplaza el nombre por el valor.

Los pares clave-valor son variables que se almacenan en un almacén de clave-valor. Cuando se utiliza una clave en la función (en lugar de valores con codificación rígida), la función es más flexible. Puede cambiar el valor de la clave sin tener que implementar cambios en el código. Los pares clave-valor también pueden reducir el tamaño de la función. Para obtener más información, consulte ???.

Contenido

- Requisitos previos
- Creación del almacén de clave-valor
- Añadido de pares clave-valor al almacén
- Asociación del almacén de clave-valor a la función
- Prueba y publicación del código de la función

Requisitos previos

Si no conoce las funciones de CloudFront Functions ni el almacén de clave-valor, le recomendamos que siga el tutorial que aparece en the section called “Tutorial: creación de una función simple de CloudFront”.

Después de completar ese tutorial, puede seguir este tutorial para ampliar la función que ha creado. En este tutorial, le recomendamos que primero cree el almacén de clave-valor.

Creación del almacén de clave-valor

En primer lugar, cree el almacén de clave-valor para usarlo en su función.

Creación del almacén clave-valor

1. Planifique los pares clave-valor que desee incluir en la función. Anote los nombres de las claves. Los pares clave-valor que desee utilizar en una función deben estar en un único almacén de clave-valor.
2. Decida el orden de trabajo. Hay dos formas de proceder:
   - Cree un almacén de clave-valor y añada pares clave-valor al almacén. A continuación, cree (o modifique) la función e incorpore los nombres de las claves.
   - O bien, puede crear (o modificar) la función e incorporar los nombres de las claves que quiera usar. A continuación, cree un almacén de clave-valor y añada los pares clave-valor.

3. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
4. En el panel de navegación, elija Funciones y, a continuación, elija la pestaña KeyValueStores.
5. Elija Crear KeyValueStore e introduzca los siguientes campos:
   - Introduzca un nombre y una descripción (opcional) para el almacén.
   - Deje el URI de S3 en blanco. En este tutorial, introducirá los pares clave-valor de forma manual.
6. Seleccione Crear. Aparece la página de detalles del nuevo almacén de clave-valor. Esta página incluye una sección de pares clave-valor que actualmente está vacía.

Añadido de pares clave-valor al almacén

A continuación, añada manualmente una lista de pares clave-valor al almacén de clave-valor que creó anteriormente.

Añadido de pares clave-valor al almacén de clave-valor

1. En la sección de Pares clave-valor, seleccione el botón Agregar pares clave-valor.
2. Elija Agregar etiqueta y, a continuación, introduzca un par clave-valor. Elija la marca de verificación para confirmar los cambios y repita este paso para añadir más.
3. Cuando haya terminado, seleccione Guardar cambios para guardar todos los pares del almacén de clave-valor. En el cuadro de diálogo de confirmación, elija Listo.

Ahora tiene un almacén que contiene un grupo de pares clave-valor.

Asociación del almacén de clave-valor a la función

Ahora ha creado el almacén de clave-valor. Y ha creado o modificado una función que incluye los nombres de las claves del almacén de clave-valor. Ahora puede asociar el almacén de clave-valor y la función. La asociación se crea desde dentro de la función.

Asociación del almacén de clave-valor a la función

1. Seleccione Funciones en el panel de navegación. La pestaña Funciones aparece en la parte superior de forma predeterminada.

2. Elija el nombre de la función y, en la sección KeyValueStore asociado, elija Asociar KeyValueStore existente.
3. Seleccione el almacén de clave-valor y elija Asociar KeyValueStore.

> **Note**
>
> Solo puede asociar un almacén de clave-valor a cada función.

Prueba y publicación del código de la función

Tras asociar el almacén de clave-valor a la función, puede probar y publicar el código de la función. Siempre debe probar el código de la función cada vez que lo modifique, incluso cuando haga lo siguiente:

- Asociar un almacén de clave-valor a la función.
- Modificar la función y su almacén de clave-valor para incluir un nuevo par de clave-valor.
- Cambiar el valor de un par clave-valor.

Prueba y publicación del código de la función

1. Para obtener más información sobre cómo probar una función, consulte the section called "Prueba de funciones". Asegúrese de elegir probar la función en la etapa de `DEVELOPMENT`.
2. Publique la función cuando esté preparado para utilizarla (con los pares clave-valor nuevos o revisados) en un entorno `LIVE`.

   Al publicar, CloudFront copia la versión de la función de la etapa de `DEVELOPMENT` a la etapa de producción en vivo. La función tiene el código nuevo y está asociada al almacén de clave-valor. (No es necesario volver a realizar la asociación en la etapa de producción en vivo).

   Para obtener más información sobre cómo publicar la función, consulte the section called "Publicación de funciones".

Escritura de código de función

Puede utilizar CloudFront Functions para escribir funciones ligeras en JavaScript para personalizaciones de CDN sensibles a la latencia a gran escala. Su código de función puede

manipular las solicitudes y respuestas que atraviesan CloudFront, realizar autenticaciones y autorizaciones básicas, generar respuestas HTTP en el borde y mucho más.

Como ayuda para escribir código de función de CloudFront Functions, consulte los siguientes temas. Para ver ejemplos de código, consulte Ejemplos de CloudFront Functions para CloudFront y el repositorio amazon-cloudfront-functions en GitHub.

Temas

- Determinación del propósito de la función
- Estructura de eventos de CloudFront Functions
- Características del tiempo de ejecución de JavaScript para CloudFront Functions
- Métodos auxiliares para almacenes de clave-valor
- Métodos auxiliares para la modificación del origen
- Métodos auxiliares para las propiedades de CloudFront SaaS Manager
- Utilice async y await
- Compatibilidad con CWT para CloudFront Functions
- Métodos de ayuda generales

Determinación del propósito de la función

Antes de escribir el código de su función, determine su propósito. La mayoría de las funciones de CloudFront Functions cumplen uno de los siguientes propósitos.

Temas

- Modificar la solicitud HTTP en un tipo de evento de solicitud de lector
- Generar una respuesta HTTP en un tipo de evento de solicitud de lector
- Modificar la respuesta HTTP en un tipo de evento de respuesta de lector
- Validación de las conexiones de mTLS en un tipo de evento de solicitud de conexión
- Información relacionada

Independientemente del propósito de la función, el `handler` es el punto de entrada para cualquier función. Toma un solo argumento llamado `event`, que se pasa a la función mediante CloudFront. El `event` es un objeto JSON que contiene una representación de la solicitud HTTP (y la respuesta, si su función modifica la respuesta HTTP).

Modificar la solicitud HTTP en un tipo de evento de solicitud de lector

Su función puede modificar la solicitud HTTP que CloudFront recibe del lector (cliente) y devolver la solicitud modificada a CloudFront para su procesamiento continuo. Por ejemplo, el código de función podría normalizar la clave de caché o modificar los encabezados de solicitud.

Cuando crea y publica una función que modifica la solicitud HTTP, asegúrese de agregar una asociación para el tipo de evento solicitud del lector. Para obtener más información, consulte Creación de la función. Esto hace que la función se ejecute cada vez que CloudFront recibe una solicitud de un lector, antes de comprobar si el objeto solicitado está en la caché de CloudFront.

Example Ejemplo

El siguiente pseudocódigo muestra la estructura de una función que modifica la solicitud HTTP.

```
function handler(event) {
    var request = event.request;

    // Modify the request object here.

    return request;
}
```

La función devuelve el objeto modificado `request` a CloudFront. CloudFront continúa procesando la solicitud devuelta comprobando la caché de CloudFront en busca de un acierto de caché y enviando la solicitud al origen si es necesario.

Generar una respuesta HTTP en un tipo de evento de solicitud de lector

Su función puede generar una respuesta HTTP en el borde y devolverla directamente al lector (cliente) sin buscar una respuesta almacenada en la caché o cualquier otro procesamiento por parte de CloudFront. Por ejemplo, el código de función podría redirigir la solicitud a una nueva URL, o comprobar la autorización y devolver una respuesta `401` o `403` a solicitudes no autorizadas.

Cuando crea una función que genera una respuesta HTTP, asegúrese de elegir el tipo de evento viewer request (solicitud del lector). Esto significa que la función se ejecuta cada vez que CloudFront recibe una solicitud de un lector, antes de que CloudFront siga procesando la solicitud.

Example Ejemplo

El siguiente pseudocódigo muestra la estructura de una función que genera una respuesta HTTP.

```
function handler(event) {
    var request = event.request;

    var response = ...; // Create the response object here,
                        // using the request properties if needed.

    return response;
}
```

La función devuelve un objeto `response` a CloudFront, que CloudFront devuelve inmediatamente al lector sin comprobar la caché de CloudFront ni enviar una solicitud al origen.

Modificar la respuesta HTTP en un tipo de evento de respuesta de lector

Su función puede modificar la respuesta HTTP antes de que CloudFront la envíe al lector (cliente), independientemente de si la respuesta proviene de la caché de CloudFront o del origen. Por ejemplo, es posible que el código de función agregue o modifique encabezados de respuesta, códigos de estado y contenido del cuerpo.

Cuando crea una función que modifica la respuesta HTTP, asegúrese de elegir el tipo de evento viewer response (respuesta al lector). Esto significa que la función se ejecuta antes de que CloudFront devuelva una respuesta al lector, independientemente de si la respuesta proviene de la caché de CloudFront o del origen.

Example Ejemplo

El siguiente pseudocódigo muestra la estructura de una función que modifica la respuesta 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 función devuelve el objeto `response` modificado a CloudFront, que CloudFront devuelve inmediatamente al lector.

Validación de las conexiones de mTLS en un tipo de evento de solicitud de conexión

Las funciones de conexión son un tipo de CloudFront Functions que se ejecutan durante las conexiones TLS para proporcionar una lógica de validación y autenticación personalizada. Las funciones de conexión están disponibles actualmente para las conexiones TLS mutuas (mTLS), con las que puede validar los certificados de los clientes e implementar una lógica de autenticación personalizada más allá de la validación de certificados estándar. Las funciones de conexión se ejecutan durante el proceso de establecimiento de comunicación de TLS y pueden permitir o denegar las conexiones en función de las propiedades de los certificados, las direcciones IP de los clientes u otros criterios.

Cuando crea y publica una función de conexión, asegúrese de agregar una asociación para el tipo de evento solicitud de conexión con una distribución con mTLS. Esto hace que la función se ejecute cada vez que un cliente intenta establecer una conexión de mTLS con CloudFront.

Example

El siguiente pseudocódigo muestra la estructura de una función de conexión:

```
function connectionHandler(connection) {
    // Validate certificate and connection properties here.

    if (/* validation passes */) {
        connection.allow();
    } else {
        connection.deny();
    }
}
```

La función utiliza métodos de ayuda para determinar si se debe permitir o denegar la conexión. A diferencia de las funciones de solicitud y respuesta del espectador, las funciones de conexión no pueden modificar las solicitudes o respuestas HTTP.

Información relacionada

Para obtener más información sobre cómo trabajar con CloudFront Functions, consulte los siguientes:

- Estructura de evento
- Características del tiempo de ejecución de JavaScript

- Ejemplos de CloudFront Functions
- Restricciones en funciones de borde

Estructura de eventos de CloudFront Functions

CloudFront Functions pasa un objeto `event` al código de función como entrada cuando ejecuta la función. Cuando prueba una función, crea el objeto `event` y lo pasa a la función. Al crear un objeto `event` para probar una función, puede omitir los campos `distributionDomainName`,`distributionId` `yrequestId` en el objeto `context`. Asegúrese de que los nombres de encabezados estén en minúsculas, esto siempre sucede en el objeto de `event` que CloudFront Functions pasa a la función en producción.

A continuación, se muestra la información general de la estructura de este objeto de evento.

```
{
    "version": "1.0",
    "context": {
        <context object>
    },
    "viewer": {
        <viewer object>
    },
    "request": {
        <request object>
    },
    "response": {
        <response object>
    }
}
```

Para obtener más información, consulte los temas siguientes:

Temas

- Campo Versión
- Objeto Context (Contexto)
- Estructura de eventos de conexión
- Objeto viewer (lector)
- Objeto Request (solicitud)

- Objeto de respuesta
- Código de estado y cuerpo
- Estructura para una cadena de consulta, encabezado o cookie
- Objeto de respuesta de ejemplo
- Objeto de evento de ejemplo

Campo Versión

El campo `version` contiene una cadena que especifica la versión del objeto de evento de CloudFront Functions. La versión actual es `1.0`.

Objeto Context (Contexto)

El objeto `context` contiene información contextual sobre el evento. Contiene los campos siguientes:

`distributionDomainName`

El nombre de dominio de CloudFront (por ejemplo, d111111abcdef8.cloudfront.net) de la distribución que está asociada al evento.

El campo `distributionDomainName` solo aparece cuando se invoca la función para distribuciones estándar.

`endpoint`

El nombre de dominio de CloudFront (por ejemplo, d111111abcdef8.cloudfront.net) del grupo de conexión asociado al evento.

El campo `endpoint` solo aparece cuando se invoca la función para distribuciones de varios inquilinos.

`distributionId`

El identificador de la distribución (por ejemplo, EDFDVBD6EXAMPLE) que está asociada al evento.

`eventType`

El tipo de evento, `viewer-request` o `viewer-response`.

`requestId`

Cadena que identifica de forma única una solicitud de CloudFront (y su respuesta asociada).

Estructura de eventos de conexión

Las funciones de conexión reciben una estructura de eventos diferente a la de las funciones del espectador. Para obtener información detallada sobre la estructura de eventos de conexión y el formato de respuesta, consulte Asociación de una función de conexión de CloudFront.

Objeto viewer (lector)

El objeto `viewer` contiene un campo `ip` cuyo valor es la dirección IP del lector (cliente) que envió la solicitud. Si el lector utiliza un proxy HTTP o un balanceador de carga para enviar la solicitud, el valor es la dirección IP del proxy o del balanceador de carga.

Objeto Request (solicitud)

El objeto `request` contiene una representación de una solicitud HTTP de lector-a-CloudFront. En el objeto `event` que se pasa a la función, el objeto `request` representa la solicitud real que CloudFront recibió del lector.

Si su código de función devuelve un objeto `request` a CloudFront, debe usar esta misma estructura.

El objeto `request` contiene los siguientes campos:

`method`

El método HTTP de la solicitud. Si su código de función devuelve una `request`, no puede modificar este campo. Este es el único campo de solo lectura en el objeto `request`.

`uri`

La ruta relativa del objeto solicitado.

> **Note**
>
> Si la función modifica el valor `uri`, se aplica lo siguiente:
>
> - El nuevo valor `uri` debe comenzar con una barra diagonal (`/`).
> - Si una función cambia el valor de `uri`, esta cambia el objeto que el lector solicita.
> - Si una función cambia el valor de `uri`, no cambia el comportamiento de la caché de la solicitud ni del origen al que se envía la solicitud.

`querystring`

Objeto que representa la cadena de consulta en la solicitud. Si la solicitud no incluye una cadena de consulta, el objeto `request` del evento incluye un valor `querystring` vacío.

El objeto `querystring` contiene un campo para cada parámetro de cadena de consulta de la solicitud.

`headers`

Objeto que representa el encabezado HTTP en la solicitud. Si la solicitud contiene algún encabezado `Cookie`, esos encabezados no forman parte del objeto `headers`. Las cookies se representan por separado en el objeto `cookies`.

El objeto `headers` contiene un campo para cada encabezado de la solicitud. Los nombres de encabezados se convierten a ASCII minúsculas en el objeto de evento; deben estar en ASCII minúsculas cuando se agregan según el código de función. Cuando CloudFront Functions convierte el objeto de evento de nuevo en una solicitud HTTP, la primera letra de cada palabra en los nombres de encabezados se escribe en mayúsculas, si es una letra ASCII. CloudFront Functions no aplica ningún cambio a los símbolos que no sean ASCII en los nombres de los encabezados. Por ejemplo, `TÈst-header` se convertirá en `tÈst-header` dentro de la función. El símbolo que no es ASCII `È` permanece inalterado.

Las palabras están separadas por un guión (`-`). Por ejemplo, si el código de la función agrega un encabezado llamado `example-header-name`, CloudFront lo convierte en `Example-Header-Name` en la solicitud HTTP.

`cookies`

Objeto que representa las cookies en la solicitud (encabezados `Cookie`).

El objeto `cookies` contiene un campo para cada cookie de la solicitud.

Para obtener más información sobre la estructura de cadenas de consulta, encabezados y cookies, consulte Estructura para una cadena de consulta, encabezado o cookie.

Para obtener un objeto de ejemplo `event`, consulte Objeto de evento de ejemplo.

Objeto de respuesta

El objeto `response` contiene una representación de una respuesta HTTP CloudFront-to-viewer. En el objeto `event` que se pasa a la función, el objeto `response` representa la respuesta real de CloudFront a una solicitud del lector.

Si su código de función devuelve un objeto `response`, debe usar esta misma estructura.

El objeto `response` contiene los siguientes campos:

`statusCode`

Código de estado HTTP de la respuesta. Este valor es un número entero, no una cadena.

La función puede generar o modificar el `statusCode`.

`statusDescription`

La descripción del estado HTTP de la respuesta. Si su código de función genera una respuesta, este campo es opcional.

`headers`

Un objeto que representa los encabezados HTTP en la solicitud. Si la respuesta contiene algún encabezado `Set-Cookie`, esos encabezados no forman parte del objeto `headers`. Las cookies se representan por separado en el objeto `cookies`.

El objeto `headers` contiene un campo para cada encabezado de la respuesta. Los nombres de encabezados se convierten a minúsculas en el objeto de evento; deben estar en minúsculas cuando se agregan con el código de función. Cuando CloudFront Functions convierte el objeto de evento de nuevo en una respuesta HTTP, la primera letra de cada palabra en los nombres de encabezados se escribe en mayúsculas. Las palabras están separadas por un guión (`-`). Por ejemplo, si el código de la función agrega un encabezado llamado `example-header-name`, CloudFront lo convierte en `Example-Header-Name` en la respuesta HTTP.

`cookies`

Objeto que representa las cookies en la respuesta (encabezados `Set-Cookie`).

El objeto `cookies` contiene un campo para cada cookie en la respuesta.

`body`

Agregar el campo `body` es opcional y no estará presente en el objeto de `response` a menos que lo especifique en la función. La función no tiene acceso al cuerpo original devuelto por la caché o

el origen de CloudFront. Si no especifica el campo `body` en la función de respuesta del lector, el cuerpo original devuelto por la memoria caché o el origen de CloudFront se devuelve al lector.

Si desea que CloudFront devuelva un cuerpo personalizado al lector, especifique el contenido del cuerpo en el campo `data` y la codificación del cuerpo en el campo `encoding`. Puede especificar la codificación como texto sin formato (`"encoding": "text"`) o como contenido cifrado en Base64 (`"encoding": "base64"`).

Como método abreviado, también puede especificar el contenido del cuerpo directamente en el campo `body` (`"body": "<specify the body content here>"`). Al hacer esto, omita los campos `data` y `encoding`. CloudFront trata el cuerpo como texto sin formato en este caso.

`encoding`

La codificación del contenido de `body` (campo `data`). Las únicas codificaciones válidas son `text` y `base64`.

Si especifica `encoding` como `base64` pero el cuerpo no tiene una codificación base64 válida, CloudFront devuelve un error.

`data`

El contenido de `body`.

Para obtener más información sobre los códigos de estado y el contenido del cuerpo modificados, consulte Código de estado y cuerpo.

Para obtener más información sobre la estructura de los encabezados y las cookies, consulte Estructura para una cadena de consulta, encabezado o cookie.

Para obtener un objeto de ejemplo `response`, consulte Objeto de respuesta de ejemplo.

Código de estado y cuerpo

Con CloudFront Functions, puede actualizar el código de estado de la respuesta del lector, sustituir todo el cuerpo de la respuesta por uno nuevo o eliminar el cuerpo de la respuesta. Algunos escenarios comunes para actualizar la respuesta del lector después de evaluar aspectos de la respuesta de la caché o el origen de CloudFront son los siguientes:

- Cambiar el estado para establecer un código de estado HTTP 200 y crear un cuerpo con contenido estático para devolverlo al lector.

- Cambiar el estado para establecer un código de estado HTTP 301 o 302 para redirigir al usuario a otro sitio web.
- Decidir si mostrar o dejar el cuerpo de la respuesta del lector.

> **Note**
>
> Si el origen devuelve un error HTTP igual o superior a 400, CloudFront Function no se ejecutará. Para obtener más información consulte () Restricciones en todas las funciones de borde.

Cuando trabaja con la respuesta HTTP, CloudFront Functions no tiene acceso al cuerpo de la respuesta. Puede sustituir el contenido del cuerpo estableciéndolo en el valor deseado o puede eliminar el cuerpo estableciendo un valor vacío. Si no actualiza el campo cuerpo de la función, el cuerpo original devuelto por la caché o el origen de CloudFront se devuelve al lector.

> **Tip**
>
> Cuando utilice CloudFront Functions para sustituir un cuerpo, asegúrese de alinear los encabezados correspondientes, como `content-encoding`, `content-type` o `content-length` con el nuevo contenido del cuerpo.
> Por ejemplo, si el origen o la caché de CloudFront devuelve `content-encoding: gzip` pero la función de respuesta del lector establece un cuerpo que es texto sin formato, la función también debe cambiar los encabezados `content-encoding` y `content-type` en consecuencia.

Si CloudFront Function está configurada para devolver un error HTTP igual o superior a 400, el visor no verá una página de error personalizada que haya especificado para el mismo código de estado.

Estructura para una cadena de consulta, encabezado o cookie

Las cadenas de consulta, los encabezados y las cookies comparten la misma estructura. Las cadenas de consulta pueden aparecer en las solicitudes. Los encabezados aparecen en las solicitudes y las respuestas. Las cookies aparecen en las solicitudes y las respuestas.

Cada cadena de consulta, encabezado o cookie es un campo único dentro del objeto principal `querystring`,`headers` o `cookies`. El nombre del campo es el nombre de la cadena de consulta,

el encabezado o la cookie. Cada campo contiene una propiedad `value` con el valor de la cadena de consulta, el encabezado o la cookie.

Contenido

- Valores de cadenas de consulta u objetos de cadenas de consulta
- Consideraciones especiales sobre el uso de los encabezados
- Cadenas de consulta, encabezados y cookies duplicados (matriz multiValue)
- Atributos de cookie

Valores de cadenas de consulta u objetos de cadenas de consulta

Una función puede devolver un valor de cadena de consulta además de un objeto de cadena de consulta. El valor de la cadena de consulta se puede utilizar para organizar los parámetros de la cadena de consulta en cualquier orden personalizado.

Example Ejemplo

Para modificar una cadena de consulta en el código de función, use código como el siguiente.

```
var request = event.request;
request.querystring =
 'ID=42&Exp=1619740800&TTL=1440&NoValue=&querymv=val1&querymv=val2,val3';
```

Consideraciones especiales sobre el uso de los encabezados

Solo en el caso de encabezados, los nombres de encabezados se convierten a minúsculas en el objeto de evento; deben estar en minúsculas cuando se agregan con el código de función. Cuando CloudFront Functions convierte el objeto de evento de nuevo en una solicitud o respuesta HTTP, la primera letra de cada palabra en los nombres de encabezados se escribe en mayúsculas. Las palabras están separadas por un guión (`-`). Por ejemplo, si el código de la función agrega un encabezado llamado `example-header-name`, CloudFront lo convierte en `Example-Header-Name` en la solicitud o respuesta HTTP.

Example Ejemplo

Considere el siguiente encabezado `Host` en una solicitud HTTP.

```
Host: video.example.com
```

Este encabezado se representa de la siguiente manera en el objeto `request`:

```
"headers": {
    "host": {
        "value": "video.example.com"
    }
}
```

Para acceder al encabezado `Host` en su código de función, use código como el siguiente:

```
var request = event.request;
var host = request.headers.host.value;
```

Para agregar o modificar un encabezado en su código de función, use código como el siguiente (este código agrega un encabezado llamado `X-Custom-Header` con el valor `example value`):

```
var request = event.request;
request.headers['x-custom-header'] = {value: 'example value'};
```

Cadenas de consulta, encabezados y cookies duplicados (matriz **`multiValue`**)

Una solicitud o respuesta HTTP puede contener más de una cadena de consulta, encabezado o cookie con el mismo nombre. En este caso, las cadenas de consulta duplicadas, encabezados o cookies se contraen en un campo del objeto `request` o `response`, pero este campo contiene una propiedad adicional denominada `multiValue`. La propiedad `multiValue` contiene una matriz con los valores de cada una de las cadenas de consulta duplicadas, encabezados o cookies.

Example Ejemplo

Considere una solicitud HTTP con los siguientes encabezados `Accept`.

```
Accept: application/json
Accept: application/xml
Accept: text/html
```

Estos encabezados se representan de la siguiente manera en el objeto `request`.

```
"headers": {
    "accept": {
        "value": "application/json",
        "multiValue": [
```

```
            {
                "value": "application/json"
            },
            {
                "value": "application/xml"
            },
            {
                "value": "text/html"
            }
        ]
    }
}
```

> **Note**
>
> El primer valor de encabezado (en este caso, `application/json`) se repite en las propiedades `value` y `multiValue`. Esto le permite acceder a todos los valores al recorrer la matriz `multiValue`.

Si el código de función modifica una cadena de consulta, encabezado o cookie que tiene una matriz `multiValue`, CloudFront Functions utiliza las siguientes reglas para aplicar los cambios:

1. Si la matriz `multiValue` existe y tiene alguna modificación, entonces esa modificación se aplica. El primer elemento de la propiedad `value` se ignora.
2. De lo contrario, se aplicará cualquier modificación a la propiedad `value` y los valores subsiguientes (si existen) permanecen sin cambios.

La propiedad `multiValue` se utiliza solo cuando la solicitud o respuesta HTTP contiene cadenas de consulta, encabezados o cookies duplicados con el mismo nombre, como se muestra en el ejemplo anterior. Sin embargo, si hay varios valores en una sola cadena de consulta, encabezado o cookie, la propiedad `multiValue` no se utiliza.

Example Ejemplo

Considere una solicitud con un encabezado `Accept` que contenga tres valores.

```
Accept: application/json, application/xml, text/html
```

Este encabezado se representa de la siguiente manera en el objeto `request`.

```
"headers": {
    "accept": {
        "value": "application/json, application/xml, text/html"
    }
}
```

Atributos de cookie

En un encabezado `Set-Cookie` de una respuesta HTTP, el encabezado contiene el par nombre-valor para la cookie y opcionalmente un conjunto de atributos separados por punto y coma.

Example Ejemplo

```
Set-Cookie: cookie1=val1; Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT
```

En el objeto `response`, estos atributos se representan en la propiedad `attributes` del campo cookie. Por ejemplo, el encabezado `Set-Cookie` anterior se representa de la siguiente manera:

```
"cookie1": {
    "value": "val1",
    "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT"
}
```

Objeto de respuesta de ejemplo

En el siguiente ejemplo se muestra un objeto `response` (el resultado de una función de respuesta del lector) en el que el cuerpo se ha sustituido por una función de respuesta del lector.

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

Objeto de evento de ejemplo

En el siguiente ejemplo se muestra un objeto `event` completo. Este es un ejemplo de invocación para una distribución estándar y no para una distribución de varios inquilinos. Para distribuciones de varios inquilinos, se utiliza el campo `endpoint` en lugar de `distributionDomainName`. El valor de `endpoint` es el nombre de dominio de CloudFront (por ejemplo, d111111abcdef8.cloudfront.net) del grupo de conexiones asociado al evento.

> **Note**
>
> El objeto `event` es la entrada a su función. Su función devuelve solo el objeto `request` o `response`, no el objeto `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"
                    }
                ]
            }
        }
    }
}
```

Características del tiempo de ejecución de JavaScript para CloudFront Functions

El entorno de tiempo de ejecución JavaScript de CloudFront Functions es compatible con la versión 5.1 de ECMAScript (ES) y también admite algunas características de las versiones 6 a 12 de ES.

Para obtener las características más actualizadas, le recomendamos que utilice el tiempo de ejecución 2.0 de JavaScript.

Las características del tiempo de ejecución 2.0 de JavaScript presentan los siguientes cambios en comparación con la versión 1.0:

- Están disponibles los métodos del módulo de búfer
- No están disponibles los siguientes métodos de prototipos de cadenas no estándares:
  - `String.prototype.bytesFrom()`
  - `String.prototype.fromBytes()`
  - `String.prototype.fromUTF8()`
  - `String.prototype.toBytes()`
  - `String.prototype.toUTF8()`
- El módulo criptográfico presenta los siguientes cambios:
  - `hash.digest()`: el tipo de retorno se cambia a `Buffer` si no se proporciona ninguna codificación
  - `hmac.digest()`: el tipo de retorno se cambia a `Buffer` si no se proporciona ninguna codificación
- Para obtener más información sobre nuevas características adicionales, consulte Características del tiempo de ejecución 2.0 de JavaScript para CloudFront Functions.

Temas

- Características del tiempo de ejecución 1.0 de JavaScript para CloudFront Functions
- Características del tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

Características del tiempo de ejecución 1.0 de JavaScript para CloudFront Functions

El entorno de tiempo de ejecución JavaScript de CloudFront Functions es compatible con la versión 5.1 de ECMAScript (ES) y también admite algunas características de las versiones 6 a 9 de ES. También proporciona algunos métodos no estándar que no forman parte de las especificaciones de ES.

En los siguientes temas se mencionan todas las características de lenguaje admitidas.

Temas

- Características principales
- Objetos primitivos

- Objetos integrados
- Tipos de error
- Globals
- Módulos integrados
- Características restringidas

Características principales

Se admiten las siguientes características principales de ES.

Types

Se admiten todos los tipos de ES 5.1. Esto incluye valores booleanos, números, cadenas, objetos, matrices, funciones, constructores de funciones y expresiones regulares.

Operadores

Se admiten todos los operadores de ES 5.1.

Se admite el operador de exponenciación ES 7 (`**`).

Instrucciones

> **Note**
>
> No se admiten las instrucciones `const` ni `let`.

Se admiten las siguientes instrucciones de ES 5.1:

- `break`
- `catch`
- `continue`
- `do-while`
- `else`
- `finally`
- `for`
- `for-in`

- `if`
- `return`
- `switch`
- `throw`
- `try`
- `var`
- `while`
- Instrucciones etiquetadas

Literales

Se admiten literales de plantilla de ES 6: cadenas de líneas múltiples, interpolación de expresiones y plantillas de anidamiento.

Funciones

Se admiten todas las características de función de ES 5.1.

Se admiten las funciones flecha de ES 6 así como la sintaxis del parámetro rest de ES 6.

Unicode

El texto de origen y los literales de cadena pueden contener caracteres codificados en Unicode. También se admiten secuencias de escape de punto de código Unicode de seis caracteres (por ejemplo, `\uXXXX`).

Modo estricto

Las funciones operan en modo estricto de forma predeterminada, por lo que no necesita agregar una instrucción `use strict` en su código de función. Esto no se puede cambiar.

Objetos primitivos

Se admiten los siguientes objetos primitivos de ES.

Objeto

Se admiten los siguientes métodos de ES 5.1 en objetos:

- `create` (sin lista de propiedades)
- `defineProperties`

- `defineProperty`
- `freeze`
- `getOwnPropertyDescriptor`
- `getOwnPropertyNames`
- `getPrototypeOf`
- `hasOwnProperty`
- `isExtensible`
- `isFrozen`
- `prototype.isPrototypeOf`
- `isSealed`
- `keys`
- `preventExtensions`
- `prototype.propertyIsEnumerable`
- `seal`
- `prototype.toString`
- `prototype.valueOf`

Se admiten los siguientes métodos de ES 6 en objetos:

- `assign`
- `is`
- `prototype.setPrototypeOf`

Se admiten los siguientes métodos de ES 8 en objetos:

- `entries`
- `values`

Cadena

Se admiten los siguientes métodos de ES 5.1 en cadenas:

- `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`

Se admiten los siguientes métodos de ES 6 en cadenas:

- `fromCodePoint`
- `prototype.codePointAt`
- `prototype.endsWith`
- `prototype.includes`
- `prototype.repeat`
- `prototype.startsWith`

Se admiten los siguientes métodos de ES 8 en cadenas:

- `prototype.padStart`
- `prototype.padEnd`

Se admiten los siguientes métodos de ES 9 en cadenas:

- `prototype.trimStart`
- `prototype.trimEnd`

Se admiten los siguientes métodos no estándar en cadenas:

- `prototype.bytesFrom(`*`array | string, encoding`*`)`

  Crea una cadena de bytes a partir de una matriz de octetos o una cadena codificada. Las opciones de codificación de cadenas son `hex`, `base64` y `base64url`.
- `prototype.fromBytes(`*`start[, end]`*`)`

Crea una cadena Unicode a partir de una cadena de bytes donde cada byte se reemplaza con el punto de código Unicode correspondiente.

- `prototype.fromUTF8(start[, end])`

  Crea una cadena Unicode a partir de una cadena de bytes codificada en UTF-8. Si la codificación es incorrecta, devuelve `null`.

- `prototype.toBytes(start[, end])`

  Crea una cadena de bytes a partir de una cadena Unicode. Todos los caracteres deben estar comprendidos en el rango [0-255]. De lo contrario, devuelve `null`.

- `prototype.toUTF8(start[, end])`

  Crea una cadena de bytes codificada en UTF-8 a partir de una cadena Unicode.

Número

Se admiten todos los métodos de ES 5.1 en números.

Se admiten los siguientes métodos de ES 6 en números:

- `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`

Objetos integrados

Se admiten los siguientes objetos integrados de ES.

Math

Se admiten todos los métodos matemáticos de ES 5.1.

> **Note**
>
> En el entorno de tiempo de ejecución de CloudFront Functions, la implementación de `Math.random()` utiliza `arc4random` de OpenBSD predefinido con la marca de tiempo de cuándo se ejecuta la función.

Se admiten los siguientes métodos matemáticos de 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`

Fecha

Se admiten todas las características `Date` de ES 5.1.

> **Note**
>
> Por razones de seguridad, `Date` siempre devuelve el mismo valor (la hora de inicio de la función) durante la vida útil de la ejecución de una sola función. Para obtener más información, consulte Características restringidas.

Función

Se admiten los métodos `apply`, `call` y `bind`.

Los constructores de funciones no son compatibles.

Expresiones regulares

Se admiten todas las características de expresión regular de ES 5.1. El lenguaje de expresión regular es compatible con Perl. Se admiten grupos de captura con nombre de ES 9.

JSON

Se admiten todas las características JSON de ES 5.1, incluidas `parse` y `stringify`.

Matriz

Se admiten los siguientes métodos de ES 5.1 en matrices:

- `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`

Se admiten los siguientes métodos de ES 6 en matrices:

- `of`
- `prototype.copyWithin`
- `prototype.fill`
- `prototype.find`
- `prototype.findIndex`

Se admiten los siguientes métodos de ES 7 en matrices:

- `prototype.includes`

Matrices con tipo

Se admiten las siguientes matrices con tipo de 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

Se admiten los siguientes métodos en `ArrayBuffer`:

- `prototype.isView`
- `prototype.slice`

Promesa

Se admiten los siguientes métodos en promesas:

- `reject`
- `resolve`
- `prototype.catch`
- `prototype.finally`
- `prototype.then`

Cripto

El módulo criptográfico proporciona ayudantes de código de autenticación de mensajes (HMAC) estándar hashing y basado en hash. Puede cargar el módulo mediante `require('crypto')`.

El módulo expone los siguientes métodos que se comportan exactamente como sus homólogos Node.js:

- `createHash(algorithm)`
- `hash.update(data)`
- `hash.digest([encoding])`
- `createHmac(algorithm, secret key)`
- `hmac.update(data)`
- `hmac.digest([encoding])`

Para obtener más información, consulte Cripto (hash y HMAC) en la sección módulos integrados.

Consola

Este es un objeto ayudante para la depuración. Solo admite el método `log()` para registrar mensajes de registro.

> **Note**
>
> CloudFront Functions no admite la sintaxis con comas, como `console.log('a', 'b')`. En su lugar, utilice el formato `console.log('a' + ' ' + 'b')`.

Tipos de error

Se admiten los siguientes objetos de error:

- `Error`
- `EvalError`
- `InternalError`
- `MemoryError`
- `RangeError`
- `ReferenceError`
- `SyntaxError`
- `TypeError`
- `URIError`

Globals

Se admite el objeto `globalThis`.

Se admiten las siguientes características globales de ES 5.1:

- `decodeURI`
- `decodeURIComponent`
- `encodeURI`
- `encodeURIComponent`
- `isFinite`
- `isNaN`
- `parseFloat`
- `parseInt`

Se admiten las siguientes constantes globales:

- `NaN`
- `Infinity`
- `undefined`

Módulos integrados

Se admiten los siguientes módulos integrados:

Modules

- Cripto (hash y HMAC)
- Cadena de consulta

Cripto (hash y HMAC)

El módulo criptográfico (`crypto`) proporciona ayudantes de código de autenticación de mensajes basado en hash (HMAC) y hashing estándar. Puede cargar el módulo mediante `require('crypto')`. El módulo proporciona los siguientes métodos que se comportan exactamente como sus homólogos Node.js.

Métodos de hashing

`crypto.createHash(algorithm)`

Crea y devuelve un objeto hash que puede utilizar para generar resúmenes hash mediante el algoritmo dado: `md5`, `sha1` o `sha256`.

`hash.update(data)`

Actualiza el contenido hash con los `data` dados.

`hash.digest([encoding])`

Calcula el resumen de todos los datos pasados con `hash.update()`. La codificación puede ser `hex`, `base64` o `base64url`.

Métodos HMAC

`crypto.createHmac(algorithm, secret key)`

Crea y devuelve un objeto HMAC que utiliza el `algorithm` y `secret key` dados. El algoritmo puede ser `md5`, `sha1` o `sha256`.

`hmac.update(data)`

Actualiza el contenido de HMAC con los `data` dados.

`hmac.digest([encoding])`

Calcula el resumen de todos los datos pasados con `hmac.update()`. La codificación puede ser `hex`, `base64` o `base64url`.

Cadena de consulta

> **Note**
>
> El objeto de evento de CloudFront Functions analiza automáticamente las cadenas de consulta de URL. Eso significa que en la mayoría de los casos no necesita usar este módulo.

El módulo de cadena de consulta (`querystring`) proporciona métodos para analizar y dar formato a las cadenas de consulta de URL. Puede cargar el módulo mediante `require('querystring')`. El módulo proporciona los siguientes métodos.

`querystring.escape(string)`

La URL codifica la `string` dada y devuelve una cadena de consulta escapada. El método es utilizado por `querystring.stringify()` y no debe utilizarse directamente.

`querystring.parse(string[, separator[, equal[, options]]])`

Analiza una cadena de consulta (`string`) y devuelve un objeto.

El parámetro `separator` es una subcadena para delimitar pares de claves y valores en la cadena de consulta. De forma predeterminada, es `&`.

El parámetro `equal` es una subcadena para delimitar claves y valores en la cadena de consulta. De forma predeterminada, es `=`.

El parámetro `options` es un objeto con las siguientes claves:

`decodeURIComponent function`

Una función para decodificar caracteres codificados por porcentaje en la cadena de consulta. De forma predeterminada, es `querystring.unescape()`.

`maxKeys number`

El número máximo de claves que se analizan. De forma predeterminada, es `1000`. Utilice un valor de `0` para eliminar las limitaciones del recuento de claves.

De forma predeterminada, se supone que los caracteres codificados con porcentaje dentro de la cadena de consulta utilizan la codificación UTF-8. Las secuencias UTF-8 no válidas se reemplazan por el carácter de reemplazo `U+FFFD`.

Por ejemplo, para la siguiente cadena de consulta:

```
'name=value&abc=xyz&abc=123'
```

El valor de retorno de `querystring.parse()` es:

```
{
name: 'value',
abc: ['xyz', '123']
}
```

`querystring.decode()` es un alias de `querystring.parse()`.

`querystring.stringify(object[, separator[, equal[, options]]])`

Serializa un `object` y devuelve una cadena de consulta.

El parámetro `separator` es una subcadena para delimitar pares de claves y valores en la cadena de consulta. De forma predeterminada, es &.

El parámetro `equal` es una subcadena para delimitar claves y valores en la cadena de consulta. De forma predeterminada, es =.

El parámetro `options` es un objeto con las siguientes claves:

`encodeURIComponent` *`function`*

La función que se va a utilizar para convertir caracteres no seguros de URL a codificación porcentual en la cadena de consulta. De forma predeterminada, es `querystring.escape()`.

De forma predeterminada, los caracteres que requieren codificación porcentual dentro de la cadena de consulta se codifican como UTF-8. Para utilizar una codificación diferente, especifique la opción `encodeURIComponent`.

Por ejemplo, el siguiente código:

```
querystring.stringify({ name: 'value', abc: ['xyz', '123'], anotherName: '' });
```

El valor de retorno es:

```
'name=value&abc=xyz&abc=123&anotherName='
```

`querystring.encode()` es un alias de `querystring.stringify()`.

`querystring.unescape(string)`

Decodifica caracteres codificados con porcentaje de URL en la `string` dada y devuelve una cadena de consulta sin escapar. Este método es utilizado por `querystring.parse()` y no debe utilizarse directamente.

Características restringidas

Las siguientes características de lenguaje JavaScript no se admiten o están restringidas debido a cuestiones de seguridad.

Evaluación dinámica de código

No se admite la evaluación dinámica de código. Si se intenta, los constructores `eval()` y `Function` arrojan un error. Por ejemplo, `const sum = new Function('a', 'b', 'return a + b')` arroja un error.

Temporizadores

No se admiten las funciones `setTimeout()`, `setImmediate()` y `clearTimeout()`. No hay nada para posponer o producir dentro de una ejecución de función. La función debe ejecutarse de manera sincrónica hasta finalizar.

Fecha y marcas temporales

Por razones de seguridad, no hay acceso a temporizadores de alta resolución. Todos los métodos `Date` para consultar la hora actual siempre devuelven el mismo valor durante la vida útil de una sola función ejecutada. La marca temporal devuelta es la hora en que la función comenzó a ejecutarse. Por eso, no puede medir el tiempo transcurrido en la función.

Acceso al sistema de archivos

No hay acceso al sistema de archivos. Por ejemplo, no hay ningún módulo `fs` para el acceso al sistema de archivos como lo hay en Node.js.

Acceso al proceso

No hay acceso al proceso. Por ejemplo, no hay ningún objeto global `process` para procesar el acceso a la información como lo hay en Node.js.

Variables de entorno

No hay acceso a las variables de entorno.

En su lugar, puede utilizar CloudFront KeyValueStore para crear un almacén de datos centralizado de pares clave-valor para las CloudFront Functions. CloudFront KeyValueStore habilita las actualizaciones dinámicas de los datos de configuración sin necesidad de implementar cambios en el código. Debe utilizar el tiempo de ejecución de JavaScript 2.0 para utilizar CloudFront KeyValueStore. Para obtener más información, consulte Amazon CloudFront KeyValueStore.

Acceso a la red

No se admiten las llamadas de red. Por ejemplo, no se admite XHR, HTTP (S) ni socket.

Características del tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

El entorno de tiempo de ejecución JavaScript de CloudFront Functions es compatible con la versión 5.1 de ECMAScript (ES) y también admite algunas características de las versiones 6 a 12 de ES. También proporciona algunos métodos no estándar que no forman parte de las especificaciones de ES. En los siguientes temas se enumeran todas las características admitidas en este tiempo de ejecución.

Temas

- Características principales
- Objetos primitivos
- Objetos integrados
- Tipos de error
- Globals
- Módulos integrados
- Características restringidas

Características principales

Se admiten las siguientes características principales de ES.

Types

Se admiten todos los tipos de ES 5.1. Esto incluye valores booleanos, números, cadenas, objetos, matrices, funciones y expresiones regulares.

Operadores

Se admiten todos los operadores de ES 5.1.

Se admite el operador de exponenciación ES 7 (`**`).

Instrucciones

Se admiten las siguientes instrucciones de ES 5.1:

- `break`
- `catch`
- `continue`

- `do-while`
- `else`
- `finally`
- `for`
- `for-in`
- `if`
- `label`
- `return`
- `switch`
- `throw`
- `try`
- `var`
- `while`

Se admiten las siguientes instrucciones de ES 6:

- `const`
- `let`

Se admiten las siguientes instrucciones de ES 8:

- `async`
- `await`

> **Note**
>
> El tiempo de ejecución 2.0 de JavaScript admite `async`, `await`, `const` y `let`. `await` solo se puede usar dentro de funciones `async`. No se admiten argumentos ni cierres de `async`.

Literales

Se admiten literales de plantilla de ES 6: cadenas de líneas múltiples, interpolación de expresiones y plantillas de anidamiento.

Funciones

Se admiten todas las características de función de ES 5.1.

Se admiten las funciones flecha de ES 6 así como la sintaxis del parámetro rest de ES 6.

Unicode

El texto de origen y los literales de cadena pueden contener caracteres codificados en Unicode. También se admiten secuencias de escape de punto de código Unicode de seis caracteres (por ejemplo, `\uXXXX`).

Modo estricto

Las funciones operan en modo estricto de forma predeterminada, por lo que no necesita agregar una instrucción `use strict` en su código de función. Esto no se puede cambiar.

Objetos primitivos

Se admiten los siguientes objetos primitivos de ES.

Objeto

Se admiten los siguientes métodos de ES 5.1 en objetos:

- `Object.create()` (sin lista de propiedades)
- `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()`

Se admiten los siguientes métodos de ES 6 en objetos:

- `Object.assign()`

Se admiten los siguientes métodos de ES 8 en objetos:

- `Object.entries()`
- `Object.values()`

Se admiten los siguientes métodos prototipo de ES 5.1 en objetos:

- `Object.prototype.hasOwnProperty()`
- `Object.prototype.isPrototypeOf()`
- `Object.prototype.propertyIsEnumerable()`
- `Object.prototype.toString()`
- `Object.prototype.valueOf()`

Se admiten los siguientes métodos prototipo de ES 6 en objetos:

- `Object.prototype.is()`
- `Object.prototype.setPrototypeOf()`

Cadena

Se admiten los siguientes métodos de ES 5.1 en cadenas:

- `String.fromCharCode()`

Se admiten los siguientes métodos de ES 6 en cadenas:

- `String.fromCodePoint()`

Se admiten los siguientes métodos prototipo de ES 5.1 en cadenas:

- `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()`

Se admiten los siguientes métodos prototipo de ES 6 en cadenas:

- `String.prototype.codePointAt()`
- `String.prototype.endsWith()`
- `String.prototype.includes()`
- `String.prototype.repeat()`
- `String.prototype.startsWith()`

Se admiten los siguientes métodos prototipo de ES 8 en cadenas:

- `String.prototype.padStart()`
- `String.prototype.padEnd()`

Se admiten los siguientes métodos prototipo de ES 9 en cadenas:

- `String.prototype.trimStart()`
- `String.prototype.trimEnd()`

Se admiten los siguientes métodos prototipo de ES 12 en cadenas:

- `String.prototype.replaceAll()`

> **Note**
>
> `String.prototype.replaceAll()` es una novedad en el tiempo de ejecución 2.0 de JavaScript.

Número

Se admiten TODOS los números de ES 5.

Se admiten las siguientes propiedades de ES 6 en números:

- `Number.EPSILON`
- `Number.MAX_SAFE_INTEGER`
- `Number.MIN_SAFE_INTEGER`
- `Number.MAX_VALUE`
- `Number.MIN_VALUE`
- `Number.NaN`
- `Number.NEGATIVE_INFINITY`
- `Number.POSITIVE_INFINITY`

Se admiten los siguientes métodos de ES 6 en números:

- `Number.isFinite()`
- `Number.isInteger()`
- `Number.isNaN()`
- `Number.isSafeInteger()`
- `Number.parseInt()`
- `Number.parseFloat()`

Se admiten los siguientes métodos prototipo de ES 5.1 en números:

- `Number.prototype.toExponential()`
- `Number.prototype.toFixed()`
- `Number.prototype.toPrecision()`

Se admiten los separadores numéricos ES 12.

> **Note**
>
> Los separadores numéricos ES 12 son nuevos en el tiempo de ejecución 2.0 de JavaScript.

Objetos integrados

Se admiten los siguientes objetos integrados de ES.

Math

Se admiten todos los métodos matemáticos de ES 5.1.

> **Note**
>
> En el entorno de tiempo de ejecución de CloudFront Functions, la implementación de `Math.random()` utiliza `arc4random` de OpenBSD predefinido con la marca de tiempo de cuándo se ejecuta la función.

Se admiten las siguientes propiedades matemáticas de ES 6:

- `Math.E`
- `Math.LN10`
- `Math.LN2`
- `Math.LOG10E`
- `Math.LOG2E`
- `Math.PI`
- `Math.SQRT1_2`
- `Math.SQRT2`

Se admiten los siguientes métodos matemáticos de 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()`

Fecha

Se admiten todas las características `Date` de ES 5.1.

> **Note**
>
> Por razones de seguridad, `Date` siempre devuelve el mismo valor (la hora de inicio de la función) durante la vida útil de la ejecución de una sola función. Para obtener más información, consulte Características restringidas.

Función

Se admiten los siguientes métodos prototipo de ES 5.1:

- `Function.prototype.apply()`
- `Function.prototype.bind()`
- `Function.prototype.call()`

Los constructores de funciones no son compatibles.

Expresiones regulares

Se admiten todas las características de expresión regular de ES 5.1. El lenguaje de expresión regular es compatible con Perl.

Se admiten las siguientes características de acceso prototipo de ES 5.1:

- `RegExp.prototype.global`
- `RegExp.prototype.ignoreCase`
- `RegExp.protoype.multiline`
- `RegExp.protoype.source`
- `RegExp.prototype.sticky`
- `RegExp.prototype.flags`

> **Note**
>
> `RegExp.prototype.sticky` y `RegExp.prototype.flags` son novedades en el tiempo de ejecución 2.0 de JavaScript.

Se admiten los siguientes métodos prototipo de ES 5.1:

- `RegExp.prototype.exec()`
- `RegExp.prototype.test()`
- `RegExp.prototype.toString()`
- `RegExp.prototype[@@replace]()`
- `RegExp.prototype[@@split]()`

> **Note**
>
> `RegExp.prototype[@@split]()` es una novedad en el tiempo de ejecución 2.0 de JavaScript.

Se admiten las siguientes propiedades de instancia de ES 5.1:

- `lastIndex`

Se admiten grupos de captura con nombre de ES 9.

JSON

Se admiten los siguientes métodos matemáticos de ES 5.1:

- `JSON.parse()`
- `JSON.stringify()`

Matriz

Se admiten los siguientes métodos de ES 5.1 en matrices:

- `Array.isArray()`

Se admiten los siguientes métodos de ES 6 en matrices:

- `Array.of()`

Se admiten los siguientes métodos prototipo de 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()`

Se admiten los siguientes métodos prototipo de ES 6

- `Array.prototype.copyWithin()`
- `Array.prototype.fill()`
- `Array.prototype.find()`
- `Array.prototype.findIndex()`

Se admiten los siguientes métodos prototipo de ES 7:

- `Array.prototype.includes()`

Matrices con tipo

Se admiten los siguientes constructores de matrices con tipo de ES 6:

- `Float32Array`
- `Float64Array`

- `Int8Array`
- `Int16Array`
- `Int32Array`
- `Uint8Array`
- `Uint8ClampedArray`
- `Uint16Array`
- `Uint32Array`

Se admiten los siguientes métodos matemáticos de ES 6:

- `TypedArray.from()`
- `TypedArray.of()`

> **Note**
>
> `TypedArray.from()` y `TypedArray.of()` son novedades en el tiempo de ejecución 2.0 de JavaScript.

Se admiten los siguientes métodos prototipo de ES 6:

- `TypedArray.prototype.copyWithin()`
- `TypedArray.prototype.every()`
- `TypedArray.prototype.fill()`
- `TypedArray.prototype.filter()`
- `TypedArray.prototype.find()`
- `TypedArray.prototype.findIndex()`
- `TypedArray.prototype.forEach()`
- `TypedArray.prototype.includes()`
- `TypedArray.prototype.indexOf()`
- `TypedArray.prototype.join()`
- `TypedArray.prototype.lastIndexOf()`
- `TypedArray.prototype.map()`
- `TypedArray.prototype.reduce()`

- `TypedArray.prototype.reduceRight()`
- `TypedArray.prototype.reverse()`
- `TypedArray.prototype.some()`
- `TypedArray.prototype.set()`
- `TypedArray.prototype.slice()`
- `TypedArray.prototype.sort()`
- `TypedArray.prototype.subarray()`
- `TypedArray.prototype.toString()`

> **Note**
>
> `TypedArray.prototype.every()`, `TypedArray.prototype.fill()`, `TypedArray.prototype.filter()`, `TypedArray.prototype.find()`, `TypedArray.prototype.findIndex()`, `TypedArray.prototype.forEach()`, `TypedArray.prototype.includes()`, `TypedArray.prototype.indexOf()`, `TypedArray.prototype.join()`, `TypedArray.prototype.lastIndexOf()`,`TypedArray.prototype.map()`, `TypedArray.prototype.reduce()`, `TypedArray.prototype.reduceRight()`, `TypedArray.prototype.reverse()` y `TypedArray.prototype.some()` son novedades en el tiempo de ejecución 2.0 de JavaScript.

ArrayBuffer

Se admiten los siguientes métodos de ES 6 en ArrayBuffer:

- `isView()`

Se admiten los siguientes métodos prototipo de ES 6 en ArrayBuffer:

- `ArrayBuffer.prototype.slice()`

Promesa

Se admiten los siguientes métodos de ES 6 en promesas:

- `Promise.all()`
- `Promise.allSettled()`
- `Promise.any()`

- `Promise.reject()`
- `Promise.resolve()`
- `Promise.race()`

> **Note**
>
> `Promise.all()`, `Promise.allSettled()`, `Promise.any()` y `Promise.race()` son novedades en el tiempo de ejecución 2.0 de JavaScript.

Se admiten los siguientes métodos prototipos de ES 6 en promesas:

- `Promise.prototype.catch()`
- `Promise.prototype.finally()`
- `Promise.prototype.then()`

DataView

Se admiten los siguientes métodos prototipo de 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**
>
> Todos los métodos prototipo de DataView ES 6 son nuevos en el tiempo de ejecución 2.0 de JavaScript.

Símbolo

Se admiten los siguientes métodos matemáticos de ES 6:

- `Symbol.for()`
- `Symbol.keyfor()`

> **Note**
>
> Todos los métodos de ES 6 de símbolos son nuevos en el tiempo de ejecución 2.0 de JavaScript.

Descodificador de texto

Se admiten los siguientes métodos prototipo:

- `TextDecoder.prototype.decode()`

Se admiten las siguientes propiedades de acceso prototipo:

- `TextDecoder.prototype.encoding`
- `TextDecoder.prototype.fatal`
- `TextDecoder.prototype.ignoreBOM`

Codificador de texto

Se admiten los siguientes métodos prototipo:

- `TextEncoder.prototype.encode()`
- `TextEncoder.prototype.encodeInto()`

Tipos de error

Se admiten los siguientes objetos de error:

- `Error`
- `EvalError`
- `InternalError`
- `RangeError`
- `ReferenceError`
- `SyntaxError`
- `TypeError`
- `URIError`

Globals

Se admite el objeto `globalThis`.

Se admiten las siguientes características globales de ES 5.1:

- `decodeURI()`
- `decodeURIComponent()`
- `encodeURI()`
- `encodeURIComponent()`
- `isFinite()`
- `isNaN()`
- `parseFloat()`
- `parseInt()`

Se admiten las siguientes características globales de ES 6:

- `atob()`
- `btoa()`

> **Note**
>
> `atob()` y `btoa()` son novedades en el tiempo de ejecución 2.0 de JavaScript.

Se admiten las siguientes constantes globales:

- `NaN`
- `Infinity`
- `undefined`
- `arguments`

Módulos integrados

Se admiten los siguientes módulos integrados:

Modules

- Búfer
- Cadena de consulta
- Cripto

Búfer

El módulo proporciona los siguientes métodos:

- `Buffer.alloc(size[, fill[, encoding]])`

  Asignación de un `Buffer`.

  - `size`: tamaño del búfer. Introduzca un número entero.
  - `fill`: opcional. Introduzca una cadena, `Buffer`, Uint8Array o entero. El valor predeterminado es `0`.
  - `encoding`: opcional. Si `fill` es una cadena, introduzca una de las siguientes opciones: `utf8`, `hex`, `base64` o `base64url`. El valor predeterminado es `utf8`.
- `Buffer.allocUnsafe(size)`

  Asigne un valor no inicializado `Buffer`.

  - `size`: introduzca un número entero.
- `Buffer.byteLength(value[, encoding])`

  Devuelve la longitud de un valor, en bytes.

  - `value`: una cadena, `Buffer`, TypedArray, Dataview o Arraybuffer.

  - `encoding`: opcional. Si `value` es una cadena, introduzca una de las siguientes opciones: `utf8`, `hex`, `base64` o `base64url`. El valor predeterminado es `utf8`.
- `Buffer.compare(buffer1, buffer2)`

  Compare dos `Buffer` para ayudar a ordenar las matrices. Devuelve `0` si son iguales, `-1` si `buffer1` aparece primero o `1` si `buffer2` aparece primero.
  - `buffer1`: introduzca un `Buffer`.
  - `buffer2`: introduzca un `Buffer` diferente.
- `Buffer.concat(list[, totalLength])`

  Concatenar varios `Buffer`. Devuelve `0` si no hay ninguno. Devuelve hasta `totalLength`.
  - `list`: introduzca una lista de `Buffer`. Tenga en cuenta que esto se truncará a `totalLength`.
  - `totalLength`: opcional. Introduzca un número entero sin signo. Utilice la suma de las instancias de `Buffer` de la lista si está en blanco.
- `Buffer.from(array)`

  Cree un `Buffer` a partir de una matriz.
  - `array`: introduzca una matriz de bytes de `0` a `255`.
- `Buffer.from(arrayBuffer, byteOffset[, length]))`

  Cree una vista desde `arrayBuffer`, empezando por el desfase `byteOffset` con la longitud `length`.
  - `arrayBuffer`: introduzca una matriz de `Buffer`.
  - `byteOffset`: introduzca un número entero.
  - `length`: opcional. Introduzca un número entero.
- `Buffer.from(buffer)`

  Cree una copia del `Buffer`.
  - `buffer`: introduzca un `Buffer`.
- `Buffer.from(object[, offsetOrEncoding[, length]])`

  Cree un `Buffer` a partir de un objeto. Devuelve `Buffer.from(object.valueOf(), offsetOrEncoding, length)` si `valueOf()` no es igual al objeto.
  - `object`: introduzca un objeto.
  - `offsetOrEncoding`: opcional. Introduzca un número entero o una cadena de codificación.

  - `length`: opcional. Introduzca un número entero.
- `Buffer.from(string[, encoding])`

  Cree un `Buffer` a partir de una cadena.

  - `string`: introduzca una cadena.
  - `encoding`: opcional. Introduzca una de las siguientes opciones: `utf8`, `hex`, `base64` o `base64url`. El valor predeterminado es `utf8`.
- `Buffer.isBuffer(object)`

  Compruebe si `object` es un búfer. Devuelve `true` o `false`.

  - `object`: introduzca un objeto.
- `Buffer.isEncoding(encoding)`

  Compruebe si `encoding` es compatible. Devuelve `true` o `false`.

  - `encoding`: opcional. Introduzca una de las siguientes opciones: `utf8`, `hex`, `base64` o `base64url`. El valor predeterminado es `utf8`.

El módulo proporciona los siguientes métodos de prototipo de búfer.

- `Buffer.prototype.compare(target[, targetStart[, targetEnd[, sourceStart[, sourceEnd]]]])`

  Compare `Buffer` con el objetivo. Devuelve `0` si son iguales, `1` si `buffer` aparece primero o `-1` si `target` aparece primero.

  - `target`: introduzca un `Buffer`.
  - `targetStart`: opcional. Introduzca un número entero. El valor predeterminado es 0.
  - `targetEnd`: opcional. Introduzca un número entero. El valor predeterminado es la longitud del `target`.
  - `sourceStart`: opcional. Introduzca un número entero. El valor predeterminado es 0.
  - `sourceEnd`: opcional. Introduzca un número entero. El valor predeterminado es la longitud del `Buffer`.
- `Buffer.prototype.copy(target[, targetStart[, sourceStart[, sourceEnd]]])`

  Copie el búfer a `target`.

  - `target`: introduzca un `Buffer` o una `Uint8Array`.

  - `targetStart`: opcional. Introduzca un número entero. El valor predeterminado es 0.
  - `sourceStart`: opcional. Introduzca un número entero. El valor predeterminado es 0.
  - `sourceEnd`: opcional. Introduzca un número entero. El valor predeterminado es la longitud del `Buffer`.
- `Buffer.prototype.equals(otherBuffer)`

  Compare `Buffer` con `otherBuffer`. Devuelve `true` o `false`.

  - `otherBuffer`: introduzca una cadena.
- `Buffer.prototype.fill(value[, offset[, end][, encoding])`

  Rellene `Buffer` con `value`.

  - `value`: introduzca una cadena, un `Buffer` o un número entero.
  - `offset`: opcional. Introduzca un número entero.
  - `end`: opcional. Introduzca un número entero.
  - `encoding`: opcional. Introduzca una de las siguientes opciones: `utf8`, `hex`, `base64` o `base64url`. El valor predeterminado es `utf8`.
- `Buffer.prototype.includes(value[, byteOffset][, encoding])`

  Busque `value` en `Buffer`. Devuelve `true` o `false`.

  - `value`: introduzca una cadena, `Buffer`, `Uint8Array` o un número entero.
  - `byteOffset`: opcional. Introduzca un número entero.
  - `encoding`: opcional. Introduzca una de las siguientes opciones: `utf8`, `hex`, `base64` o `base64url`. El valor predeterminado es `utf8`.
- `Buffer.prototype.indexOf(value[, byteOffset][, encoding])`

  Busque el primer `value` en el `Buffer`. Devuelve `index` si se encuentra; devuelve `-1` si no se encuentra.

  - `value`: introduzca una cadena, `Buffer`, Unit8Array o un número entero comprendido entre 0 y 255.
  - `byteOffset`: opcional. Introduzca un número entero.
  - `encoding`: opcional. Introduzca una de las siguientes opciones si `value` es una cadena: `utf8`, `hex`, `base64`, `base64url`. El valor predeterminado es `utf8`.
- `Buffer.prototype.lastIndexOf(value[, byteOffset][, encoding])`

Busque el último `value` en el `Buffer`. Devuelve `index` si se encuentra; devuelve `-1` si no se encuentra.

- `value`: introduzca una cadena, `Buffer`, Unit8Array o un número entero comprendido entre 0 y 255.
- `byteOffset`: opcional. Introduzca un número entero.
- `encoding`: opcional. Introduzca una de las siguientes opciones si `value` es una cadena: `utf8`, `hex`, `base64`, `base64url`. El valor predeterminado es `utf8`.

- `Buffer.prototype.readInt8(offset)`

  Lea `Int8` en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.

- `Buffer.prototype.readIntBE(offset, byteLength)`

  Lea el `Int` como big-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.
  - `byteLength`: opcional. Introduzca un número entero comprendido entre 1 y 6.

- `Buffer.prototype.readInt16BE(offset)`

  Lea el `Int16` como big-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.

- `Buffer.prototype.readInt32BE(offset)`

  Lea el `Int32` como big-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.

- `Buffer.prototype.readIntLE(offset, byteLength)`

  Lea el `Int` como little-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.readInt16LE(offset)`

  Lea el `Int16` como little-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.

- `Buffer.prototype.readInt32LE(offset)`

Lea el `Int32` como little-endian en `offset` desde `Buffer`.

- `offset`: introduzca un número entero.

- `Buffer.prototype.readUInt8(offset)`

  Lea `UInt8` en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.

- `Buffer.prototype.readUIntBE(offset, byteLength)`

  Lea el `UInt` como big-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.readUInt16BE(offset)`

  Lea el `UInt16` como big-endian en `offset` desde `Buffer`.

- • `offset`: introduzca un número entero.

- `Buffer.prototype.readUInt32BE(offset)`

  Lea el `UInt32` como big-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.

- `Buffer.prototype.readUIntLE(offset, byteLength)`

  Lea el `UInt` como little-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.readUInt16LE(offset)`

  Lea el `UInt16` como little-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.

- `Buffer.prototype.readUInt32LE(offset)`

  Lea el `UInt32` como little-endian en `offset` desde `Buffer`.

  - `offset`: introduzca un número entero.

- `Buffer.prototype.readDoubleBE([offset])`

  Lea un doble de 64 bits como big-endian en `offset` desde `Buffer`.

  - `offset`: opcional. Introduzca un número entero.
- `Buffer.prototype.readDoubleLE([offset])`

  Lea un doble de 64 bits como little-endian en `offset` desde `Buffer`.

  - `offset`: opcional. Introduzca un número entero.
- `Buffer.prototype.readFloatBE([offset])`

  Lea un flotante de 32 bits como big-endian en `offset` desde `Buffer`.

  - `offset`: opcional. Introduzca un número entero.
- `Buffer.prototype.readFloatLE([offset])`

  Lea un flotante de 32 bits como little-endian en `offset` desde `Buffer`.

  - `offset`: opcional. Introduzca un número entero.
- `Buffer.prototype.subarray([start[, end]])`

  Devuelve una copia de `Buffer` desplazada y recortada con un nuevo `start` y `end`.

  - `start`: opcional. Introduzca un número entero. El valor predeterminado es 0.
  - `end`: opcional. Introduzca un número entero. El valor predeterminado es la longitud del búfer.
- `Buffer.prototype.swap16()`

  Cambie el orden de los bytes de la matriz del `Buffer`, tratándolo como una matriz de números de 16 bits. La longitud de `Buffer` debe ser divisible entre 2 o recibirá un error.
- `Buffer.prototype.swap32()`

  Cambie el orden de los bytes de la matriz del `Buffer`, tratándolo como una matriz de números de 32 bits. La longitud de `Buffer` debe ser divisible entre 4 o recibirá un error.
- `Buffer.prototype.swap64()`

  Cambie el orden de los bytes de la matriz del `Buffer`, tratándolo como una matriz de números de 64 bits. La longitud de `Buffer` debe ser divisible entre 8 o recibirá un error.
- `Buffer.prototype.toJSON()`

  Devuelve `Buffer` como JSON.
- `Buffer.prototype.toString([encoding[, start[, end]]])`

  Convierte `Buffer`, de `start` a `end`, en una cadena codificada.

  - `encoding`: opcional. Introduzca una de las siguientes opciones: `utf8`, `hex`, `base64` o `base64url`. El valor predeterminado es `utf8`.
  - `start`: opcional. Introduzca un número entero. El valor predeterminado es 0.
  - `end`: opcional. Introduzca un número entero. El valor predeterminado es la longitud del búfer.
- `Buffer.prototype.write(string[, offset[, length]][, encoding])`

  Escribe codificada la `string` en el `Buffer` si hay espacio, o una `string` truncada si no hay suficiente espacio.

  - `string`: introduzca una cadena.
  - `offset`: opcional. Introduzca un número entero. El valor predeterminado es 0.
  - `length`: opcional. Introduzca un número entero. El valor predeterminado es la longitud de la cadena.
  - `encoding`: opcional. Si lo desea, introduzca una de las siguientes opciones: `utf8`, `hex`, `base64` o `base64url`. El valor predeterminado es `utf8`.
- `Buffer.prototype.writeInt8(value, offset, byteLength)`

  Escriba el `Int8` `value` de la `byteLength` en `offset` en `Buffer`.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.
- `Buffer.prototype.writeIntBE(value, offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando big-endian.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.
- `Buffer.prototype.writeInt16BE(value, offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando big-endian.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.
- `Buffer.prototype.writeInt32BE(value, offset, byteLength)`

Escriba un `value` en `offset` para el `Buffer`, usando big-endian.

- `value`: introduzca un número entero.
- `offset`: introduzca un número entero
- `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeIntLE(offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando little-endian.

  - `offset`: introduzca un número entero.
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeInt16LE(offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando little-endian.

  - `offset`: introduzca un número entero.
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeInt32LE(offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando little-endian.

  - `offset`: introduzca un número entero.
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeUInt8(value, offset, byteLength)`

  Escriba el `UInt8` `value` de la `byteLength` en `offset` en `Buffer`.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeUIntBE(value, offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando big-endian.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeUInt16BE(value, offset, byteLength)`

Escriba un `value` en `offset` para el `Buffer`, usando big-endian.

- `value`: introduzca un número entero.
- `offset`: introduzca un número entero
- `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeUInt32BE(value, offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando big-endian.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeUIntLE(value, offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando little-endian.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeUInt16LE(value, offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando little-endian.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeUInt32LE(value, offset, byteLength)`

  Escriba un `value` en `offset` para el `Buffer`, usando little-endian.

  - `value`: introduzca un número entero.
  - `offset`: introduzca un número entero
  - `byteLength`: introduzca un número entero entre 1 y 6.

- `Buffer.prototype.writeDoubleBE(value, [offset])`

  Escriba un `value` en `offset` para el `Buffer`, usando big-endian.

  - `value`: introduzca un número entero.
  - `offset`: opcional. Introduzca un número entero. El valor predeterminado es 0.

- `Buffer.prototype.writeDoubleLE(value, [offset])`

  Escriba un `value` en `offset` para el `Buffer`, usando little-endian.

  - `value`: introduzca un número entero.
  - `offset`: opcional. Introduzca un número entero. El valor predeterminado es 0.
- `Buffer.prototype.writeFloatBE(value, [offset])`

  Escriba un `value` en `offset` para el `Buffer`, usando big-endian.

  - `value`: introduzca un número entero.
  - `offset`: opcional. Introduzca un número entero. El valor predeterminado es 0.
- `Buffer.prototype.writeFloatLE(value, [offset])`

  Escriba un `value` en `offset` para el `Buffer`, usando little-endian.

  - `value`: introduzca un número entero.
  - `offset`: opcional. Introduzca un número entero. El valor predeterminado es 0.

Se admiten los siguientes métodos de instancia:

- `buffer[index]`

  Obtenga y establezca el octeto (byte) en `index` en `Buffer`.

  - Obtenga un número de `0` a `255`. O establezca un número de `0` a `255`.

Se admiten las siguientes propiedades de instancia:

- `buffer`

  Obtenga el objeto `ArrayBuffer` para el búfer.
- `byteOffset`

  Obtenga el `byteOffset` del objeto `Arraybuffer` del búfer.
- `length`

  Obtenga el recuento de bytes del búfer.

> **Note**
>
> Todos los métodos del módulo del búfer son nuevos en el tiempo de ejecución 2.0 de JavaScript.

Cadena de consulta

> **Note**
>
> El objeto de evento de CloudFront Functions analiza automáticamente las cadenas de consulta de URL. Eso significa que en la mayoría de los casos no necesita usar este módulo.

El módulo de cadena de consulta (`querystring`) proporciona métodos para analizar y dar formato a las cadenas de consulta de URL. Puede cargar el módulo mediante `require('querystring')`. El módulo proporciona los siguientes métodos.

`querystring.escape(`*`string`*`)`

La URL codifica la `string` dada y devuelve una cadena de consulta escapada. El método es utilizado por `querystring.stringify()` y no debe utilizarse directamente.

`querystring.parse(`*`string`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Analiza una cadena de consulta (`string`) y devuelve un objeto.

El parámetro `separator` es una subcadena para delimitar pares de claves y valores en la cadena de consulta. De forma predeterminada, es &.

El parámetro `equal` es una subcadena para delimitar claves y valores en la cadena de consulta. De forma predeterminada, es =.

El parámetro `options` es un objeto con las siguientes claves:

`decodeURIComponent` *`function`*

Una función para decodificar caracteres codificados por porcentaje en la cadena de consulta. De forma predeterminada, es `querystring.unescape()`.

`maxKeys` *`number`*

El número máximo de claves que se analizan. De forma predeterminada, es `1000`. Utilice un valor de `0` para eliminar las limitaciones del recuento de claves.

De forma predeterminada, se supone que los caracteres codificados con porcentaje dentro de la cadena de consulta utilizan la codificación UTF-8. Las secuencias UTF-8 no válidas se reemplazan por el carácter de reemplazo `U+FFFD`.

Por ejemplo, para la siguiente cadena de consulta:

```
'name=value&abc=xyz&abc=123'
```

El valor de retorno de `querystring.parse()` es:

```
{
name: 'value',
abc: ['xyz', '123']
}
```

`querystring.decode()` es un alias de `querystring.parse()`.

`querystring.stringify(`*`object`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Serializa un `object` y devuelve una cadena de consulta.

El parámetro `separator` es una subcadena para delimitar pares de claves y valores en la cadena de consulta. De forma predeterminada, es `&`.

El parámetro `equal` es una subcadena para delimitar claves y valores en la cadena de consulta. De forma predeterminada, es `=`.

El parámetro `options` es un objeto con las siguientes claves:

`encodeURIComponent` *`function`*

La función que se va a utilizar para convertir caracteres no seguros de URL a codificación porcentual en la cadena de consulta. De forma predeterminada, es `querystring.escape()`.

De forma predeterminada, los caracteres que requieren codificación porcentual dentro de la cadena de consulta se codifican como UTF-8. Para utilizar una codificación diferente, especifique la opción `encodeURIComponent`.

Por ejemplo, el siguiente código:

```
querystring.stringify({ name: 'value', abc: ['xyz', '123'], anotherName: '' });
```

El valor de retorno es:

```
'name=value&abc=xyz&abc=123&anotherName='
```

`querystring.encode()` es un alias de `querystring.stringify()`.

`querystring.unescape(`*`string`*`)`

Decodifica caracteres codificados con porcentaje de URL en la `string` dada y devuelve una cadena de consulta sin escapar. Este método es utilizado por `querystring.parse()` y no debe utilizarse directamente.

Cripto

El módulo criptográfico (`crypto`) proporciona ayudantes de código de autenticación de mensajes basado en hash (HMAC) y hashing estándar. Puede cargar el módulo mediante `require('crypto')`.

Métodos de hashing

`crypto.createHash(`*`algorithm`*`)`

Crea y devuelve un objeto hash que puede utilizar para generar resúmenes hash mediante el algoritmo dado: `md5`, `sha1` o `sha256`.

`hash.update(`*`data`*`)`

Actualiza el contenido hash con los `data` dados.

`hash.digest([`*`encoding`*`])`

Calcula el resumen de todos los datos pasados con `hash.update()`. La codificación puede ser `hex`, `base64` o `base64url`.

Métodos HMAC

`crypto.createHmac(algorithm, secret key)`

Crea y devuelve un objeto HMAC que utiliza el `algorithm` y `secret key` dados. El algoritmo puede ser `md5`, `sha1` o `sha256`.

`hmac.update(data)`

Actualiza el contenido de HMAC con los `data` dados.

`hmac.digest([encoding])`

Calcula el resumen de todos los datos pasados con `hmac.update()`. La codificación puede ser `hex`, `base64` o `base64url`.

Características restringidas

Las siguientes características de lenguaje JavaScript no se admiten o están restringidas debido a cuestiones de seguridad.

Evaluación dinámica de código

No se admite la evaluación dinámica de código. Si se intenta, los constructores `eval()` y `Function` arrojan un error. Por ejemplo, `const sum = new Function('a', 'b', 'return a + b')` arroja un error.

Temporizadores

No se admiten las funciones `setTimeout()`, `setImmediate()` y `clearTimeout()`. No hay nada para posponer o producir dentro de una ejecución de función. La función debe ejecutarse de manera sincrónica hasta finalizar.

Fecha y marcas temporales

Por razones de seguridad, no hay acceso a temporizadores de alta resolución. Todos los métodos `Date` para consultar la hora actual siempre devuelven el mismo valor durante la vida útil de una sola función ejecutada. La marca temporal devuelta es la hora en que la función comenzó a ejecutarse. Por eso, no puede medir el tiempo transcurrido en la función.

Acceso al sistema de archivos

No hay acceso al sistema de archivos. Por ejemplo, no hay ningún módulo `fs` para el acceso al sistema de archivos como lo hay en Node.js.

Acceso al proceso

No hay acceso al proceso. Por ejemplo, no hay ningún objeto global `process` para procesar el acceso a la información como lo hay en Node.js.

Variables de entorno

No hay acceso a las variables de entorno. En su lugar, puede utilizar CloudFront KeyValueStore para crear un almacén de datos centralizado de pares clave-valor para las CloudFront Functions. CloudFront KeyValueStore habilita las actualizaciones dinámicas de los datos de configuración sin necesidad de implementar cambios en el código. Para obtener más información, consulte Amazon CloudFront KeyValueStore.

Acceso a la red

No se admiten las llamadas de red. Por ejemplo, no se admite XHR, HTTP (S) ni socket.

Métodos auxiliares para almacenes de clave-valor

> **Note**
>
> Las llamadas de métodos auxiliares del almacén de valores de claves desde CloudFront Functions no desencadenan un evento de datos de AWS CloudTrail. Estos eventos no se registran en el historial de eventos de CloudTrail. Para obtener más información, consulte Registro de llamadas a la API de Amazon CloudFront con AWS CloudTrail.

Esta sección se aplica si utiliza el Almacén de clave-valor de CloudFront para incluir claves-valores en la función que cree. CloudFront Functions tiene un módulo que proporciona tres métodos auxiliares para leer valores del almacén de clave-valor.

Para utilizar este módulo en el código de la función, asegúrese de haber asociado un almacén de clave-valor a la función.

A continuación, incluya las siguientes instrucciones en las primeras líneas del código de la función:

```
import cf from 'cloudfront';
const kvsHandle = cf.kvs();
```

`get()`Método de

Utilice este método para devolver el valor de clave del nombre de clave que especifique.

Solicitud

```
get("key", options);
```

- `key`: el nombre de la clave cuyo valor desea recuperar
- `options`: hay una opción, `format`. Garantiza que la función analice correctamente los datos. Valores posibles:
  - `string`: (predeterminado) codificado en UTF8
  - `json`
  - `bytes`: búfer de datos binarios sin procesar

Ejemplo de solicitud

```
const value = await kvsHandle.get("myFunctionKey", { format: "string"});
```

Respuesta

La respuesta es una `promise` que se resuelve en un valor en el formato solicitado mediante el uso de `options`. De forma predeterminada, el valor se devuelve como una cadena.

Gestión de errores

El método `get()` devolverá un error cuando la clave que ha solicitado no exista en el almacén de clave-valor asociado. Para administrar este caso de uso, puede agregar un bloque `try` y `catch` al código.

> **Warning**
>
> El uso de combinadores de promesas (por ejemplo, `Promise.all`, `Promise.any`) y métodos de cadena de promesas (por ejemplo, `then` y `catch`) puede requerir un uso elevado de la memoria de la función. Si la función supera la cuota de memoria máxima de la función, no se ejecutará. Para evitar este error, le recomendamos que utilice la sintaxis `await` de forma secuencial o en bucles para solicitar varios valores.
> Ejemplo

```
var value1 = await kvs.get('key1');
var value2 = await kvs.get('key2');
```

Actualmente, el uso de combinadores de promesas para obtener varios valores no mejorará el rendimiento, como en el siguiente ejemplo.

```
var values = await Promise.all([kvs.get('key1'), kvs.get('key2'),]);
```

`exists()` Método de

Utilice este método para identificar si la clave existe o no en el almacén de clave-valor.

Solicitud

```
exists("key");
```

Ejemplo de solicitud

```
const exist = await kvsHandle.exists("myFunctionkey");
```

Respuesta

La respuesta es una `promise` que devuelve un valor booleano (`true` o `false`). Este valor especifica si la clave existe o no en el almacén de clave-valor.

`meta()` Método de

Utilice este método para devolver metadatos sobre el almacén de clave-valor.

Solicitud

```
meta();
```

Ejemplo de solicitud

```
const meta = await kvsHandle.meta();
```

Respuesta

La respuesta es una `promise` que se resuelve en un objeto con las siguientes propiedades:

- `creationDateTime`: la fecha y hora en formato ISO 8601 de creación del almacén de clave-valor.
- `lastUpdatedDateTime`: la fecha y hora en formato ISO 8601 de última sincronización del almacén de clave-valor desde el origen. El valor no incluye el tiempo de propagación hasta la periferia.
- `keyCount`: el número total de claves del KVS tras la última sincronización desde el origen.

Ejemplo de respuesta

```
{keyCount:3,creationDateTime:2023-11-30T23:07:55.765Z,lastUpdatedDateTime:2023-12-15T03:57:52.4
```

Métodos auxiliares para la modificación del origen

Esta sección se aplica si actualiza o cambia dinámicamente el origen utilizado en la solicitud dentro del código de CloudFront Functions. Solo puede actualizar el origen cuando el espectador solicite CloudFront Functions. CloudFront Functions tiene un módulo que proporciona métodos auxiliares para actualizar o cambiar el origen de forma dinámica.

Para usar este módulo, cree una función de CloudFront con tiempo de ejecución 2.0 de JavaScript e incluya la siguiente instrucción en la primera línea del código de la función:

```
import cf from 'cloudfront';
```

Para obtener más información, consulte Características del tiempo de ejecución 2.0 de JavaScript para CloudFront Functions.

> **Note**
>
> Las páginas de la API de pruebas y la consola de pruebas no comprueban si se ha producido una modificación del origen. Sin embargo, las pruebas garantizan que el código de la función se ejecute sin errores.

Elección entre CloudFront Functions y Lambda@Edge

Puede actualizar sus orígenes mediante CloudFront Functions o Lambda@Edge.

Cuando se utiliza CloudFront Functions para actualizar los orígenes, se utiliza el desencadenador de eventos de solicitud del espectador, lo que significa que esta lógica se ejecutará en todas las solicitudes cuando se utilice esta función. Cuando se utiliza Lambda@Edge, las funciones de actualización del origen se encuentran en el desencadenador de eventos de solicitud de origen, lo que significa que esta lógica solo se ejecuta cuando se pierde memoria caché.

La elección depende en gran medida de la carga de trabajo y del uso actual de CloudFront Functions y Lambda@Edge en sus distribuciones. Las siguientes consideraciones pueden ayudarlo a decidir si debe utilizar CloudFront Functions o Lambda@Edge para actualizar sus orígenes.

CloudFront Functions es más útil en las siguientes situaciones:

- Cuando sus solicitudes son dinámicas (es decir, no se pueden almacenar en caché) y siempre van al origen. CloudFront Functions ofrece un mejor rendimiento y un coste total más bajo.
- Si tiene una función de CloudFront de solicitud de espectador existente que se ejecutará en cada solicitud, puede añadir la lógica de actualización del origen a la función existente.

Para usar CloudFront Functions para actualizar los orígenes, consulte los métodos auxiliares en los temas siguientes.

Lambda@Edge es más útil en las siguientes situaciones:

- Cuando tiene contenido que se puede almacenar en caché con gran frecuencia, Lambda@Edge puede ser más rentable, ya que solo se ejecuta cuando se pierde memoria caché, mientras que CloudFront Functions se ejecuta en todas las solicitudes.
- Si tiene una función de Lambda@Edge de solicitud de origen existente, puede añadir la lógica de actualización del origen a la función existente.
- Cuando la lógica de actualización de origen requiere obtener datos de orígenes de datos de terceros, como Amazon DynamoDB o Amazon S3.

Para obtener más información sobre Lambda@Edge, consulte Personalización en la periferia con Lambda@Edge.

Método updateRequestOrigin()

Use el método `updateRequestOrigin()` para actualizar la configuración de origen de una solicitud. Puede usar este método para actualizar las propiedades de origen existentes para los

orígenes que ya están definidos en su distribución o para definir un nuevo origen para la solicitud. Para ello, especifique las propiedades que desea cambiar.

> **Important**
>
> Cualquier configuración que no especifique en `updateRequestOrigin()` heredará la misma configuración de la configuración del origen existente.

El origen establecido por el método `updateRequestOrigin()` puede ser cualquier punto de conexión HTTP y no es necesario que sea un origen existente en la distribución de CloudFront.

> **Notas**
>
> - Si está actualizando un origen que forma parte de un grupo de origen, solo se actualiza el origen principal del grupo de origen. El origen secundario no cambia. Cualquier código de respuesta del origen modificado que coincida con los criterios de conmutación por error desencadenará una conmutación por error al origen secundario.
> - Si va a cambiar el tipo de origen y tiene habilitado el OAC, asegúrese de que el tipo de origen en `originAccessControlConfig` coincida con el nuevo tipo de origen.
> - No puede usar el método `updateRequestOrigin()` para actualizar los orígenes de la VPC. Se producirá un error en la solicitud.

Solicitud

```
updateRequestOrigin({origin properties})
```

Las `origin properties` pueden incluir lo siguiente:

domainName (opcional)

El nombre de dominio del origen. Si no se proporciona, se utiliza en su lugar el nombre de dominio del origen asignado.

Para orígenes personalizados

Especifique un nombre de dominio DNS, como `www.example.com`. El nombre de dominio no puede incluir dos puntos (`:`) ni puede ser una dirección IP. El nombre de dominio puede tener una longitud de hasta 253 caracteres.

Para orígenes de S3

Especifique el nombre de dominio DNS del bucket de Amazon S3, como `amzn-s3-demo-bucket.s3.eu-west-1.amazonaws.com`. El nombre puede tener una longitud de hasta 128 caracteres y debe escribirse en letras minúsculas.

hostHeader (opcional, para orígenes personalizados que no sean de S3)

El encabezado del host que se utilizará al realizar la solicitud al origen. Si no se proporciona, se utiliza el valor del parámetro domainName. Si no se proporciona ningún parámetro de encabezado de host ni de nombre de dominio, se utiliza el nombre de dominio del origen asignado o el encabezado de host de la solicitud entrante si la política de reenvío al origen (FTO) incluye el host. El encabezado del host no puede incluir dos puntos (`:`) ni puede ser una dirección IP. El encabezado del host puede tener una longitud de hasta 253 caracteres.

originPath (opcional)

La ruta de directorio del servidor donde la solicitud debería encontrar el contenido. La ruta debe comenzar con una barra diagonal (/), pero no debe terminar con una. Por ejemplo, no debería terminar con `example-path/`. Si no se proporciona, se utiliza la ruta de origen del origen asignado.

Para orígenes personalizados

La ruta debe estar codificada en URL y tener una longitud máxima de 255 caracteres.

customHeaders (opcional)

Si desea incluir encabezados personalizados con la solicitud, especifique un nombre de encabezado y un par de valores para cada uno de ellos. El formato es diferente al de los encabezados de solicitud y respuesta de la estructura de eventos. Use la siguiente sintaxis de pares clave-valor:

```
{"key1": "value1", "key2": "value2", ...}
```

No puede agregar encabezados que no estén permitidos y un encabezado con el mismo nombre tampoco puede estar presente en la solicitud entrante `headers`. El nombre del encabezado debe

estar en minúsculas en el código de la función. Cuando CloudFront Functions convierte el objeto de evento de nuevo en una solicitud HTTP, la primera letra de cada palabra en los nombres de encabezados se escribe en mayúsculas, y las palabras se separan con guiones.

Por ejemplo, si el código de la función agrega un encabezado llamado `example-header-name`, CloudFront lo convierte en `Example-Header-Name` en la solicitud HTTP. Para obtener más información, consulte Encabezados personalizados que CloudFront no puede agregar a solicitudes de origen y Restricciones en funciones de borde.

Si no se proporciona, se utilizará cualquier encabezado personalizado del origen asignado.

connectionAttempts (opcional)

El número de veces que CloudFront intenta conectarse al origen. El valor mínimo es 1 y el máximo, 3. Si no se proporciona, se utilizarán los intentos de conexión del origen asignado.

originShield (opcional)

Esto habilita o actualiza Origin Shield de CloudFront. El uso de Origin Shield puede ayudar a reducir la carga en el origen. Para obtener más información, consulte Uso de Amazon CloudFront Origin Shield. Si no se proporciona, se utiliza la configuración de Origin Shield del origen asignado.

enabled (obligatorio)

Expresión booleana para activar o desactivar Origin Shield. Acepta un valor `true` o `false`.

region (obligatorio cuando está habilitado)

La Región de AWS para Origin Shield. Especifique la Región de AWS que tiene la latencia más baja en su origen. Use el código de la región, no el nombre de la región. Por ejemplo, use `us-east-2` para especificar la región Este de EE. UU. (Ohio).

Cuando habilite Origin Shield de CloudFront, debe especificar la Región de AWS para Origin Shield. Para ver una lista de las Regiones de AWS disponibles y ayudarlo a elegir la mejor región para su origen, consulte Elección de la región de AWS para Origin Shield.

originAccessControlConfig (opcional)

El identificador único de un control de acceso de origen (OAC) para este origen. Esto solo se usa cuando el origen admite un OAC de CloudFront, como Amazon S3, las URL de funciones de Lambda, MediaStore y MediaPackage V2. Si no se proporciona, se utiliza la configuración de OAC del origen asignado.

Esto no admite la identidad de acceso de origen (OAI) heredada. Para obtener más información, consulte Restricción del acceso a un origen de AWS.

enabled (obligatorio)

Expresión booleana para activar o desactivar OAC. Acepta un valor `true` o `false`.

signingBehavior (obligatorio cuando está habilitado)

Especifica qué solicitudes firma CloudFront (agrega información de autenticación). Especifique `always` para el caso de uso más común. Para obtener más información, consulte Configuración avanzada para el control de acceso de origen.

Este campo puede tener uno de los siguientes valores:

- `always`: CloudFront firma todas las solicitudes de origen y sobrescribe el encabezado `Authorization` de la solicitud del lector, si existe.
- `never`: CloudFront no firma ninguna solicitud de origen. Este valor desactiva el control de acceso de origen para el origen.
- `no-override`: si la solicitud del espectador no contiene el encabezado `Authorization`, CloudFront firma la solicitud de origen. Si la solicitud del espectador contiene el encabezado `Authorization`, CloudFront no firma la solicitud de origen y, en cambio, pasa el encabezado `Authorization` de la solicitud del espectador.

> **Warning**
>
> Para pasar el encabezado `Authorization` de la solicitud del espectador, debe agregarlo a una política de solicitud de origen para todos los comportamientos de caché que utilizan los orígenes asociados a este control de acceso de origen. Para obtener más información, consulte Control de las solicitudes de origen con una política.

signingProtocol (obligatorio cuando está habilitado)

El protocolo de firma del OAC, que determina cómo CloudFront firma (autentica) las solicitudes. El único valor válido es `sigv4`.

originType (obligatorio cuando está habilitado)

El tipo de origen de este OAC. Los valores válidos son `s3`, `mediapackagev2`, `mediastore` y `lambda`.

timeouts (opcional)

Tiempos de espera en los que puede especificar durante cuánto tiempo CloudFront debe intentar esperar a que los orígenes respondan o envíen datos. Si no se proporciona, se utiliza la configuración de tiempo de espera del origen asignado.

> **Note**
>
> A menos que se especifique lo contrario, estos tiempos de espera son compatibles tanto con orígenes personalizados como con orígenes de Amazon S3.

readTimeout (opcional)

`readTimeout` se aplica a los dos valores siguientes:

- Tiempo (en segundos) que CloudFront espera una respuesta después de enviar una solicitud al origen.
- Tiempo (en segundos) que CloudFront espera después de recibir el paquete de una respuesta desde el origen y antes de recibir el paquete siguiente.

El tiempo de espera mínimo es 1 segundo; el máximo es 120 segundos. Para obtener más información, consulte Tiempo de espera de respuesta.

responseCompletionTimeout (opcional)

El tiempo (en segundos) que una solicitud de CloudFront al origen puede permanecer abierta y esperar una respuesta. Si en ese tiempo no se recibe la respuesta completa del origen, CloudFront finaliza la conexión.

El valor de `responseCompletionTimeout` debe ser igual o mayor que el valor para `readTimeout`. Para obtener más información, consulte Tiempo de espera de finalización de la respuesta.

keepAliveTimeout (opcional)

Este tiempo de espera solo se aplica a los orígenes personalizados, no a los orígenes de Amazon S3. (Las configuraciones de origen S3 omitirán esta configuración).

`keepAliveTimeout` especifica el tiempo que CloudFront debería intentar mantener la conexión con el origen después de recibir el último paquete de la respuesta. El tiempo de espera mínimo es 1 segundo; el máximo es 120 segundos. Para obtener más información, consulte Tiempo de espera de keep-alive (solo orígenes personalizados y de VPC).

connectionTimeout (opcional)

Número de segundos que espera CloudFront al intentar establecer una conexión con el origen. El tiempo de espera mínimo es 1 segundo; el máximo es 10 segundos. Para obtener más información, consulte Tiempo de espera de conexión.

customOriginConfig (opcional)

Se utiliza `customOriginConfig` para especificar la configuración de conexión para los orígenes que no son un bucket de Amazon S3. Hay una excepción: puede especificar esta configuración si el bucket de S3 está configurado con alojamiento de sitios web estáticos. (Otros tipos de configuraciones de bucket de S3 ignorarán esta configuración). Si no se proporciona `customOriginConfig`, se utiliza la configuración del origen asignado.

port (obligatorio)

El puerto HTTP que CloudFront utiliza para conectarse al origen. Especifique el puerto HTTP que escucha el origen.

protocol (obligatorio)

Especifica el protocolo (HTTP o HTTPS) que CloudFront utiliza para conectarse al origen. Los valores válidos son los siguientes:

- `http`: CloudFront utiliza siempre HTTP para conectarse al origen
- `https`: CloudFront utiliza siempre HTTPS para conectarse al origen

sslProtocols (obligatorio)

Una lista que especifica el protocolo SSL/TLS mínimo que CloudFront utiliza al conectarse a su origen a través de HTTPS. Los valores válidos son `SSLv3`, `TLSv1`, `TLSv1.1` y `TLSv1.2`. Para obtener más información, consulte Protocolo SSL mínimo del origen.

ipAddressType (opcional)

Especifica el tipo de dirección IP que CloudFront utiliza para conectarse al origen. Los valores válidos son `ipv4`, `ipv6` y `dualstack`. Los cambios de `ipAddressType` solo se admiten cuando también se está cambiando la propiedad de `domainName`.

sni (opcional, para orígenes personalizados que no sean de S3)

La indicación de nombre de servidor (SNI) es una extensión del protocolo seguridad de la capa de transporte (TLS) mediante el cual un cliente indica el nombre de host al que intenta conectarse al inicio del proceso de establecimiento de comunicación de TLS. Este valor debe coincidir con un

nombre común de un certificado TLS del servidor de origen. De lo contrario, el servidor de origen puede generar un error.

Si no se proporciona, se utiliza el valor del parámetro `hostHeader`. Si no se proporciona el encabezado del host, se utiliza el valor del parámetro `domainName`.

Si no se proporciona ningún parámetro de encabezado de host ni de nombre de dominio, se utiliza el nombre de dominio del origen asignado o el encabezado de host de la solicitud entrante si la política de reenvío al origen (FTO) incluye el host. La SNI no puede incluir dos puntos (`:`) ni puede ser una dirección IP. La SNI puede tener hasta 253 caracteres.

allowedCertificateNames (opcional, para orígenes personalizados que no sean de S3)

Puede incluir una lista de nombres de certificados válidos que CloudFront utilizará para validar la coincidencia del dominio con el certificado TLS del servidor de origen durante el establecimiento de comunicación de TLS con el servidor de origen. Este campo espera una matriz de nombres de dominio válidos y puede incluir dominios comodín, como `*.example.com`.

Puede especificar hasta 20 nombres de certificado permitidos. Cada nombre de certificado puede tener hasta 64 caracteres.

Example: actualización al origen de la solicitud de Amazon S3

El siguiente ejemplo cambia el origen de la solicitud del espectador a un bucket de S3, activa el OAC y restablece los encabezados personalizados enviados al origen.

```
cf.updateRequestOrigin({
    "domainName" : "amzn-s3-demo-bucket-in-us-east-1.s3.us-east-1.amazonaws.com",
    "originAccessControlConfig": {
        "enabled": true,
        "signingBehavior": "always",
        "signingProtocol": "sigv4",
        "originType": "s3"
    },
    // Empty object resets any header configured on the assigned origin
    "customHeaders": {}
});
```

Example: actualización al origen de la solicitud del equilibrador de carga de aplicación

El siguiente ejemplo cambia el origen de la solicitud del espectador a un origen de equilibrador de carga de aplicación y establece un encabezado personalizado y tiempos de espera.

```
cf.updateRequestOrigin({
    "domainName" : "example-1234567890.us-east-1.elb.amazonaws.com",
    "timeouts": {
        "readTimeout": 30,
        "connectionTimeout": 5
    },
    "customHeaders": {
        "x-stage": "production",
        "x-region": "us-east-1"
    }
});
```

Example: actualización al origen con Origin Shield activado

En el siguiente ejemplo, el origen de la distribución tiene Origin Shield activado. El código de función actualiza solo el nombre de dominio utilizado para el origen y omite todos los demás parámetros opcionales. En este caso, Origin Shield seguirá utilizándose con el nombre de dominio del origen modificado porque los parámetros de Origin Shield no se actualizaron.

```
cf.updateRequestOrigin({
    "domainName" : "www.example.com"
});
```

Example- Actualización del encabezado del host, la SNI y los nombres de los certificados permitidos

> **Warning**
>
> En la mayoría de los casos de uso, no necesitará usar este tipo de modificación en las solicitudes que se dirijan al origen. Estos parámetros no deberían usarse a menos que entienda el impacto de cambiar estos valores.

En el siguiente ejemplo, se cambia al origen el nombre de dominio, el encabezado del host, la SNI y los certificados permitidos en la solicitud.

```
cf.updateRequestOrigin({
    "domainName": "www.example.com",
    "hostHeader": "test.example.com",
    "sni": "test.example.net",
    "allowedCertificateNames": ["*.example.com", "*.example.net"],
```

```
});
```

Método selectRequestOriginById()

Utilice `selectRequestOriginById()` para actualizar un origen existente mediante la selección un origen diferente que ya esté configurado en la distribución. Este método utiliza toda la configuración definida por el origen actualizado.

Este método solo acepta orígenes que ya estén definidos en la misma distribución utilizada al ejecutar la función. Se hace referencia a los orígenes por el ID de origen, que es el nombre del origen que se ha definido al configurar el origen.

Si tiene un origen de VPC configurado en la distribución, puede utilizar este método para actualizar el origen al origen de VPC. Para obtener más información, consulte Restricción del acceso con orígenes de la VPC.

> **Notas**
>
> - La función `selectRequestOriginById()` no puede seleccionar un origen que tenga habilitado TLS mutua (origen). Si se intenta seleccionar un origen habilitado de TLS mutua (origen) mediante esta función, se producirá un error de validación.
> - Si su caso de uso requiere una selección de origen dinámica con TLS mutua (origen), utilice `updateRequestOrigin()` en su lugar, asegurándose de que todos los orígenes de destino utilicen el mismo certificado de cliente.

Solicitud

```
cf.selectRequestOriginById(origin_id, {origin_overrides})
```

En el ejemplo anterior, `origin_id` es una cadena que apunta al nombre de un origen en la distribución que está ejecutando la función. El parámetro `origin_overrides` puede contener lo siguiente:

hostHeader (opcional, para orígenes personalizados que no sean de S3)

El encabezado del host que se utilizará al realizar la solicitud al origen. Si no se proporciona, se utiliza el valor del parámetro `domainName`.

Si no se proporciona ningún parámetro de encabezado de host ni de nombre de dominio, se utiliza el nombre de dominio del origen asignado o el encabezado de host de la solicitud entrante si la política de reenvío al origen (FTO) incluye el host. El encabezado del host no puede incluir dos puntos (`:`) ni puede ser una dirección IP. El encabezado del host puede tener una longitud de hasta 253 caracteres.

sni (opcional, para orígenes personalizados que no sean de S3)

La indicación de nombre de servidor (SNI) es una extensión del protocolo seguridad de la capa de transporte (TLS) mediante el cual un cliente indica el nombre de host al que intenta conectarse al inicio del proceso de establecimiento de comunicación de TLS. Este valor debe coincidir con un nombre común de un certificado TLS del servidor de origen. De lo contrario, el servidor de origen puede generar un error.

Si no se proporciona, se utiliza el valor del parámetro `hostHeader`. Si no se proporciona el encabezado del host, se utiliza el valor del parámetro `domainName`.

Si no se proporciona ningún parámetro de encabezado de host ni de nombre de dominio, se utiliza el nombre de dominio del origen asignado o el encabezado de host de la solicitud entrante si la política de reenvío al origen (FTO) incluye el host. La SNI no puede incluir dos puntos (`:`) ni puede ser una dirección IP. La SNI puede tener hasta 253 caracteres.

allowedCertificateNames (opcional, para orígenes personalizados que no sean de S3)

Puede incluir una lista de nombres de certificados válidos que CloudFront utilizará para validar la coincidencia del dominio con el certificado TLS del servidor de origen durante el establecimiento de comunicación de TLS con el servidor de origen. Este campo espera una matriz de nombres de dominio válidos y puede incluir dominios comodín, como `*.example.com`.

Puede especificar hasta 20 nombres de certificado permitidos. Cada nombre de certificado puede tener hasta 64 caracteres.

Solicitud

```
selectRequestOriginById(origin_id)
```

En el ejemplo anterior, `origin_id` es una cadena que apunta al nombre de un origen en la distribución que está ejecutando la función.

Example: selección del origen de solicitud de Amazon S3

El siguiente ejemplo selecciona el origen denominado `amzn-s3-demo-bucket-in-us-east-1` de la lista de orígenes asociados a la distribución y aplica los ajustes de configuración del origen `amzn-s3-demo-bucket-in-us-east-1` a la solicitud.

```
cf.selectRequestOriginById("amzn-s3-demo-bucket-in-us-east-1");
```

Example: selección del origen de la solicitud del equilibrador de carga de aplicación

El siguiente ejemplo selecciona un origen del equilibrador de carga de aplicación denominado `myALB-prod` de la lista de orígenes asociada a la distribución y aplica los ajustes de configuración de `myALB-prod` a la solicitud.

```
cf.selectRequestOriginById("myALB-prod");
```

Example- Selección del origen de la solicitud del equilibrador de carga de aplicación e invalidación del encabezado del host

Como en el ejemplo anterior, el siguiente ejemplo selecciona un origen del equilibrador de carga de aplicación denominado `myALB-prod` de la lista de orígenes asociada a la distribución y aplica los ajustes de configuración de `myALB-prod` a la solicitud. Sin embargo, este ejemplo invalida el valor del encabezado del host mediante `origin_overrides`.

```
cf.overrideRequestOrigin("myALB-prod",{
        "hostHeader" : "test.example.com"
});
```

Método createRequestOriginGroup()

Utilice `createRequestOriginGroup()` para definir dos orígenes que se utilizarán como grupo de orígenes para la conmutación por error en escenarios que requieren alta disponibilidad.

Un grupo de orígenes incluye dos orígenes (uno principal y otro secundario) y un criterio de conmutación por error especificado. Cree un grupo de origen para admitir la conmutación por error de origen en CloudFront. Cuando cree o actualice un grupo de orígenes mediante este método, puede especificar el grupo de orígenes en lugar de un único origen. CloudFront realizará la conmutación por error del origen principal al secundario, mediante los criterios de conmutación por error.

Si tiene un origen de VPC configurado en la distribución, puede utilizar este método para crear un grupo de orígenes utilizando un origen de VPC. Para obtener más información, consulte Restricción del acceso con orígenes de la VPC.

> **Notas**
>
> - La función `createRequestOriginGroup()` no admite la creación de grupos de orígenes que incluyan orígenes habilitados de TLS mutua (origen). Los grupos de origen con orígenes de TLS mutua (origen) no se pueden crear dinámicamente mediante CloudFront Functions.
> - Si necesita capacidades de conmutación por error de origen con TLS mutua (origen), configure los grupos de origen directamente en la configuración de distribución de CloudFront, en lugar de crearlos de forma dinámica en funciones.

Solicitud

```
createRequestOriginGroup({origin_group_properties})
```

En el ejemplo anterior, el archivo `origin_group_properties` contiene lo siguiente:

originIds (obligatorio)

Matriz de `origin_ids`, donde `origin_id` es una cadena que apunta al nombre de un origen en la distribución que ejecuta la función. Debe proporcionar dos orígenes como parte de la matriz. El primer origen de la lista es el origen principal y el segundo sirve como segundo origen a efectos de conmutación por error.

originOverrides (opcional)

Se pueden sobrescribir algunos ajustes avanzados mediante el parámetro `{origin_overrides}`. Las `origin overrides` pueden incluir lo siguiente:

hostHeader (opcional, para orígenes personalizados que no sean de S3)

El encabezado del host que se utilizará al realizar la solicitud al origen. Si no se proporciona, se utiliza el valor del parámetro `domainName`.

Si no se proporciona ningún parámetro de encabezado de host ni de nombre de dominio, se utiliza el nombre de dominio del origen asignado o el encabezado de host de la solicitud

entrante si la política de reenvío al origen (FTO) incluye el host. El encabezado del host no puede incluir dos puntos (`:`) ni puede ser una dirección IP. El encabezado del host puede tener una longitud de hasta 253 caracteres.

sni (opcional, para orígenes personalizados que no sean de S3)

La indicación de nombre de servidor (SNI) es una extensión del protocolo seguridad de la capa de transporte (TLS) mediante el cual un cliente indica el nombre de host al que intenta conectarse al inicio del proceso de establecimiento de comunicación de TLS. Este valor debe coincidir con un nombre común de un certificado TLS del servidor de origen, de lo contrario, el servidor de origen puede generar un error.

Si no se proporciona, se utiliza el valor del parámetro `hostHeader`. Si no se proporciona el encabezado del host, se utiliza el valor del parámetro `domainName`.

Si no se proporciona ningún parámetro de encabezado de host ni de nombre de dominio, se utiliza el nombre de dominio del origen asignado o el encabezado de host de la solicitud entrante si la política de reenvío al origen (FTO) incluye el host. La SNI no puede incluir dos puntos (`:`) ni puede ser una dirección IP. La SNI puede tener hasta 253 caracteres.

allowedCertificateNames (opcional, para orígenes personalizados que no sean de S3)

Puede incluir una lista de nombres de certificados válidos que CloudFront utilizará para validar la coincidencia del dominio con el certificado TLS del servidor de origen durante el establecimiento de comunicación de TLS con el servidor de origen. Este campo espera una matriz de nombres de dominio válidos y puede incluir dominios comodín, como `*.example.com`.

Puede especificar hasta 20 nombres de certificado permitidos. Cada nombre de certificado puede tener hasta 64 caracteres.

selectionCriteria (opcional)

Seleccione si desea utilizar los criterios de conmutación por error del origen `default` o utilizar la lógica de conmutación por error basada en `media-quality-score`. Los valores válidos son los siguientes:

- `default` utiliza los criterios de conmutación por error basados en los códigos de estado que se especifican en `failoverCriteria`. Si no configura `selectionCriteria` en la función, se utilizará `default`.
- `media-quality-score` se utiliza cuando se emplea la capacidad de enrutamiento con reconocimiento multimedia.

failoverCriteria (obligatorio)

Una matriz de códigos de estado que, cuando se devuelven desde el origen principal, desencadenarán que CloudFront conmute por error al origen secundario. Si sobrescribe un grupo de orígenes existente, esta matriz sobrescribirá todos los códigos de estado de conmutación por error establecidos en la configuración original del grupo de orígenes.

Cuando utilice `media-quality-score` `selectionCriteria`, CloudFront intentará enrutar las solicitudes basándose en la puntuación de calidad de los medios. Si el origen seleccionado devuelve un código de error establecido en esta matriz, CloudFront realizará la conmutación por error al otro origen.

Example: creación del grupo de orígenes de solicitudes

En el siguiente ejemplo se crea un grupo de orígenes para una solicitud mediante los ID de origen. Estos ID de origen proceden de la configuración del grupo de orígenes para la distribución utilizada para ejecutar esta función.

Si lo desea, puede usar `originOverrides` para invalidar las configuraciones del grupo de origen para `sni`, `hostHeader` y `allowedCertificateNames`.

```
import cf from 'cloudfront';

function handler(event) {
    cf.createRequestOriginGroup({
        "originIds": [
            {
                "originId": "origin-1",
                "originOverrides": {
                    "hostHeader": "hostHeader.example.com",
                    "sni": "sni.example.com",
                    "allowedCertificateNames": ["cert1.example.com",
 "cert2.example.com", "cert3.example.com"]
                }
            },
            {
                "originId": "origin-2",
                "originOverrides": {
                    "hostHeader": "hostHeader2.example.com",
                    "sni": "sni2.example.com",
                    "allowedCertificateNames": ["cert4.example.com",
 "cert5.example.com"]
```

```
                }
            }
        ],
        "failoverCriteria": {
            "statusCodes": [500]
        }
    });

    event.request.headers['x-hookx'] = { value: 'origin-overrides' };
    return event.request;
}
```

Métodos auxiliares para las propiedades de CloudFront SaaS Manager

Utilice las siguientes funciones auxiliares de CloudFront SaaS Manager para recuperar los valores de las distribuciones de varios inquilinos en la función que cree. Para utilizar los ejemplos de esta página, primero debe crear una función de CloudFront utilizando el tiempo de ejecución 2.0 de JavaScript. Para obtener más información, Características del tiempo de ejecución 2.0 de JavaScript para CloudFront Functions.

Temas

- Grupos de conexiones
- Inquilinos de distribución

Grupos de conexiones

El grupo de conexiones que está asociado a los inquilinos de distribución tiene un nombre de dominio.

Para obtener este valor, utilice el campo `endpoint` del subobjeto `context` del objeto de evento.

Solicitud

```
const value = event.context.endpoint;
```

Respuesta

La respuesta es una `string` que contiene el nombre de dominio del grupo de conexiones, como d111111abcdef8.cloudfront.net. El campo `endpoint` solo aparece cuando se invoca la función

para una distribución de varios inquilinos con un grupo de conexiones asociado. Para obtener más información, consulte Objeto Context (Contexto).

Inquilinos de distribución

CloudFront Functions tiene un módulo que proporciona acceso a valores específicos de inquilinos de distribución.

Para usar este módulo, incluya la siguiente instrucción en la primera línea del código de la función:

```
import cf from 'cloudfront';
```

Puede usar los siguientes ejemplos solo en la función `handler`, ya sea directamente o mediante cualquier función de llamada anidada.

`distributionTenant.id`Campo de

Utilice este campo para obtener el valor del ID del inquilino de distribución.

Solicitud

```
const value = cf.distributionTenant.id;
```

Respuesta

La respuesta es una `string` que contiene el ID del inquilino de distribución, por ejemplo, `dt_1a2b3c4d5e6f7`.

Gestión de errores

Si se invoca la función para una distribución estándar, al especificar el campo `distributionTenant.id` se devolverá el error de tipo `distributionTenant module is not available`. Para gestionar este caso de uso, puede agregar un bloque `try` y `catch` al código.

`distributionTenant.parameters.get()`Método de

Utilice este método para devolver el valor de los nombres de parámetro de inquilino de distribución que especifique.

```
distributionTenant.parameters.get("key");
```

`key`: el nombre del parámetro del inquilino de distribución cuyo valor desea obtener.

Solicitud

```
const value = distributionTenant.parameters.get("key");
```

Respuesta

La respuesta es una `string` que contiene el valor del parámetro del inquilino de distribución. Por ejemplo, si el nombre de la clave es `TenantPath`, entonces el valor de este parámetro podría ser `tenant1`.

Gestión de errores

Es posible que reciba los errores siguientes:

- Si se invoca la función para una distribución estándar, el método `distributionTenant.parameters.get()` devolverá el error de tipo `distributionTenant module is not available`.
- El error `DistributionTenantParameterKeyNotFound` se devuelve cuando el parámetro de inquilino de distribución que especificó no existe.

Para administrar estos casos de uso, puede agregar un bloque `try` y `catch` al código.

Utilice async y await

Las funciones de tiempo de ejecución 2.0 de JavaScript de CloudFront Functions proporcionan una sintaxis `async` y `await` para gestionar los objetos `Promise`. Las promesas representan resultados retrasados a los que se puede acceder mediante la palabra clave `await` en las funciones marcadas como `async`. Varias funciones nuevas de WebCrypto utilizan promesas.

Para obtener más información sobre los objetos `Promise`, consulte Promesa.

> **Note**
>
> Debe usar el tiempo de ejecución de JavaScript 2.0 para las siguientes muestras de código. `await` solo se puede usar dentro de funciones `async`. No se admiten argumentos ni cierres de `async`.

```
async function answer() {
```

```
    return 42;
}

// Note: async, await can be used only inside an async function. async arguments and
 closures are not supported.

async function handler(event) {
    // var answer_value = answer(); // returns Promise, not a 42 value
    let answer_value = await answer(); // resolves Promise, 42
    console.log("Answer"+answer_value);
    event.request.headers['answer'] = { value : ""+answer_value };
    return event.request;
}
```

El siguiente ejemplo de código JavaScript muestra cómo ver las promesas con el método en cadena `then`. Se puede utilizar `catch` para ver los errores.

> **Warning**
>
> El uso de combinadores de promesas (por ejemplo, `Promise.all`, `Promise.any`) y métodos de cadena de promesas (por ejemplo, `then` y `catch`) puede requerir un uso elevado de la memoria de la función. Si la función supera la cuota de memoria máxima de la función, no se ejecutará. Para evitar este error, recomendamos que utilice la sintaxis `await` en lugar de los métodos `promise`.

```
async function answer() {
    return 42;
}

async function squared_answer() {
   return answer().then(value => value * value)
}
// Note: async, await can be used only inside an async function. async arguments and
 closures are not supported.
async function handler(event) {
    // var answer_value = answer(); // returns Promise, not a 42 value
    let answer_value = await squared_answer(); // resolves Promise, 42
    console.log("Answer"+answer_value);
    event.request.headers['answer'] = { value : ""+answer_value };
    return event.request;
```

```
}
```

Compatibilidad con CWT para CloudFront Functions

En esta sección, se proporcionan detalles sobre la compatibilidad con los tókenes web CBOR (CWT) en las CloudFront Functions, lo que permite la autenticación y la autorización seguras basadas en tókenes en las ubicaciones periféricas de CloudFront. Esta compatibilidad se proporciona como un módulo, al que se puede acceder desde CloudFront Functions.

Para usar este módulo, cree una función de CloudFront con tiempo de ejecución 2.0 de JavaScript e incluya la siguiente instrucción en la primera línea del código de la función:

```
import cf from 'cloudfront';
```

Los métodos asociados a este módulo son accesibles mediante (donde * es un comodín que representa las diferentes funciones presentes en el módulo):

```
cf.cwt.*
```

Para obtener más información, consulte Características del tiempo de ejecución 2.0 de JavaScript para CloudFront Functions.

Actualmente, el módulo solo admite la estructura MAC0 con el algoritmo HS256 (HMAC-SHA256) con un límite de 1 KB para el tamaño máximo del token.

Estructura de token

En esta sección se describe la estructura de token que espera el módulo de CWT. El módulo espera que el token esté correctamente etiquetado y sea identificable (por ejemplo, COSE MAC0). Además, en cuanto a la estructura del token, el módulo sigue los estándares establecidos por Firma y cifrado de objetos CBOR (COSE) [RFC 8152].

```
( // CWT Tag (Tag value: 61) --- optional
    ( // COSE MAC0 Structure Tag (Tag value: 17) --- required
        [
            protectedHeaders,
            unprotectedHeaders,
            payload,
            tag,
        ]
    )
```

```
)
```

Example: CWT utiliza la estructura COSE MAC0

```
61( // CWT tag
    17( // COSE_MAC0 tag
        [
            { // Protected Headers
                1: 4  // algorithm : HMAC-256-64
            },
            { // Unprotected Headers
                4: h'53796d6d6574726963323536' // kid : Symmetric key id
            },
            { // Payload
                1: "https://iss.example.com", // iss
                2: "exampleUser", // sub
                3: "https://aud.example.com", // aud
                4: 1444064944, // exp
                5: 1443944944, // nbf
                6: 1443944944, // iat
            },
            h'093101ef6d789200' // tag
        ]
    )
)
```

> **Note**
>
> La etiqueta de CWT es opcional a la hora de generar los tókenes. Sin embargo, se requiere la etiqueta de estructura COSE.

método validateToken()

La función decodifica y valida un token de CWT con la clave especificada. Si la validación es exitosa, devuelve el token de CWT decodificado. De lo contrario, emite un error. Tenga en cuenta que esta función no valida el conjunto de reclamaciones.

Solicitud

```
cf.cwt.validateToken(token, handlerContext{key})
```

Parameters

token (obligatorio)

Token codificado para la validación. Debe ser un búfer de JavaScript.

handlerContext (obligatorio)

Un objeto de JavaScript que almacena el contexto de la llamada a validateToken. Por el momento, solo se admite la propiedad de la clave.

clave (obligatorio)

Clave secreta para el cálculo del resumen del mensaje. Se puede proporcionar como cadena o búfer de JavaScript.

Respuesta

Cuando el método `validateToken()` devuelve un token validado correctamente, la respuesta de la función es un `CWTObject` en el siguiente formato. Una vez decodificadas, todas las claves de reclamación se representan como cadenas.

```
CWTObject {
    protectedHeaders,
    unprotectedHeaders,
    payload
}
```

Ejemplo: Validación del token con el identificador enviado como parte del token

En este ejemplo, se muestra la validación del token de CWT, en la que se extrae el identificador del encabezado. A continuación, el identificador pasa a KeyValueStore de CloudFront Functions para obtener la clave secreta utilizada para validar el token.

```
import cf from 'cloudfront'

const CwtClaims = {
   iss: 1,
   aud: 3,
   exp: 4
}

async function handler(event) {
```

```
    try {
        let request = event.request;
        let encodedToken = request.headers['x-cwt-token'].value;
        let kid = request.headers['x-cwt-kid'].value;

        // Retrieve the secret key from the kvs
        let secretKey = await cf.kvs().get(kid);

        // Now you can use the secretKey to decode & validate the token.
        let tokenBuffer = Buffer.from(encodedToken, 'base64url');

        let handlerContext = {
           key: secretKey,
        }

        try {
            let cwtObj = cf.cwt.validateToken(tokenBuffer, handlerContext);

            // Check if token is expired
            const currentTime = Math.floor(Date.now() / 1000); // Current time in
 seconds
            if (cwtObj[CwtClaims.exp] && cwtObj[CwtClaims.exp] < currentTime) {
                return {
                    statusCode: 401,
                    statusDescription: 'Token expired'
                };
            }
        } catch (error) {
            return {
               statusCode: 401,
               statusDescription: 'Invalid token'
            };
         }
    } catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
     }
    return request;
}
```

método generateToken()

Esta función genera un nuevo token de CWT mediante la carga útil y la configuración de contexto proporcionados.

Solicitud

```
cf.cwt.generateToken(generatorContext, payload)
```

Parameters

generatorContext (obligatorio)

Se trata de un objeto de JavaScript que se utiliza como contexto para generar el token y contiene los siguientes pares de valores clave:

cwTag (opcional)

Este valor es un booleano que, si `true` lo especifica, `cwtTag` se debe agregar.

coseTag (obligatorio)

Especifica el tipo de etiqueta de COSE. Actualmente, solo admite `MAC0`.

clave (obligatorio)

Clave secreta para el cálculo del resumen del mensaje. Este valor puede ser una cadena o JavaScript `Buffer`.

carga útil (obligatorio)

Carga útil del token para la codificación. La carga útil debe estar en formato `CWTObject`.

Respuesta

Devuelve un búfer de JavaScript que contiene el token codificado.

Example: genera un token de CWT

```
import cf from 'cloudfront';

const CwtClaims = {
    iss: 1,
    sub: 2,
    exp: 4
```

```
};

const CatClaims = {
    catu: 401,
    catnip: 402,
    catm: 403,
    catr: 404
};

const Catu = {
    host: 1,
    path: 2,
    ext: 3
};

const CatuMatchTypes = {
    prefix_match: 1,
    suffix_match: 2,
    exact_match: 3
};

const Catr = {
    renewal_method: 1,
    next_renewal_time: 2,
    max_uses: 3
};

async function handler(event) {
    try {
        const response = {
            statusCode: 200,
            statusDescription: 'OK',
            headers: {}
        };

        const commonAccessToken = {
            protected: {
                1: "5",
            },
            unprotected: {},
            payload: {
                [CwtClaims.iss]: "cloudfront-documentation",
                [CwtClaims.sub]: "cwt-support-on-cloudfront-functions",
                [CwtClaims.exp]: 1740000000,
```

```
                [CatClaims.catu]: {
                    [Catu.host]: {
                        [CatuMatchTypes.suffix_match]: ".cloudfront.net"
                    },
                    [Catu.path]: {
                        [CatuMatchTypes.prefix_match]: "/media/live-stream/cf-4k/"
                    },
                    [Catu.ext]: {
                        [CatuMatchTypes.exact_match]: [
                            ".m3u8",
                            ".ts",
                            ".mpd"
                        ]
                    }
                },
                [CatClaims.catnip]: [
                    "[IP_ADDRESS]",
                    "[IP_ADDRESS]"
                ],
                [CatClaims.catm]: [
                    "GET",
                    "HEAD"
                ],
                [CatClaims.catr]: {
                    [Catr.renewal_method]: "header_renewal",
                    [Catr.next_renewal_time]: 1750000000,
                    [Catr.max_uses]: 5
                }
            }
        };

        if (!request.headers['x-cwt-kid']) {
            throw new Error('Missing x-cwt-kid header');
        }

        const kid = request.headers['x-cwt-kid'].value;
        const secretKey = await cf.kvs().get(kid);

        if (!secretKey) {
            throw new Error('Secret key not found for provided kid');
        }

        try {
            const genContext = {
```

```
                cwtTag: true,
                coseTag: "MAC0",
                key: secretKey
            };

            const tokenBuffer = cf.cwt.generateToken(commonAccessToken, genContext);
            response.headers['x-generated-cwt-token'] = { value:
 tokenBuffer.toString('base64url') };

            return response;
        } catch (tokenError) {
            return {
                statusCode: 401,
                statusDescription: 'Could not generate the token'
            };
        }
    } catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
    }
}
```

Example: actualice el token según alguna lógica

```
import cf from 'cloudfront'

const CwtClaims = {
   iss: 1,
   aud: 3,
   exp: 4
}

async function handler(event) {
    try {
        let request = event.request;
        let encodedToken = request.headers['x-cwt-token'].value;
        let kid = request.headers['x-cwt-kid'].value;
        let secretKey = await cf.kvs().get(kid); // Retrieve the secret key from the
 kvs

        // Now you can use the secretKey to decode & validate the token.
```

```
        let tokenBuffer = Buffer.from(encodedToken, 'base64url');

        let handlerContext = {
           key: secretKey,
        }

        try {
            let cwtJSON = cf.cwt.validateToken(tokenBuffer, handlerContext);

            // Check if token is expired
            const currentTime = Math.floor(Date.now() / 1000); // Current time in
 seconds
            if (cwtJSON[CwtClaims.exp] && cwtJSON[CwtClaims.exp] < currentTime) {
                // We can regnerate the token and add 8 hours to the expiry time
                cwtJSON[CwtClaims.exp] = Math.floor(Date.now() / 1000) + (8 * 60 * 60);

                let genContext = {
                  coseTag: "MAC0",
                  key: secretKey
                }

                let newTokenBuffer = cf.cwt.generateToken(cwtJSON, genContext);
                 request.headers['x-cwt-regenerated-token'] =
 newTokenBuffer.toString('base64url');
            }
        } catch (error) {
            return {
               statusCode: 401,
               statusDescription: 'Invalid token'
            };
         }
    }
    catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
     }
    return request;
}
```

Métodos de ayuda generales

Esta página proporciona métodos de ayuda adicionales en CloudFront Functions. Para usar estos métodos, cree una función de CloudFront con tiempo de ejecución 2.0 de JavaScript.

```
import cf from 'cloudfront';
```

Para obtener más información, consulte Características del tiempo de ejecución 2.0 de JavaScript para CloudFront Functions.

`edgeLocation`Metadatos de

Este método requiere el uso del modulo `cloudfront`.

> **Note**
>
> Solo puede utilizar este método para las funciones de solicitud del espectador. Para las funciones de respuesta del espectador, este método está vacío.

Utilice este objeto de JavaScript para obtener el código del aeropuerto de ubicación periférica, la región de Caché periférica regional prevista o la dirección IP del servidor de CloudFront utilizada para gestionar la solicitud. Estos metadatos solo están disponibles cuando el espectador solicita desencadenar el evento.

```
cf.edgeLocation = {
    name: SEA
    serverIp: 1.2.3.4
    region: us-west-2
}
```

El objeto `cf.edgeLocation` puede incluir lo siguiente:

name

El código IATA de tres letras de la ubicación periférica que gestionó la solicitud.

serverIp

Dirección IPv4 o IPv6 del servidor que gestionó la solicitud.

region

La caché periférica regional (REC) de CloudFront que se espera que utilice la solicitud en caso de falta de memoria caché. Este valor no se actualiza en caso de que el REC esperado no esté disponible y se utilice un REC de copia de seguridad para la solicitud. Esto no incluye la ubicación de Origin Shield que se utilice, excepto en los casos en que el REC principal y el Origin Shield estén en la misma ubicación.

> **Note**
>
> CloudFront Functions no se invoca por segunda vez cuando CloudFront está configurado para usar la conmutación por error de origen. Para obtener más información, consulte Optimización de alta disponibilidad con conmutación por error de origen de CloudFront.

`rawQueryString()`Método de

Este método no requiere el módulo `cloudFront`.

Utilice el método `rawQueryString()` para recuperar la cadena de consulta no analizada y no modificada como una cadena.

Solicitud

```
function handler(event) {
    var request = event.request;
    const qs = request.rawQueryString();
}
```

Respuesta

Devuelve la cadena de consulta completa de la solicitud entrante como un valor de cadena sin ? al principio.

- Si no hay una cadena de consulta, pero ? está presente, la función devuelve una cadena vacía.
- Si no hay una cadena de consulta y ? no está presente, la función devuelve `undefined`.

Caso 1: se devuelve la cadena de consulta completa (sin **?** al principio)

URL de solicitud entrante: `https://example.com/page?name=John&age=25&city=Boston`

`rawQueryString()` devuelve: `"name=John&age=25&city=Boston"`

Caso 2: se devuelve una cadena vacía (cuando **?** está presente pero sin parámetros)

URL de solicitud entrante: `https://example.com/page?`

`rawQueryString()` devuelve: `""`

Caso 3: se devuelve **`undefined`** (sin cadena de consulta ni **?**)

URL de solicitud entrante: `https://example.com/page`

`rawQueryString()` devuelve: `undefined`

Creación de funciones

La función se crea en dos etapas:

1. Crear el código de función como JavaScript. Puede utilizar el ejemplo predeterminado de la consola de CloudFront o escribir el suyo propio. Para obtener más información, consulte los temas siguientes:
   - Escritura de código de función
   - the section called “Estructura de evento”
   - Ejemplos de CloudFront Functions para CloudFront
2. Utilice CloudFront para crear la función e incluir el código. El código existe dentro de la función (no como referencia).

Console

Para crear una función

1. Inicie sesión en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions y elija la página Funciones.
2. Seleccione Creación de función.

3. Introduzca un nombre de función que sea único en la Cuenta de AWS, elija la versión de Java Script y, a continuación, elija Continuar. Aparece la página de detalles de la nueva función.

> **Note**
>
> Para utilizar pares clave-valor en la función, debe elegir tiempo de ejecución 2.0 de Java Script.

4. En la sección Código de función, seleccione la pestaña Compilación e introduzca el código de función. El código de ejemplo que se incluye en la pestaña Compilación ilustra la sintaxis básica del código de la función.
5. Elija Guardar cambios.
6. Si el código de la función utiliza pares clave-valor, debe asociar un almacén de clave-valor.

   Puede asociar el almacén de clave-valor cuando crea en primer lugar la función. O bien, puede asociarlo más adelante, actualizando la función.

   Para asociar un almacén clave-valor ahora, siga estos pasos:

   - Vaya a la sección Asociar KeyValueStore y elija Asociar KeyValueStore existente.
   - Seleccione el almacén de clave-valor que contiene los pares clave-valor de la función y, a continuación, elija Asociar KeyValueStore.

   CloudFront asocia inmediatamente el almacén a la función. No necesita guardar la función.

CLI

Si utiliza la CLI, normalmente crea primero el código de la función en un archivo y, a continuación, crea la función con la AWS CLI.

Para crear una función

1. Cree el código de la función en un archivo y guárdelo en un directorio al que se pueda conectar el equipo.
2. Ejecute el comando como se muestra en el ejemplo. En este ejemplo, se utiliza la notación `fileb://` para transmitir el archivo. También incluye saltos de línea para que el comando sea más legible.

```
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
```

Notas

- `Runtime`: la versión de Java Script. Para utilizar pares clave-valor en la función, debe especificar la versión 2.0.
- `KeyValueStoreAssociations`: si la función usa pares clave-valor, puede asociar el almacén de clave-valor en la creación inicial de la función. O bien, puede asociarlo más adelante, utilizando `update-function`. La `Quantity` siempre es 1, porque cada función solo puede tener asociado un almacén de clave-valor.

Si el comando se ejecuta correctamente, verá un resultado parecido al siguiente.

```
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 mayor parte de la información se repite desde la solicitud. CloudFront agrega el resto de información.

> **Notas**
>
> - `ETag`: este valor cambia cada vez que se modifica el almacén de clave-valor. Utilice este valor y el nombre de la función para hacer referencia a la función en el futuro. Asegúrese de utilizar siempre la `ETag` actual.
> - `FunctionARN`: el ARN de la función CloudFront.
> - 111122223333: la Cuenta de AWS.
> - `Stage`: la fase de la función (`LIVE` o `DEVELOPMENT`).
> - `Status`: el estado de la función (`PUBLISHED` o `UNPUBLISHED`).

Después de crear la función, se agrega a la fase `DEVELOPMENT`. Le recomendamos que pruebe la función antes de publicarla. Tras publicar la función, la función cambia a la fase `LIVE`.

Prueba de funciones

Antes de implementar función en la etapa activa (producción), puede probarla para verificar que funciona según lo previsto. Para probar una función, especifica un objeto de evento que representa una solicitud o respuesta HTTP que su distribución de CloudFront podría recibir en producción.

CloudFront Functions realiza lo siguiente:

1. Ejecuta la función con el objeto de evento proporcionado como entrada.
2. Devuelve el resultado de la función (el objeto de evento modificado) junto con los registros de función o mensajes de error y la utilización de cómputode la función. Para obtener más información acerca del uso de cómputo, consulte the section called “Descripción del uso de cómputo”.

> **Note**
>
> Al probar una función, CloudFront solo la valida en función de los errores de ejecución de la función. CloudFront no valida si la solicitud se tramitará correctamente una vez publicada. Por ejemplo, si su función elimina un encabezado obligatorio, la prueba se

realizará correctamente porque no hay ningún problema con el código. Sin embargo, si publica la función y la asocia a una distribución, la función fallará cuando se realice una solicitud a través de CloudFront.

Contenido

- Configuración del objeto del evento
- Prueba de la función
- Descripción del uso de cómputo

Configuración del objeto del evento

Antes de probar una función, debe configurar el objeto de evento con el cual la probará. Hay varias opciones para hacerlo.

Opción 1: Configurar un objeto de evento sin guardarlo

Puede configurar un objeto de evento en el editor visual de la consola de CloudFront y no guardarlo.

Puede usar este objeto de evento para probar la función desde la consola de CloudFront, aunque no esté guardado.

Opción 2: Crear un objeto de evento en el editor visual

Puede configurar un objeto de evento en el editor visual de la consola de CloudFront y no guardarlo. Puede crear 10 objetos de eventos para cada función para, por ejemplo, probar diferentes entradas posibles.

Al crear el objeto de evento de esta manera, puede usarlo para probar la función en la consola de CloudFront. No puede usarlo para probar la función mediante una API o un SDK de AWS.

Opción 3: Crear un objeto de evento mediante un editor de texto

Puede usar un editor de texto para crear un objeto de evento a mano en formato JSON. Para obtener información sobre la estructura de un objeto de evento, consulte Estructura de evento.

Puede usar este objeto de evento para probar la función mediante la CLI. Sin embargo, no se puede utilizar para probar la función en la consola de CloudFront.

Para crear un objeto de evento (opción 1 o 2)

1. Inicie sesión en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions y elija la página Funciones.

   Elija la función que desea probar.
2. En la página de detalles de la función, seleccione la pestaña Probar.
3. En Tipo de evento, elija una de las siguientes opciones:
   - Elija Solicitud del lector si la función modifica una solicitud HTTP o genera una respuesta basada en la solicitud. Aparece la sección Solicitud.
   - O bien, seleccione Respuesta del lector. Aparecen las secciones Solicitud y Respuesta.
4. Complete los campos que desee incluir en el evento. Puede elegir Editar JSON para ver el JSON sin procesar.
5. (Opcional) Para guardar el evento, elija Guardar y, en Save test event, introduzca un nombre y, a continuación, seleccione Guardar.

   También puede elegir Editar JSON, copiar el JSON sin procesar y guardarlo en su propio archivo, fuera de CloudFront.

Para crear un objeto de evento (opción 3)

Cree el objeto de evento mediante un editor de texto. Guarde el archivo en un directorio al que se pueda conectar su equipo.

Asegúrese de seguir estas directrices:

- Omita los campos `distributionDomainName`, `distributionId` y `requestId`.
- Los nombres de encabezados, cookies y cadenas de consulta deben estar en minúsculas.

Una opción para crear un objeto de evento de esta manera es crear una muestra mediante el editor visual. Puede estar seguro de que la muestra tiene el formato correcto. A continuación, puede copiar el JSON sin procesar, pegarlo en un editor de texto y guardar el archivo.

Para obtener más información sobre la estructura de un evento, consulte Estructura de evento.

Prueba de la función

Puede probar una función en la consola de CloudFront o con la AWS Command Line Interface (AWS CLI).

Console

Para probar la función

1. Inicie sesión en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions y elija la página Funciones.
2. Elija la función que desea probar.
3. Elija la pestaña Prueba.
4. Asegúrese de que se muestre el evento correcto. Si desea cambiar desde el evento que se muestra actualmente, elija otro evento en el campo Seleccionar evento de prueba.
5. Seleccione Probar función. La consola muestra el resultado de la función, incluidos los registros de funciones y el uso del cómputo.

CLI

Puede probar una función mediante el comando aws cloudfront test-function.

Para probar la función

1. Abra una ventana de línea de comandos.
2. Ejecute el siguiente comando desde el directorio que contiene el archivo especificado.

   En este ejemplo, se utiliza la notación `fileb://` para transmitir el archivo del objeto de evento. También incluye saltos de línea para que el comando sea más legible.

```
aws cloudfront test-function \
    --name MaxAge \
    --if-match ETVABCEXAMPLE \
    --event-object fileb://event-maxage-test01.json \
    --stage DEVELOPMENT
```

> **Notas**
>
> - Se hace referencia a la función por su nombre y por la ETag (en el parámetro `if-match`). Se hace referencia al objeto de evento por su ubicación en el sistema de archivos.
> - El estado puede ser `DEVELOPMENT` o `LIVE`.

Si el comando se ejecuta correctamente, verá un resultado parecido al siguiente.

```
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
```

> **Notas**
>
> - `FunctionExecutionLogs` contiene una lista de líneas de registro que la función escribió en instrucciones `console.log()` (si las hay).

- `ComputeUtilization` contiene información sobre la ejecución de la función. Consulte the section called “Descripción del uso de cómputo”.
- `FunctionOutput` contiene el objeto de evento que devolvió la función.

Descripción del uso de cómputo

Utilización de cómputo es la cantidad de tiempo que la función tardó en ejecutarse como un porcentaje del tiempo máximo permitido. Por ejemplo, un valor de 35 significa que la función se completó en el 35 % del tiempo máximo permitido.

Si una función supera continuamente el tiempo máximo permitido, CloudFront la limita. En la siguiente lista se explica la probabilidad de que una función se limite en función del valor de utilización de cómputo.

Valor de utilización de cómputo

- 1 — 50: la función está cómodamente por debajo del tiempo máximo permitido y debe ejecutarse sin limitación.
- 51 — 70: la función se acerca al tiempo máximo permitido. Considere optimizar el código de la función.
- 71 — 100: la función está muy cerca o supera el tiempo máximo permitido. Es probable que CloudFront limite esta función si la asocia a una distribución.

Actualización de funciones

Puede actualizar una función en cualquier momento. Los cambios se realizan únicamente en la versión de la función que se encuentra en la etapa `DEVELOPMENT`. Para copiar los cambios de la etapa `DEVELOPMENT` a `LIVE`, debe publicar la función.

Puede actualizar el código de una función en la consola de CloudFront o con la AWS Command Line Interface (AWS CLI).

Console

Actualización del código de la función

1. Inicie sesión en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions y elija la página Funciones.

Elija la función que desea actualizar.

2. Elija Editar y realice los siguientes cambios:

   - Actualice todos los campos de la sección Detalles.

   - Cambie o elimine el almacén de clave-valor asociado. Para obtener más información sobre los almacenes de clave-valor, consulte the section called “ CloudFront KeyValueStore”.

   - Cambie el código de la función. Seleccione la pestaña Compilación, realice los cambios y, a continuación, seleccione Guardar cambios para guardar los cambios en el código.

CLI

Para actualizar el código de la función

1. Abra una ventana de línea de comandos.
2. Ejecute el siguiente comando.

   En este ejemplo, se utiliza la notación `fileb://` para transmitir el archivo. También incluye saltos de línea para que el comando sea más legible.

```
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
```

> **Notas**
>
> - Puede identificar la función por su nombre y ETag (en el parámetro `if-match`). Asegúrese de utilizar siempre la ETag actual. Puede obtener este valor de la operación de la API DescribeFunction.
> - Debe incluir el `function-code`, incluso aunque no desee cambiarlo.

- Tenga cuidado con la `function-config`. Debe transmitir todo lo que quiera conservar en la configuración. En concreto, gestione el almacén de clave-valor de la siguiente manera:
  - Para retener la asociación de almacenes de clave-valor existentes (si existen), especifique el nombre del almacén existente.
  - Para cambiar la asociación, especifique el nombre del nuevo almacén de clave-valor.
  - Para eliminar la asociación, omita el parámetro `KeyValueStoreAssociations`.

Si el comando se ejecuta correctamente, verá un resultado parecido al siguiente.

```
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 mayor parte de la información se repite desde la solicitud. CloudFront agrega el resto de información.

Notas

- `ETag`: este valor cambia cada vez que se modifica el almacén de clave-valor.
- `FunctionARN`: el ARN de la función CloudFront.

- `Stage`: la fase de la función (`LIVE` o `DEVELOPMENT`).
- `Status`: el estado de la función (`PUBLISHED` o `UNPUBLISHED`).

Publicación de funciones

Al publicar la función, se copia la función de la fase `DEVELOPMENT` a la fase `LIVE`.

Si no hay ningún comportamiento de la caché asociado a la función, publicarla permite asociarla a un comportamiento de la caché. Solo se pueden asociar comportamientos de la caché a funciones que se encuentran en la etapa `LIVE`.

> **Important**
>
> - Antes de la publicación, le recomendamos que pruebe la función.
> - Después de publicar la función, todos los comportamientos de la caché asociados a la función comienzan automáticamente a usar la copia recién publicada, tan pronto como las distribuciones terminen de implementarse.

Puede publicar una función en la consola de CloudFront o con la AWS CLI.

Console

Publicación de una función

1. Inicie sesión en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions y elija la página Funciones.
2. Elija la función que desea actualizar.
3. Elija la pestaña Publicar y, a continuación, elija Publicar. Si la función ya está asociada a uno o varios comportamientos de la caché, elija Publish and update.
4. (Opcional) Para ver las distribuciones asociadas a la función, seleccione Associated CloudFront distributions (Distribuciones de CloudFront asociadas) a fin de expandir esa sección.

Cuando se guarda correctamente, aparece un banner en la parte superior de la página que dice ***Function name*** published successfully. También puede seleccionar la pestaña Compilación y, a continuación, Activa para ver la versión activa del código de función.

CLI

Publicación de una función

1. Abra una ventana de línea de comandos.
2. Ejecute el siguiente comando de la aws cloudfront publish-function. En el ejemplo, se proporcionan saltos de línea para que el ejemplo sea más legible.

```
aws cloudfront publish-function \
    --name MaxAge \
    --if-match ETVXYZEXAMPLE
```

Si el comando se ejecuta correctamente, verá un resultado parecido al siguiente.

```
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
```

Asociación de funciones con distribuciones

Para utilizar una función con una distribución, asocie la función a uno o varios comportamientos de caché en la distribución. Puede asociar una función a varios comportamientos de la caché en varias distribuciones.

Puede asociar una función con cualquiera de los siguientes elementos:

- Un comportamiento de la caché existente
- Un nuevo comportamiento de la caché en una distribución existente

- Un nuevo comportamiento de la caché en una distribución nueva.

Cuando asocia una función a un comportamiento de la caché, debe selecciona un tipo de evento. El tipo de evento determina cuándo CloudFront ejecuta la función.

Puede elegir los siguientes tipos de evento:

- Solicitud del lector: la función se ejecuta cuando CloudFront recibe una solicitud de un lector.
- Viewer Response (Respuesta al lector): la función se ejecuta antes de que CloudFront devuelva una respuesta al lector.

No se pueden utilizar tipos de eventos orientados al origen (solicitud de origen y respuesta de origen) con CloudFront Functions. En su lugar, puede utilizar Lambda@Edge. Para obtener más información, consulte Eventos de CloudFront que pueden desencadenar una función de Lambda@Edge.

> **Note**
>
> Antes de asociar una función, debe publicarla en la etapa `LIVE`.

Puede asociar una función a una distribución en la consola de CloudFront o con la AWS Command Line Interface (AWS CLI). En el siguiente procedimiento, se muestra cómo asociar una función a un comportamiento existente de la caché.

Console

Asociación de una función a un comportamiento existente de la caché

1. Inicie sesión en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions y elija la página Funciones.
2. Elija la función que desee asociar.
3. En la página Función, seleccione la pestaña Publicar.
4. Elija la función Publicar.
5. Elija Add association. En el cuadro de diálogo que aparece, elija una distribución, un tipo de evento o un comportamiento de caché.

   Para el tipo de evento, seleccione cuándo desea que se ejecute esta función:

- Solicitud del lector: ejecute la función cada vez que CloudFront reciba una solicitud.
- Respuesta al lector: ejecute la función cada vez que CloudFront devuelve una respuesta.

6. Para guardar la configuración, elija Agregar asociación.

CloudFront asocia la distribución a la función. Espere unos minutos para que la distribución asociada termine de implementarse. Puede seleccionar Ver distribución en la página de detalles de la función para comprobar el progreso.

CLI

Asociación de una función a un comportamiento existente de la caché

1. Abra una ventana de línea de comandos.
2. Introduzca el siguiente comando para guardar la configuración de la distribución cuyo comportamiento de la caché desea asociar a una función. Este comando guarda la configuración de distribución en un archivo llamado `dist-config.yaml`. Para utilizar este comando, haga lo siguiente:

   - Reemplace *`DistributionID`* por el ID de la distribución.
   - Ejecute el comando en una línea. En el ejemplo, se proporcionan saltos de línea para que el ejemplo sea más legible.

```
aws cloudfront get-distribution-config \
    --id DistributionID \
    --output yaml > dist-config.yaml
```

   Si el comando se ejecuta correctamente, la AWS CLI no devuelve ninguna salida.

3. Abra el archivo llamado `dist-config.yaml` que ha creado. Edite el archivo para realizar los siguientes cambios.

   a. Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

   b. En el comportamiento de la caché, busque el objeto llamado `FunctionAssociations`. Actualice este objeto para agregar una asociación de función. La sintaxis YAML para una asociación de función se parece al siguiente ejemplo.

- En el siguiente ejemplo, se muestra un tipo de evento de solicitud del lector (disparador). Para utilizar un tipo de evento de respuesta al lector, reemplace `viewer-request` por `viewer-response`.
- Reemplace *`arn:aws:cloudfront::111122223333:function/ExampleFunction`* por el nombre de recurso de Amazon (ARN) de la función que está asociando a este comportamiento de la caché. Para obtener el ARN de la función, puede usar el comando aws cloudfront list-functions.

```
FunctionAssociations:
  Items:
    - EventType: viewer-request
      FunctionARN: arn:aws:cloudfront::111122223333:function/ExampleFunction
  Quantity: 1
```

c. Después de realizar estos cambios, guarde el archivo.

4. Utilice el siguiente comando para actualizar la distribución y agregue la asociación de función. Para utilizar este comando, haga lo siguiente:

   - Reemplace *`DistributionID`* por el ID de la distribución.
   - Ejecute el comando en una línea. En el ejemplo, se proporcionan saltos de línea para que el ejemplo sea más legible.

```
aws cloudfront update-distribution \
    --id DistributionID \
    --cli-input-yaml file://dist-config.yaml
```

Cuando el comando se realiza correctamente verá una salida como la siguiente, que describe la distribución que se acaba de actualizar con la asociación de función. La siguiente salida de ejemplo se trunca para que sea más legible.

```
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
```

El `Status` de la distribución cambia a `InProgress` mientras la distribución se vuelve a implementar. Cuando la nueva configuración de distribución llega a una ubicación periférica de CloudFront, esa ubicación periférica comienza a utilizar la función asociada. Cuando la distribución esté completamente implementada, `Status` volverá a `Deployed`. Esto indica que la CloudFront Function asociada está activa en todas las ubicaciones periféricas de CloudFront en todo el mundo. Esto normalmente dura unos minutos.

Amazon CloudFront KeyValueStore

CloudFront KeyValueStore es un almacén de datos clave-valor seguro, global y de baja latencia que permite el acceso de lectura desde CloudFront Functions, lo que permite una lógica personalizable avanzada en las ubicaciones periféricas de CloudFront.

Con CloudFront KeyValueStore, puede actualizar el código de la función y los datos asociados a una función de forma independiente. Esta separación simplifica el código de la función y facilita la actualización de los datos sin necesidad de implementar cambios en el código.

> **Note**
>
> Para usar CloudFront KeyValueStore, la función de CloudFront debe usar el tiempo de ejecución 2.0 de JavaScript.

A continuación, se muestra el procedimiento general para usar pares clave-valor:

- Cree almacenes de clave-valor y llénelos con un conjunto de pares clave-valor. Puede agregar los almacenes de clave-valor a un bucket de Amazon S3 o introducirlos manualmente.

- Asocie los almacenes de clave-valor a la función de CloudFront.
- En el código de la función, utilice el nombre de la clave para recuperar el valor asociado a la clave o para evaluar si existe una clave. Para obtener más información sobre el uso de pares clave-valor en el código de la función y sobre los métodos auxiliares, consulte the section called “Métodos auxiliares para almacenes de clave-valor”.

Casos de uso

Puede utilizar pares clave-valor para los siguientes ejemplos:

- Reescrituras o redirecciones de URL: el par clave-valor puede contener las URL reescritas o las URL redirigidas.
- Pruebas A/B y marcadores de características: puede crear una función para realizar experimentos asignando un porcentaje del tráfico a una versión específica del sitio web.
- Autorización de acceso: puede implementar el control de acceso para permitir o denegar las solicitudes en función de los criterios que haya definido y de los datos almacenados en un almacén de clave-valor.

Formatos de valores compatibles

Puede almacenar el valor en un par clave-valor en cualquiera de los siguientes formatos:

- Cadena
- Cadena codificada en bytes
- JSON

Seguridad

La función de CloudFront y todos los datos de los almacenes de clave-valor se gestionan de forma segura, de la siguiente manera:

- CloudFront cifra cada almacén de clave-valor en reposo y durante el tránsito (al leer o escribir en los almacenes de clave-valor) cuando llame a las operaciones de la API CloudFront KeyValueStore.
- Cuando se ejecuta la función, CloudFront descifra cada par clave-valor de la memoria en las ubicaciones periféricas de CloudFront.

Para comenzar a utilizar CloudFront KeyValueStore, consulte los siguientes temas.

Temas

- Trabajo con un almacén de clave-valor
- Trabajo con datos de clave-valor

- Para obtener más información sobre la introducción a CloudFront KeyValueStore, consulte la entrada de blog de AWS Introducing Amazon CloudFront KeyValueStore.

Trabajo con un almacén de clave-valor

Debe crear un almacén de clave-valor para almacenar los pares clave-valor que desee utilizar en CloudFront Functions.

Una vez que cree los almacenes de clave-valor y los pares clave-valor agregados, puede usar las claves-valores en el código de la función de CloudFront.

Para comenzar, consulte los siguientes temas:

Temas

- Creación de un almacén de clave-valor
- Asociación de un almacén de clave-valor a una función
- Actualización de un almacén de clave-valor
- Obtención de una referencia a un almacén de clave-valor
- Eliminación de un almacén de clave-valor
- Formato de archivo para pares clave-valor

> **Note**
>
> El tiempo de ejecución 2.0 de JavaScript incluye algunos métodos auxiliares para trabajar con claves-valor en el código de la función. Para obtener más información, consulte the section called “Métodos auxiliares para almacenes de clave-valor”.

Creación de un almacén de clave-valor

Puede crear un almacén de clave-valor y los pares clave-valor al mismo tiempo. Puede crear también un almacén de clave-valor vacío ahora y luego agregar pares clave-valor.

> **Note**
>
> Si especifica el origen de datos de un bucket de Amazon S3, debe tener los permisos `s3:GetObject` y `s3:GetBucketLocation` de ese bucket. Si no tiene estos permisos, CloudFront no podrá crear correctamente el almacén de clave-valor.

Decida si quiere agregar pares clave-valor al mismo tiempo cuando crea el almacén de clave-valor. Puede importar los pares clave-valor mediante la consola de CloudFront, la API de CloudFront o los AWS SDK. Sin embargo, solo puede importar el archivo de pares clave-valor cuando inicialmente crea el almacén de clave-valor.

Para crear un archivo de pares clave-valor, consulte Formato de archivo para pares clave-valor.

Console

Creación de un almacén de clave-valor

1. Inicie sesión en Consola de administración de AWS y abra la página Funciones en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Elija la pestaña KeyValueStores y, a continuación, elija Crear KeyValueStore.
3. Introduzca un nombre y una descripción opcional para el almacén de clave-valor.
4. Complete URI de S3:
   - Si tiene un archivo de pares clave-valor, ingrese la ruta al bucket de Amazon S3 donde ha almacenado el archivo.
   - Deje este campo en blanco si piensa ingresar los pares clave-valor manualmente.
5. Seleccione Crear. El almacén de clave-valor ya existe.

   Aparece la página de detalles del nuevo almacén de clave-valor. La información de la página incluye el ID y el ARN del almacén de clave-valor.

   - El ID es una cadena aleatoria de caracteres que es única en la Cuenta de AWS.
   - El ARN tiene la siguiente sintaxis:

     ```
     Cuenta de AWS:key-value-store/el ID del almacén de clave-valor
     ```

6. Consulte la sección de Pares clave-valor. Si ha importado un archivo, en esta sección se muestran algunos pares clave-valor. Puede hacer lo siguiente:
   - Si ha importado un archivo, también puede agregar más valores manualmente.
   - Si no ha importado un archivo desde un bucket de Amazon S3 y desea agregar pares clave-valor ahora, puede completar el siguiente paso.
   - Puede omitir este paso y agregar los pares clave-valor más adelante.
7. Para agregar los pares ahora:
   a. Elija Agregar pares clave-valor.
   b. Seleccione Agregar par e introduzca un nombre y un valor. Repita este paso para agregar más pares.
   c. Cuando haya terminado, elija Guardar cambios para guardar todos los pares clave-valor del almacén de clave-valor. En el cuadro de diálogo que aparece, elija Listo.
8. Para asociar ahora el almacén de clave-valor a una función, complete la sección Funciones asociadas. Para obtener más información, consulte ??? o ???.

   También puede asociar la función más adelante, ya sea desde esta página de detalles del almacén de clave-valor o desde la página de detalles de la función.

AWS CLI

Creación de un almacén de clave-valor

- Ejecute el siguiente comando para crear un almacén clave-valor e importar los pares clave-valor de un bucket de Amazon S3.

```
aws cloudfront create-key-value-store \
    --name=keyvaluestore1 \
    --comment="This is my key value store file" \
    --import-source=SourceType=S3,SourceARN=arn:aws:s3:::amzn-s3-demo-
bucket1/kvs-input.json
```

Respuesta

```
{
    "ETag": "ETVABCEXAMPLE",
```

```
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/key-value-store/
arn:aws:cloudfront::123456789012:key-value-store/8aa76c93-3198-462c-aaf6-
example",
    "KeyValueStore": {
        "Name": "keyvaluestore1",
        "Id": "8aa76c93-3198-462c-aaf6-example",
        "Comment": "This is my key value store file",
        "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
        "Status": "PROVISIONING",
        "LastModifiedTime": "2024-08-06T22:19:10.813000+00:00"
    }
}
```

API

Creación de un almacén de clave-valor

1. Utilice la operación CreateKeyValueStore de CloudFront. La operación requiere varios parámetros:
   - Un `name` del almacén de clave-valor.
   - Un parámetro `comment` que incluye un comentario.
   - Un parámetro `import-source` que permite importar pares clave-valor desde un archivo almacenado en un bucket de Amazon S3. Solo podrá importar desde un archivo cuando cree por primera vez el almacén clave-valor. Para obtener información sobre la estructura de archivos, consulte the section called “Formato de archivo para pares clave-valor”.

La respuesta de la operación incluye la siguiente información:

- Los valores transferidos en la solicitud, incluido el nombre que asignó.
- Datos como la hora de creación.
- Una `ETag` (por ejemplo, `ETVABCEXAMPLE`), el ARN que incluye el nombre del almacén de clave-valor (por ejemplo, `arn:aws:cloudfront::123456789012:key-value-store/keyvaluestore1`).

  Utilizará alguna combinación de la `ETag`, el ARN y el nombre para trabajar con el almacén de clave-valor mediante programación.

Estados del almacén de clave-valor

Al crear un almacén de clave-valor, el almacén de datos puede tener los siguientes valores de estado.

Valor	Descripción
Aprovisionando	Se ha creado el almacén de clave-valor y CloudFront está procesando el origen de datos que usted ha especificado.
Ready	Se ha creado el almacén de clave-valor y CloudFront ha procesado correctamente el origen de datos que usted ha especificado.
Error al importar	CloudFront no ha podido procesar el origen de datos que usted ha especificado. Este estado puede aparecer si el formato de archivo no es válido o si supera el límite de tamaño. Para obtener más información, consulte Formato de archivo para pares clave-valor.

Asociación de un almacén de clave-valor a una función

Después de crear el almacén de clave-valor, puede actualizar la función para asociarla al almacén de clave-valor. Debe realizar esta asociación para utilizar los pares clave-valor de ese almacén en esa función. Se aplican las siguientes reglas:

- Una función solo puede tener un almacén de clave-valor
- Puede asociar el mismo almacén de clave-valor a varias funciones

Console

Asociación de un almacén de clave-valor a una función

1. Inicie sesión en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions y elija la página Funciones.
2. Elija el nombre de la función.
3. Vaya a la sección Asociar KeyValueStore y elija Asociar KeyValueStore existente.
4. Seleccione el almacén de clave-valor que contiene los pares clave-valor de la función y, a continuación, elija Asociar KeyValueStore.

CloudFront asocia inmediatamente el almacén a la función. No necesita guardar la función.

5. Para especificar un almacén de clave-valor diferente, elija Actualizar KeyValueStore asociado, seleccione otro nombre de almacén de clave-valor y, a continuación, elija Asociar KeyValueStore.

Para obtener más información, consulte the section called “Actualización de funciones”.

AWS CLI

Asociación de un almacén de clave-valor a una función

- Ejecute el siguiente comando para actualizar la función *MaxAge* y asociar un recurso de almacén de clave-valor.

```
aws cloudfront update-function \
    --name MaxAge \
    --function-config '{"Comment":"Max Age 2 years","Runtime":"cloudfront-
js-2.0","KeyValueStoreAssociations":{"Quantity":1,"Items":
[{"KeyValueStoreARN":"arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example"}]}}' \
    --function-code fileb://function-max-age-v1.js \
    --if-match ETVABCEXAMPLE
```

- Para asociar un almacén de clave-valor a una función, especifique el parámetro `KeyValueStoreAssociations` y el ARN del almacén de clave-valor.
- Para cambiar la asociación, especifique otro ARN de almacén de clave-valor.
- Para eliminar la asociación, quite el parámetro `KeyValueStoreAssociations`.

Para obtener más información, consulte the section called “Actualización de funciones”.

API

Asociación de un almacén de clave-valor a una función

- Utilice la operación de la API UpdateFunction. Para obtener más información, consulte the section called “Actualización de funciones”.

Notas

- Si modifica un almacén de clave-valor sin cambiar los pares clave-valor o si solo modifica los pares clave-valor sin cambiar el almacén de clave-valor, no necesita volver a asociarlo. Tampoco necesita volver a publicar la función.

  Sin embargo, le recomendamos que pruebe la función para comprobar que funciona según lo previsto. Para obtener más información, consulte Prueba de funciones.
- Puede ver todas las funciones que utilizan determinados almacenes de clave-valor. En la consola de CloudFront, elija la página de detalles del almacén de clave-valor.

Actualización de un almacén de clave-valor

Al actualizar un almacén de clave-valor, puede cambiar los pares clave-valor o cambiar la asociación entre el almacén de clave-valor y la función.

Console

Actualización de un almacén de clave-valor

1. Inicie sesión en Consola de administración de AWS y abra la página Funciones en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Elija la pestaña KeyValueStores.
3. Seleccione el almacén de clave-valor que desee actualizar.
   - Para actualizar los pares clave-valor, elija Editar en la sección Pares clave-valor. Puede agregar o eliminar cualquier par clave-valor. También puede cambiar el valor de un par clave-valor existente. Cuando haya finalizado, elija Save changes (Guardar cambios).
   - Para actualizar la asociación de este almacén de clave-valor, elija Ir a las funciones. Para obtener más información, consulte the section called “Asociación de un almacén de clave-valor a una función”.

AWS CLI

Actualización de un almacén de clave-valor

1. Cambiar los pares clave-valor: puede agregar más pares clave-valor, eliminar uno o varios pares clave-valor y cambiar el valor de un par clave-valor existente. Para obtener más información, consulte Trabajo con datos de clave-valor.
2. Cambiar la asociación de funciones para el almacén de clave-valor: para actualizar la asociación de funciones para el almacén de clave-valor, consulte Asociación de un almacén de clave-valor a una función.

> **Tip**
>
> Necesitará el ARN del almacén de clave-valor. Para obtener más información, consulte the section called “Obtención de una referencia a un almacén de clave-valor”.

API

Actualización de un almacén de clave-valor

1. Cambiar los pares clave-valor: puede agregar más pares clave-valor, eliminar uno o varios pares clave-valor y cambiar el valor de un par clave-valor existente. Para obtener más información, consulte Trabajo con datos de clave-valor.
2. Cambiar la asociación de funciones para el almacén de clave-valor: para actualizar la asociación de funciones para el almacén de clave-valor, utilice la operación de la API UpdateFunction. Para obtener más información, consulte the section called “Actualización de funciones”.

> **Tip**
>
> Necesitará el ARN del almacén de clave-valor. Para obtener más información, consulte the section called “Obtención de una referencia a un almacén de clave-valor”.

Obtención de una referencia a un almacén de clave-valor

Para trabajar con los almacenes de clave-valor mediante programación, necesita la `ETag` y el nombre del almacén de clave-valor.

Para obtener ambos valores, puede usar la AWS Command Line Interface (AWS CLI) o la API de CloudFront.

AWS CLI

Obtención de la referencia del almacén de clave-valor

1. Para obtener una lista de almacenes de clave-valor, ejecute el siguiente comando. Busque el nombre del almacén de clave-valor que desea modificar.

```
aws cloudfront list-key-value-stores
```

2. A partir de la respuesta, busque el nombre del almacén de clave-valor que desee.

   Respuesta

```
{
    "KeyValueStoreList": {
        "Items": [
            {
                "Name": "keyvaluestore3",
                "Id": "37435e19-c205-4271-9e5c-example3",
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/37435e19-c205-4271-9e5c-example3",
                "Status": "READY",
                "LastModifiedTime": "2024-05-08T14:50:18.876000+00:00"
            },
            {
                "Name": "keyvaluestore2",
                "Id": "47970d59-6408-474d-b850-example2",
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/47970d59-6408-474d-b850-example2",
                "Status": "READY",
                "LastModifiedTime": "2024-05-30T21:06:22.113000+00:00"
            },
            {
                "Name": "keyvaluestore1",
                "Id": "8aa76c93-3198-462c-aaf6-example",
```

```
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
                "Status": "READY",
                "LastModifiedTime": "2024-08-06T22:19:30.510000+00:00"
            }
        ]
    }
}
```

3. Ejecute el siguiente comando para devolver la `ETag` para el almacén de clave-valor especificado.

```
aws cloudfront describe-key-value-store \
    --name=keyvaluestore1
```

Respuesta

```
{
    "ETag": "E3UN6WX5RRO2AG",
    "KeyValueStore": {
        "Name": "keyvaluestore1",
        "Id": "8aa76c93-3198-462c-aaf6-example",
        "Comment": "This is an example KVS",
        "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
        "Status": "READY",
        "LastModifiedTime": "2024-08-06T22:19:30.510000+00:00"
    }
}
```

API

Obtención de la referencia del almacén de clave-valor

1. Utilice la operación de la API CloudFront ListKeyValueStores para obtener una lista de almacenes de clave-valor. Busque el nombre del almacén de clave-valor que desee cambiar.
2. Utilice la operación de la API CloudFront DescribeKeyValueStore y especifique el nombre del almacén de clave-valor que devolvió en el paso anterior.

La respuesta incluye un UUID, el ARN del almacén de clave-valor y la `ETag` del almacén de clave-valor.

- Una `ETag`, como `E3UN6WX5RRO2AG`
- El UUID es de 128 bits, como `8aa76c93-3198-462c-aaf6-example`
- El ARN incluye el número de Cuenta de AWS, el `key-value-store` constante y el UUID, como en el siguiente ejemplo:

  ```
  arn:aws:cloudfront::123456789012:key-value-store/8aa76c93-3198-462c-aaf6-example
  ```

Para obtener más información acerca de la operación `DescribeKeyValueStore`, consulte the section called “Acerca de CloudFront KeyValueStore”.

Eliminación de un almacén de clave-valor

Puede eliminar el almacén de clave-valor mediante la consola de Amazon CloudFront o la API.

Console

Eliminación de un almacén de clave-valor

1. Inicie sesión en Consola de administración de AWS y abra la página Funciones en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Elija el nombre de la función.
3. En la sección KeyValueStore asociado, compruebe si hay un almacén de clave-valor asociado a la función. Si es así, elimine la asociación eligiendo Desasociar KeyValueStore y, a continuación, elija Eliminar asociación.
4. En el panel de navegación, elija la página Funciones y, a continuación, elija la pestaña KeyValueStores.
5. Seleccione el almacén de clave-valor que desea eliminar y, a continuación, elija Eliminar.

AWS CLI

Eliminación de un almacén de clave-valor

1. Obtenga la `ETag` y el nombre de los almacenes de clave-valor. Para obtener más información, consulte the section called “Obtención de una referencia a un almacén de clave-valor”.
2. Compruebe si los almacenes de clave-valor están asociados a una función. Si lo está, elimine la asociación. Para obtener más información sobre los dos pasos, consulte ???.
3. Cuando tenga el nombre y la `ETag` del almacén de clave-valor y ya no esté asociado a una función, podrá eliminarlo.

   Ejecute el siguiente comando para eliminar el almacén de clave-valor especificado.

```
aws cloudfront delete-key-value-store \
    --name=keyvaluestore1 \
    --if-match=E3UN6WX5RRO2AG
```

API

Eliminación de un almacén de clave-valor

1. Obtenga la `ETag` y el nombre de los almacenes de clave-valor. Para obtener más información, consulte the section called “Obtención de una referencia a un almacén de clave-valor”.
2. Compruebe si los almacenes de clave-valor están asociados a una función. Si lo está, elimine la asociación. Para obtener más información sobre los dos pasos, consulte ???.
3. Para eliminar el almacén de clave-valor, utilice la operación de la API DeleteKeyValueStore de CloudFront.

Formato de archivo para pares clave-valor

Al crear un archivo codificado con UTF-8, utilice el siguiente formato JSON:

```
{
  "data":[
    {
      "key":"key1",
```

```
      "value":"value"
    },
    {
      "key":"key2",
      "value":"value"
    }
  ]
}
```

El archivo no puede incluir claves duplicadas. Si especificó un archivo no válido en el bucket de Amazon S3, puede actualizar el archivo para eliminar cualquier duplicado y, a continuación, intentar crear de nuevo el almacén de clave-valor.

Para obtener más información, consulte Creación de un almacén de clave-valor.

> **Note**
>
> El archivo de su origen de datos y sus pares clave-valor tienen los siguientes límites:
>
> - Tamaño del archivo: 5 MB
> - Tamaño de la clave: 512 caracteres
> - Tamaño del valor: 1024 caracteres

Trabajo con datos de clave-valor

Este tema describe cómo agregar pares clave-valor a un almacén de clave-valor existente. Para incluir pares clave-valor al crear inicialmente los almacenes de clave-valor, consulte the section called “Creación de un almacén de clave-valor”.

Temas

- Uso de pares clave-valor (consola)
- Acerca de CloudFront KeyValueStore
- Uso de pares clave-valor (AWS CLI)
- Uso de pares clave-valor (API)

Uso de pares clave-valor (consola)

Puede utilizar la consola de CloudFront para trabajar con los pares clave-valor.

Trabajo con pares clave-valor

1. Inicie sesión en Consola de administración de AWS y abra la página Funciones en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Elija la pestaña KeyValueStores.
3. Seleccione el almacén de clave-valor que desee cambiar.
4. En la sección Pares clave-valor, elija Editar.
5. Puede agregar un par clave-valor, eliminar cualquier par clave-valor o cambiar el valor de un par clave-valor existente.
6. Cuando haya finalizado, elija Save changes (Guardar cambios).

Acerca de CloudFront KeyValueStore

> **Tip**
>
> La API KeyValueStore de CloudFront es un servicio global que utiliza Signature Version 4A (SigV4A) para la autenticación. Utilizar credenciales temporales con SigV4A requiere tokens de sesión de la versión 2. Para obtener más información, consulte Uso de credenciales temporales con la API KeyValueStore de CloudFront.

Si utiliza la AWS Command Line Interface (AWS CLI) o el código propio para llamar a la API KeyValueStore de CloudFront, consulte las secciones siguientes.

Cuando trabaja con un almacén de clave-valor y sus pares clave-valor, el servicio al que llame depende del caso de uso:

- Para trabajar con pares clave-valor en un almacén de clave-valor existente, utilice el servicio KeyValueStore de CloudFront.
- Para incluir pares clave-valor en el almacén de clave-valor al crear inicialmente el almacén de clave-valor, utilice el servicio de CloudFront.

Tanto la API de CloudFront como la API de CloudFront KeyValueStore tienen una operación `DescribeKeyValueStore`. Las llama por diferentes motivos. Para entender las diferencias, consulte la siguiente tabla.

	API de CloudFront DescribeKeyValueStore	API de CloudFront KeyValueStore DescribeKeyValueStore
Datos sobre el almacén de clave-valor	Devuelve datos, como el estado y la fecha en que se modificó por última vez el propio almacén de clave-valor.	Devuelve datos sobre el contenido del recurso de almacenamiento: los pares clave-valor del almacén y el tamaño del contenido.
Datos que identifican el almacén de clave-valor	Devuelve una `ETag`, el UUID y el ARN del almacén de clave-valor.	Devuelve una `ETag` y el ARN del almacén de clave-valor.

Notas

- Cada operación DescribeKeyValueStore devuelve una `ETag` diferente. Las `ETags` no son intercambiables.
- Al llamar a una operación de la API para completar una acción, debe especificar la `ETag` de la API correspondiente. Por ejemplo, en la operación DeleteKey de KeyValueStore de CloudFront, especifique la `ETag` que devolvió de la operación DescribeKeyValueStore de KeyValueStore de CloudFront.
- Cuando invoca CloudFront Functions mediante CloudFront KeyValueStore, los valores del almacén de valores clave no se actualizan ni cambian durante la invocación de la función. Las actualizaciones se procesan entre las invocaciones de una función.

Uso de pares clave-valor (AWS CLI)

Puede ejecutar los siguientes comandos de la AWS Command Line Interface para KeyValueStore de CloudFront.

Contenido

- Enumeración de pares clave-valor

- Obtención de pares clave-valor
- Descripción de un almacén de clave-valor
- Creación de un par clave-valor
- Eliminación de un par clave-valor
- Actualización de pares clave-valor

Enumeración de pares clave-valor

Para enumerar los pares clave-valor del almacén de clave-valor, ejecute el siguiente comando.

```
aws cloudfront-keyvaluestore list-keys \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Respuesta

```
{
    "Items": [
        {
            "Key": "key1",
            "Value": "value1"
        }
    ]
}
```

Obtención de pares clave-valor

Para obtener un par clave-valor del almacén de clave-valor, ejecute el siguiente comando.

```
aws cloudfront-keyvaluestore get-key \
    --key=key1 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Respuesta

```
{
    "Key": "key1",
    "Value": "value1",
```

```
    "ItemCount": 1,
    "TotalSizeInBytes": 11
}
```

Descripción de un almacén de clave-valor

Para describir un almacén de clave-valor, ejecute el siguiente comando.

```
aws cloudfront-keyvaluestore describe-key-value-store \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Respuesta

```
{
    "ETag": "KV1F83G8C2ARO7P",
    "ItemCount": 1,
    "TotalSizeInBytes": 11,
    "KvsARN": "arn:aws:cloudfront::123456789012:key-value-store/37435e19-
c205-4271-9e5c-example",
    "Created": "2024-05-08T07:48:45.381000-07:00",
    "LastModified": "2024-08-05T13:50:58.843000-07:00",
    "Status": "READY"
}
```

Creación de un par clave-valor

Para crear un par clave-valor en el almacén de clave-valor, ejecute el siguiente comando.

```
aws cloudfront-keyvaluestore put-key \
    --if-match=KV1PA6795UKMFR9 \
    --key=key2 \
    --value=value2 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Respuesta

```
{
    "ETag": "KV13V1IB3VIYZZH",
    "ItemCount": 3,
```

```
    "TotalSizeInBytes": 31
}
```

Eliminación de un par clave-valor

Para eliminar un par clave-valor, ejecute el siguiente comando.

```
aws cloudfront-keyvaluestore delete-key \
    --if-match=KV13V1IB3VIYZZH \
    --key=key1 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Salida

```
{
    "ETag": "KV1VC38T7YXB528",
    "ItemCount": 2,
    "TotalSizeInBytes": 22
}
```

Actualización de pares clave-valor

Puede utilizar el comando `update-keys` para actualizar más de un par clave-valor. Por ejemplo, para eliminar un par clave-valor existente y crear otro, ejecute el siguiente comando.

```
aws cloudfront-keyvaluestore update-keys \
    --if-match=KV2EUQ1WTGCTBG2 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example \
    --deletes '[{"Key":"key2"}]' \
    --puts '[{"Key":"key3","Value":"value3"}]'
```

Respuesta

```
{
    "ETag": "KV3AEGXETSR30VB",
    "ItemCount": 3,
    "TotalSizeInBytes": 28
}
```

Uso de pares clave-valor (API)

Siga esta sección para trabajar con los pares clave-valor mediante programación.

Contenido

- Obtención de una referencia a un almacén de clave-valor
- Cambio de los pares clave-valor en un almacén de clave-valor
- Código de ejemplo para CloudFront KeyValueStore

Obtención de una referencia a un almacén de clave-valor

Cuando utilice la API KeyValueStore de CloudFront para llamar a una operación de escritura, debe especificar el ARN y la `ETag` del almacén de clave-valor. Para obtener estos datos, haga lo siguiente:

Obtención de una referencia a un almacén de clave-valor

1. Utilice la operación de la API CloudFront ListKeyValueStores para obtener una lista de almacenes de clave-valor. Busque el almacén de clave-valor que desee cambiar.
2. Utilice la operación de la API CloudFrontKeyValueStore DescribeKeyValueStore y especifique el almacén de clave-valor del paso anterior.

   La respuesta incluye el ARN y la `ETag` del almacén de clave-valor.

   - El ARN incluye el número de Cuenta de AWS, el `key-value-store` constante y el UUID, como en el siguiente ejemplo:

     ```
     arn:aws:cloudfront::123456789012:key-value-store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
     ```

   - Una `ETag` como la del siguiente ejemplo:

     ```
     ETVABCEXAMPLE2
     ```

Cambio de los pares clave-valor en un almacén de clave-valor

Puede especificar el almacén de clave-valor que contiene el par clave-valor que desea actualizar.

Consulte las siguientes operaciones de la API de CloudFront KeyValueStore:

- CloudFrontKeyValueStore DeleteKey: elimina un par clave-valor
- CloudFrontKeyValueStore GetKey: devuelve un par clave-valor
- CloudFrontKeyValueStore ListKeys: devuelve una lista de pares clave-valor
- CloudFrontKeyValueStore PutKey: puede realizar las siguientes tareas:
  - Cree un par clave-valor en un almacén de clave-valor especificando un nombre y un valor de clave nuevos.
  - Establezca un valor diferente en un par clave-valor existente especificando un nombre de clave existente y un valor de clave nuevo.
- CloudFrontKeyValueStore UpdateKeys: puede realizar una o más de las siguientes acciones en una operación de todo o nada:
  - Eliminación de uno o varios pares clave-valor
  - Creación de uno o varios pares clave-valor nuevos
  - Establecimiento de un valor diferente en uno o varios pares clave-valor existentes

Código de ejemplo para CloudFront KeyValueStore

Example

En el siguiente código, se muestra cómo llamar a la operación de la API `DescribeKeyValueStore` de un almacén de clave-valor.

```
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);
  }
})();
```

Personalización con funciones de conexión de CloudFront

Las funciones de conexión de CloudFront permiten escribir funciones de JavaScript sencillas para la validación de certificados mTLS y la lógica de autenticación personalizada. Las funciones de conexión se ejecutan durante el establecimiento de la conexión de mTLS para validar los certificados de los clientes, implementar reglas de autenticación específicas del dispositivo y gestionar los escenarios de revocación de certificados. El entorno de tiempo de ejecución de funciones de conexión ofrece tiempos de arranque de submilisegundos, se escala inmediatamente para gestionar millones de solicitudes por segundo y es altamente seguro. Las funciones de conexión son características nativas de CloudFront, lo que significa que puede compilar, probar e implementar el código completamente dentro de CloudFront.

Cuando asocia una función de conexión con una distribución de CloudFront habilitada para mTLS, CloudFront intercepta solicitudes de conexión de TLS en ubicaciones periféricas de CloudFront y pasa la información de certificado a la función. Puede invocar funciones de conexión cuando se produce el siguiente evento:

- Durante el establecimiento de la conexión de TLS (solicitud de conexión): para conexiones de TLS mutuas (mTLS)

Para obtener más información sobre las funciones de conexión, consulte los siguientes temas.

Temas

- Información general y flujo de trabajo
- Configuración y límites
- Creación de funciones de conexión de CloudFront para la validación de TLS mutua (espectador)
- Escritura de código de función de conexión de CloudFront para la validación de TLS mutua (espectador)
- Prueba de las funciones de conexión de CloudFront antes de la implementación
- Asociación de funciones de conexión con distribuciones

- Implementación de la revocación de certificados para TLS mutua (espectador) con CloudFront Functions y KeyValueStore

Información general y flujo de trabajo

Las funciones de conexión de CloudFront son un tipo especializado de CloudFront Functions que se ejecutan durante el establecimiento de comunicación de TLS cuando un cliente intenta establecer una conexión de mTLS. La función de conexión puede acceder a la información de los certificados del cliente, a los parámetros de configuración de mTLS, a los resultados de las comprobaciones de revocación de certificados y a la dirección IP del cliente.

Las funciones de conexión se invocan después de que CloudFront lleve a cabo la validación estándar del certificado (cadena de confianza, caducidad, verificación de firma), pero pueden ejecutarse incluso si las comprobaciones de revocación de certificados producen un error. Esto permite implementar una lógica personalizada para gestionar los certificados revocados o agregar criterios de validación adicionales.

Cuando crea y publica una función de conexión, asegúrese de agregar una asociación para el tipo de evento solicitud de conexión con una distribución con mTLS. Esto hace que la función se ejecute cada vez que un cliente intenta establecer una conexión de mTLS con CloudFront.

Las funciones de conexión de CloudFront siguen un ciclo de vida de dos etapas que permite desarrollar y probar funciones antes de implementarlas en producción. Este flujo de trabajo garantiza que las funciones de conexión funcionen correctamente antes de que afecten al tráfico en directo.

Temas

- Etapas de la función
- Flujo de trabajo de desarrollo
- Diferencias con otros tipos de funciones

Etapas de la función

Las funciones de conexión existen en una de estas dos etapas:

- DESARROLLO: las funciones de esta etapa se pueden modificar, probar y actualizar. Utilice esta etapa para escribir y depurar el código de la función.
- ACTIVA: las funciones de esta etapa son de solo lectura y gestionan el tráfico de producción. No se pueden modificar las funciones directamente en la etapa ACTIVA.

Cuando se crea una nueva función de conexión, esta comienza en la etapa de DESARROLLO. Tras la prueba y la validación, se publica la función para pasarla a la etapa ACTIVA.

Flujo de trabajo de desarrollo

Siga este flujo de trabajo para desarrollar e implementar las funciones de conexión:

1. Crear: cree una nueva función de conexión en la etapa de DESARROLLO con el código y la configuración iniciales.
2. Probar: utilice la funcionalidad de prueba para validar la función con ejemplos de eventos de conexión antes de la implementación.
3. Actualizar: modifique el código y la configuración de la función según sea necesario en función de los resultados de las pruebas.
4. Publicar: cuando esté lista para la producción, publique la función para pasarla de la etapa de DESARROLLO a la etapa ACTIVA.
5. Asociar: asocie la función publicada a la distribución compatible con mTLS para gestionar las conexiones en directo.

Para realizar cambios en una función ACTIVA, debe actualizar la versión de DESARROLLO y volver a publicarla. Así se creará una versión nueva en la etapa ACTIVA.

Diferencias con otros tipos de funciones

Las funciones de conexión se diferencian de las funciones de solicitud y respuesta del espectador en varios aspectos importantes:

- Las funciones de conexión se ejecutan después del establecimiento de comunicación de mTLS, antes de que se produzca cualquier procesamiento HTTP.
- Las funciones de conexión tienen acceso a la información del certificado TLS en lugar de a los datos de solicitud/respuesta HTTP.
- Las funciones de conexión solo pueden permitir o denegar las conexiones, no modificar los datos HTTP.
- Las funciones de conexión solo se invocan para las nuevas conexiones TLS, no para su reutilización.
- mTLS no admite la reanudación de la sesión TLS para garantizar que la validación del certificado se realice en todas las conexiones.

- Las funciones de conexión se ejecutan de forma adicional a las funciones de solicitud del espectador y respuesta del espectador.
- Las funciones de conexión se asocian por distribución, en lugar de por comportamiento de la caché.
- Las funciones de conexión solo admiten tiempo de ejecución 2.0 de JavaScript.

Configuración y límites

Las funciones de conexión de CloudFront tienen requisitos de configuración y límites de servicio específicos debido al rol especializado en la validación de la conexión TLS y a los requisitos de rendimiento de la computación de periferia.

Temas

- Requisitos del código de función
- Límites de los servicios
- Opciones de filtrado de funciones

Requisitos del código de función

Las funciones de conexión requieren un código JavaScript que procese los eventos de conexión de TLS. El código de la función debe:

- Estar escrito en JavaScript
- Procesar los eventos de conexión y tomar decisiones de permitir/denegar
- Realizar una ejecución completa dentro de los límites de tiempo
- Gestionar la lógica de validación de certificados y conexiones

Límites de los servicios

Las funciones de conexión están sujetas a los siguientes límites:

- Tamaño de la función: el código de función y la configuración tienen un tamaño limitado
- Tiempo de ejecución: las funciones tienen límites de tiempo de ejecución estrictos para el procesamiento de la conexión TLS
- Límites de asociación: cada distribución solo puede tener asociada una función de conexión

- Restricciones de etapa: solo las funciones de la etapa ACTIVA se pueden asociar a las distribuciones

Opciones de filtrado de funciones

Cuando se muestran funciones de conexión, puede usar los siguientes filtros:

- Filtro de etapa: filtre por etapa de DESARROLLO o ACTIVA
- Filtro de asociación: filtre por ID de distribución o asociaciones de ID de almacén de clave-valor

Estos filtros lo ayudan a organizar y administrar las funciones de conexión en diferentes entornos y casos de uso.

Creación de funciones de conexión de CloudFront para la validación de TLS mutua (espectador)

Se crea una función de conexión de CloudFront en dos etapas:

1. Crear el código de función como JavaScript. Puede utilizar el ejemplo predeterminado de la consola de CloudFront o escribir el suyo propio. Para obtener más información, consulte los temas siguientes:
   - Escritura de código de la función de conexión de CloudFront para la validación de mTLS
   - Estructura de eventos y formato de respuesta de la función de conexión de CloudFront
   - Ejemplos de código de función de conexión
2. Utilice CloudFront para crear la función de conexión e incluir el código. El código existe dentro de la función (no como referencia).

Temas

- Consola de CloudFront
- AWS CLI

Consola de CloudFront

Creación de una función de conexión

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleccione Creación de función.
3. Ingrese un nombre de función que sea único en la Cuenta de AWS, elija Función de conexión como tipo de función y, a continuación, elija Continuar.
4. Aparece la página de detalles de la nueva función de conexión.

> **Note**
>
> Las funciones de conexión solo admiten tiempo de ejecución 2.0 de JavaScript. Para utilizar la integración de KeyValueStore de la función de conexión de CloudFront en la función, debe utilizar esta versión de tiempo de ejecución.

5. En la sección Código de función, elija la pestaña Compilación e ingrese el código de función de conexión. El código de ejemplo que se incluye en la pestaña Compilación ilustra la sintaxis básica del código de la función de conexión.
6. Seleccione Save changes (Guardar cambios).
7. Si el código de la función de conexión utiliza KeyValueStore para comprobar la revocación de certificados o la validación de dispositivos, debe asociar un KeyValueStore.

   Puede asociar KeyValueStore cuando crea en primer lugar la función. O bien, puede asociarlo más adelante, mediante la asociación de funciones de conexión.

   Para asociar un KeyValueStore ahora, siga estos pasos:

   - Vaya a la sección Asociar KeyValueStore y elija Asociar KeyValueStore existente.
   - Seleccione el KeyValueStore que contiene los datos del certificado para la función de conexión y, a continuación, elija Asociar KeyValueStore.

   CloudFront asocia inmediatamente el almacén a la función. No necesita guardar la función.

AWS CLI

Si utiliza la AWS CLI, normalmente crea primero el código de la función de conexión en un archivo y, a continuación, crea la función con la AWS CLI.

Creación de una función de conexión

1. Cree el código de la función de conexión en un archivo y guárdelo en un directorio al que se pueda conectar el equipo.
2. Ejecute el comando como se muestra en el ejemplo. En este ejemplo, se utiliza la notación `fileb://` para transmitir el archivo. También incluye saltos de línea para que el comando sea más legible.

```
aws cloudfront create-connection-function \
    --name CertificateValidator \
    --connection-function-config '{
        "Comment":"Device certificate validation",
        "Runtime":"cloudfront-js-2.0",
        "KeyValueStoreAssociations":{
            "Quantity":1,
            "Items":[{
                "KeyValueStoreARN":"arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }]
        }
    }' \
    --connection-function-code fileb://certificate-validator.js
```

> **Note**
>
> - Tiempo de ejecución: las funciones de conexión solo admiten el tiempo de ejecución 2.0 de JavaScript (cloudfront-js-2.0).
> - KeyValueStoreAssociations: si la función de conexión usa KeyValueStore para la validación de certificados, puede asociar KeyValueStore en la creación inicial de la función. O bien, puede asociarlo más adelante, mediante update-connection-function. La cantidad siempre es 1, porque cada función de conexión solo puede tener asociado un KeyValueStore.

3. Si el comando se ejecuta correctamente, verá un resultado parecido al siguiente.

```
ETag: ETVABCEXAMPLE
ConnectionFunctionSummary:
  ConnectionFunctionConfig:
    Comment: Device certificate validation
    Runtime: cloudfront-js-2.0
    KeyValueStoreAssociations:
      Quantity: 1
      Items:
        - KeyValueStoreARN: arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
  ConnectionFunctionMetadata:
    CreatedTime: '2024-09-04T16:32:54.292000+00:00'
    ConnectionFunctionARN: arn:aws:cloudfront::111122223333:connection-function/
CertificateValidator
    LastModifiedTime: '2024-09-04T16:32:54.292000+00:00'
    Stage: DEVELOPMENT
  Name: CertificateValidator
  Status: UNPUBLISHED
Location: https://cloudfront.amazonaws.com/2020-05-31/connection-function/
arn:aws:cloudfront:::connection-function/CertificateValidator
```

La mayor parte de la información se repite desde la solicitud. CloudFront agrega el resto de información.

> **Note**
>
> - ETag: este valor cambia cada vez que se modifica la función de conexión. Necesitará este valor para actualizar o publicar la función.
> - Etapa: las nuevas funciones de conexión comienzan en la etapa de DESARROLLO. Debe publicar la función para moverla al escenario ACTIVA antes de asociarla a una distribución.
> - Estado: el estado de la función es NO PUBLICADA hasta que la publique en la etapa ACTIVA.

Escritura de código de función de conexión de CloudFront para la validación de TLS mutua (espectador)

Las funciones de conexión de CloudFront permiten escribir funciones de JavaScript sencillas para la validación de certificados de mTLS y la lógica de autenticación personalizada. El código de la función de conexión puede validar los certificados de los clientes, implementar reglas de autenticación específicas del dispositivo, gestionar escenarios de revocación de certificados y tomar decisiones de permitir o denegar las conexiones TLS en las ubicaciones periféricas de CloudFront de todo el mundo.

Las funciones de conexión proporcionan una forma eficaz de ampliar la validación de certificados integrada en CloudFront con su propia lógica empresarial. A diferencia de las funciones de solicitud y respuesta del espectador que procesan datos HTTP, las funciones de conexión funcionan en la capa de TLS y tienen acceso a la información del certificado, a las direcciones IP del cliente y a los detalles de la conexión de TLS. Esto las hace ideales para implementar modelos de seguridad de confianza cero, sistemas de autenticación de dispositivos y políticas de validación de certificados personalizadas que van más allá de la validación estándar de PKI.

El código de la función de conexión se ejecuta en un entorno seguro y aislado con tiempos de inicio de submilisegundos y se puede escalar para gestionar millones de conexiones por segundo. El tiempo de ejecución está optimizado para las cargas de trabajo de validación de certificados y proporciona una integración integrada con CloudFront KeyValueStore para operaciones de búsqueda de datos en tiempo real, lo que permite escenarios de autenticación sofisticados, como la comprobación de la lista de revocación de certificados y la validación de la lista de dispositivos permitidos.

Como ayuda para escribir código de la función de conexión eficaz, consulte los siguientes temas. Para ver ejemplos de código completos y tutoriales paso a paso, consulte las secciones de tutoriales de esta guía y explore los ejemplos de funciones de conexión disponibles en la consola de CloudFront.

Temas

- Casos de uso y finalidades de la función de conexión de CloudFront
- Estructura de eventos y formato de respuesta de la función de conexión de CloudFront
- Características del tiempo de ejecución de JavaScript de funciones de conexión de CloudFront
- API y métodos auxiliares de la función de conexión de CloudFront
- Integración de KeyValueStore con la función de conexión de CloudFront

- Uso de async y await
- Ejemplos de código de función de conexión

Casos de uso y finalidades de la función de conexión de CloudFront

Antes de escribir la función de conexión de CloudFront, determine cuidadosamente qué tipo de lógica de autenticación o validación de certificados debe implementar. Las funciones de conexión están diseñadas para casos de uso específicos que requieren una validación personalizada más allá de la comprobación estándar de los certificados de PKI. La comprensión del caso de uso lo ayuda a diseñar un código eficiente que cumpla con los requisitos de seguridad y, al mismo tiempo, mantenga un rendimiento óptimo.

Los casos de uso comunes de la función de conexión incluyen:

- Gestión de la revocación de certificados: implemente políticas personalizadas para gestionar los certificados revocados, incluidos los periodos de gracia para la rotación de los certificados, las excepciones de redes de confianza para los dispositivos internos o los escenarios de acceso de emergencia en los que los certificados revocados podrían necesitar un acceso temporal.
- Compatibilidad con mTLS opcional: gestione las conexiones de mTLS y las que no lo son con políticas de autenticación diferentes, lo que permite ofrecer una mayor seguridad a los clientes que admiten certificados y, al mismo tiempo, mantener la compatibilidad con los clientes antiguos.
- Autenticación basada en IP: combine la validación de los certificados con las comprobaciones de las direcciones IP de los clientes para mejorar la seguridad, por ejemplo, restringiendo el acceso desde regiones geográficas específicas, redes corporativas o rangos de IP maliciosos conocidos.
- Validación de certificados multiusuario: implemente reglas de validación específicas para cada inquilino en las que se apliquen diferentes autoridades de certificación o criterios de validación en función del emisor del certificado del cliente o de los atributos del sujeto.
- Control de acceso basado en el tiempo: aplique restricciones basadas en el tiempo para que los certificados solo sean válidos durante horas, periodos de mantenimiento o periodos laborables específicos, incluso si el certificado en sí no ha caducado.

Las funciones de conexión se ejecutan después de que CloudFront lleve a cabo la validación estándar del certificado (verificación de la cadena de confianza, comprobaciones de caducidad y validación de firmas), pero antes de que se establezca la conexión de TLS. Este tiempo brinda la flexibilidad de agregar criterios de validación personalizados y, al mismo tiempo, beneficiarse de la validación de certificados integrada de CloudFront. La función recibe los resultados de la validación

estándar y puede tomar decisiones fundamentadas sobre si permitir o denegar la conexión en función de criterios estándar y personalizados.

Al diseñar la función de conexión, tenga en cuenta las implicaciones de rendimiento de la lógica de validación. Las funciones tienen un límite de ejecución de 5 milisegundos, por lo que las operaciones complejas deben optimizarse para aumentar su velocidad. Utilice KeyValueStore para realizar búsquedas rápidas de datos en lugar de realizar cálculos complejos y estructure su lógica de validación para que los certificados no válidos respondan rápido a los errores.

Estructura de eventos y formato de respuesta de la función de conexión de CloudFront

Las funciones de conexión de CloudFront reciben una estructura de eventos diferente a la de las funciones de solicitud y respuesta del espectador. En lugar de datos de solicitud/respuesta HTTP, las funciones de conexión reciben información sobre certificados y conexiones que puede utilizar para tomar decisiones de autenticación.

Temas

- Estructura de eventos para las funciones de conexión
- Formato de respuesta de funciones de conexión

Estructura de eventos para las funciones de conexión

Las funciones de conexión reciben un objeto de eventos que contiene el certificado y la información de conexión. La estructura de eventos de la función se muestra a continuación:

```
{
  "clientCertificate": {
    "certificates": {
      "leaf": {
        "serialNumber": "string",
        "issuer": "string",
        "subject": "string",
        "validity": {
          "notBefore": "string",
          "notAfter": "string",
        },
        "sha256Fingerprint": "string"
      }
    }
  },
```

```
  "clientIp": "string",
  "endpoint": "string",
  "distributionId": "string",
  "connectionId": "string"
}
```

A continuación, se muestra un ejemplo de la estructura del objeto de eventos:

```
{
  "clientCertificate": {
    "certificates": {
      "leaf": {
        "serialNumber": "00:9e:2a:af:16:56:e5:47:25:7d:2e:38:c3:f9:9d:57:fa",
        "issuer": "C=US, O=Ram, OU=Edge, ST=WA, CN=mTLS-CA, L=Snoqualmie",
        "subject": "C=US, O=Ram, OU=Edge, ST=WA, CN=mTLS-CA, L=Snoqualmie",
        "validity": {
          "notBefore": "2025-09-10T23:43:10Z",
          "notAfter": "2055-09-11T00:43:02Z"
        },
        "sha256Fingerprint": "_w6bJ7aOAlGOj7NUhJxTfsfee-ONg_xop3_PTgTJpqs="
      }
    }
  },
  "clientIp": "127.0.0.1",
  "endpoint": "d3lch071jze0cb.cloudfront.net",
  "distributionId": "E1NXS4MQZH501R",
  "connectionId": "NpvTe1925xfj24a67sPQr7ae42BIq03FGhJJKfrQYWZcWZFp96SIIg=="
}
```

Formato de respuesta de funciones de conexión

La función de conexión debe devolver un objeto de respuesta que indique si se va a permitir o denegar la conexión. Utilice los métodos auxiliares para tomar decisiones de conexión:

```
function connectionHandler(connection) {
    // Helper methods to allow or deny connections
    if (/* some logic to determine if function should allow connection */) {
        connection.allow();
    } else {
        connection.deny();
    }
}
```

A diferencia de las funciones de solicitud y respuesta del espectador, las funciones de conexión no pueden modificar las solicitudes o respuestas HTTP. Solo pueden permitir o denegar la conexión de TLS.

Características del tiempo de ejecución de JavaScript de funciones de conexión de CloudFront

Las funciones de conexión de CloudFront utilizan el tiempo de ejecución de JavaScript 2.0 de CloudFront Functions, que proporciona un entorno seguro y de alto rendimiento optimizado específicamente para las cargas de trabajo de validación de certificados. El tiempo de ejecución está diseñado para comenzar en submilisegundos y gestionar millones de ejecuciones simultáneas en la red de periferia global de CloudFront.

El entorno de tiempo de ejecución incluye una amplia compatibilidad con el lenguaje de JavaScript:

- Compatibilidad con ECMAScript 2020 (ES11): características modernas de JavaScript que incluyen el encadenamiento opcional (?.), la fusión de NULL (??), y BigInt para gestionar números de serie de certificados de gran tamaño.
- Objetos integrados: objetos de JavaScript estándar como Object, Array, JSON, Math y Date.
- Registro de consola: utilice console.log() para depurar y supervisar las decisiones de validación de certificados. Los registros están disponibles en tiempo real durante las pruebas y pueden ayudar a solucionar los problemas de la lógica de validación durante el desarrollo.
- Integración con KeyValueStore: acceso nativo a CloudFront KeyValueStore para operaciones de búsqueda de datos ultrarrápidas, lo que permite comprobar la revocación de certificados en tiempo real, validar las listas de dispositivos permitidos y recuperar la configuración específica del inquilino.

Las funciones de conexión están optimizadas para ofrecer un alto rendimiento en los escenarios de validación de certificados. El tiempo de ejecución gestiona automáticamente la administración de la memoria, la recopilación de elementos no utilizados y la limpieza de recursos para garantizar un rendimiento coherente en millones de conexiones simultáneas. Todas las operaciones están diseñadas para ser deterministas y rápidas, y las búsquedas de KeyValueStore suelen completarse en microsegundos.

El entorno de tiempo de ejecución está completamente aislado entre las ejecuciones de las funciones, lo que garantiza que no se filtren datos entre las diferentes conexiones de los clientes. La

ejecución de cada función comienza con un estado limpio y no tiene acceso a los resultados de la ejecución anterior ni a los datos del cliente desde otras conexiones.

API y métodos auxiliares de la función de conexión de CloudFront

Las funciones de conexión de CloudFront proporcionan métodos auxiliares especializados diseñados para simplificar las decisiones de validación de certificados y mejorar la observabilidad. Estos métodos están optimizados para el flujo de trabajo de validación de conexiones y se integran perfectamente con los sistemas de registro y supervisión de conexiones de CloudFront.

- connection.allow(): permita que continúe la conexión de TLS. Este método indica a CloudFront que complete el establecimiento de comunicación de TLS y permita al cliente establecer la conexión. Úselo cuando se apruebe la validación del certificado y se cumpla cualquier lógica de autenticación personalizada.
- connection.deny(): deniegue la conexión de TLS y finalice el establecimiento de comunicación. Este método cierra inmediatamente la conexión e impide que fluya el tráfico HTTP. El cliente recibirá un error de conexión de TLS. Úselo para los certificados no válidos, los errores de autenticación o las infracciones de las políticas.
- connection.logCustomData(): agregue datos personalizados a los registros de conexión (hasta 800 bytes de texto UTF-8). Este método permite incluir los resultados de la validación, los detalles del certificado o el fundamento de la decisión en los registros de conexión de CloudFront para la supervisión de la seguridad, la auditoría de conformidad y la solución de problemas.

Estos métodos proporcionan una interfaz clara y declarativa para tomar decisiones de conexión y registrar la información relevante para la supervisión y la depuración. El patrón de permitir/denegar garantiza que la intención de la función sea clara y que CloudFront pueda optimizar la gestión de la conexión en función de la decisión. Los datos de registro personalizados están disponibles inmediatamente en los registros de conexión de CloudFront y se pueden utilizar con herramientas de análisis de registros para supervisar la seguridad y obtener información operativa.

Llame siempre a connection.allow() o connection.deny() antes de que finalice la función. Si no se llama a ninguno de los dos métodos, CloudFront denegará la conexión de forma predeterminada como medida de seguridad.

Integración de KeyValueStore con la función de conexión de CloudFront

Las funciones de conexión de CloudFront pueden usar KeyValueStore de CloudFront para realizar búsquedas de datos ultrarrápidas para escenarios de validación de certificados. KeyValueStore es

especialmente eficaz para las funciones de conexión, ya que proporciona un acceso a los datos global y, en última instancia, coherente con tiempos de búsqueda de microsegundos en todas las ubicaciones periféricas de CloudFront. Esto lo hace ideal para mantener listas de revocación de certificados, listas de dispositivos permitidos, configuraciones de inquilinos y otros datos de validación a los que es necesario acceder durante los establecimientos de comunicación de TLS.

La integración de KeyValueStore está diseñada específicamente para flujos de trabajo de validación de conexiones de alto rendimiento:

- kvsHandle.exists(clave): compruebe si existe una clave en el KeyValueStore sin recuperar el valor. Este es el método más eficaz para los escenarios de validación binaria, como la comprobación de la revocación de certificados, en los que solo necesita saber si el número de serie de un certificado está en una lista de revocaciones.
- kvsHandle.get(clave): recupere un valor del KeyValueStore para escenarios de validación más complejos. Úselo cuando necesite acceder a los datos de configuración, las reglas de validación o los metadatos asociados a un certificado o identificador de dispositivo.

Las operaciones de KeyValueStore son asíncronas y deben usarse con la sintaxis async/await. El KeyValueStore tiene un límite de tamaño total de 10 MB y admite hasta 10 millones de pares clave-valor. Con el tiempo, los datos de KeyValueStore son coherentes en todas las ubicaciones periféricas y, por lo general, las actualizaciones se propagan en cuestión de segundos.

Para obtener un rendimiento óptimo, estructure las claves de KeyValueStore para minimizar las operaciones de búsqueda. Utilice los números de serie de los certificados como claves para comprobar las revocaciones de forma sencilla o cree claves compuestas que combinen el hash del emisor y el número de serie para entornos con varias autoridades de certificación. Tenga en cuenta las ventajas y desventajas entre la complejidad de las claves y la capacidad de KeyValueStore al diseñar la estructura de datos.

Uso de async y await

Las funciones de conexión admiten operaciones asíncronas mediante la sintaxis de async/await, que es esencial cuando se trabaja con operaciones de KeyValueStore u otras tareas asincrónicas. El patrón async/await garantiza que la función espere a que se completen las búsquedas en KeyValueStore antes de tomar decisiones de conexión, a la vez que mantiene las características de alto rendimiento necesarias para el procesamiento del establecimiento de comunicación de TLS.

El uso adecuado de la función async/await es fundamental para las funciones de conexión, ya que las operaciones de KeyValueStore, si bien son muy rápidas, siguen siendo operaciones de red que requieren la coordinación de toda la infraestructura distribuida de CloudFront. El tiempo de ejecución gestiona automáticamente la resolución prometida y garantiza que la función se complete dentro del límite de ejecución de 5 milisegundos.

Example: función de conexión asíncrona con KeyValueStore

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Async operation to check KeyValueStore for certificate revocation
    const isRevoked = await
 kvsHandle.exists(connection.clientCertificate.certificates.leaf.serialNumber);

    if (isRevoked) {
        // Log the revocation decision with certificate details
        connection.logCustomData(`REVOKED_CERT:
${connection.clientCertificate.certificates.leaf.serialNumber}:
${connection.clientCertificate.certificates.leaf.issuer}`);
        console.log(`Denying connection for revoked certificate:
 ${connection.clientCertificate.certificates.leaf.serialNumber}`);
        return connection.deny();
    }

    // Log successful validation for monitoring
    connection.logCustomData(`VALID_CERT:
${connection.clientCertificate.certificates.leaf.serialNumber}`);
    console.log(`Allowing connection for valid certificate:
 ${connection.clientCertificate.certificates.leaf.serialNumber}`);
    return connection.allow();
}
```

Utilice siempre async/await al llamar a los métodos de KeyValueStore u otras operaciones asincrónicas. El tiempo de ejecución de la función de conexión gestiona automáticamente la resolución de las promesas y garantiza un flujo de ejecución adecuado dentro de las estrictas restricciones temporales del procesamiento de establecimiento de comunicación de TLS. Evite utilizar los patrones .then() o callback, ya que async/await permite gestionar los errores de forma más limpia y ofrece un mejor rendimiento en el entorno de la función de conexión.

Al diseñar funciones de conexión asíncronas, estructure el código para minimizar el número de operaciones de KeyValueStore y realícelas lo antes posible en su lógica de validación. Esto garantiza el máximo rendimiento y reduce el riesgo de problemas de tiempo de espera durante los periodos de tráfico alto. Considere agrupar las comprobaciones de validación relacionadas con los lotes y utilizar el método KeyValueStore más eficiente (exists() frente a get()) para el caso de uso.

Ejemplos de código de función de conexión

Los siguientes ejemplos muestran patrones de funciones de conexión comunes para diferentes escenarios comunes. Utilice estos ejemplos como puntos de partida para las propias implementaciones de funciones de conexión.

Example: validación de certificados de dispositivo

Este ejemplo valida los números de serie de los dispositivos y los campos de asunto de los certificados para dispositivos IoT, consolas de juegos y otros escenarios de autenticación de clientes:

```
async function connectionHandler(connection) {
    // Custom validation: check device serial number format
    const serialNumber = connection.clientCertificate.certificates.leaf.serialNumber;
    if (!serialNumber.startsWith("DEV")) {
        connection.logCustomData(`INVALID_SERIAL:${serialNumber}`);
        return connection.deny();
    }

    // Validate certificate subject contains required organizational unit
    const subject = connection.clientCertificate.certificates.leaf.subject;
    if (!subject.includes("OU=AuthorizedDevices")) {
        connection.logCustomData(`INVALID_OU:${subject}`);
        return connection.deny();
    }

    // Allow connection for valid devices
    connection.logCustomData(`VALID_DEVICE:${serialNumber}`);
    return connection.allow();
}
```

Esta función realiza varias comprobaciones de validación además de la validación estándar del certificado, como el formato del número de serie del dispositivo y la verificación de la unidad organizativa.

Example: mTLS opcionales con autenticación mixta

Este ejemplo gestiona las conexiones de mTLS y las que no lo son con políticas de autenticación diferentes:

```
async function connectionHandler(connection) {
    if (connection.clientCertificate) {
        // mTLS connection - enhanced validation for certificate holders
        const subject = connection.clientCertificate.certificates.leaf.subject;
        connection.logCustomData(`MTLS_SUCCESS:${subject}:${connection.clientIp}`);
        console.log(`mTLS connection from: ${subject}`);
        return connection.allow();
    } else {
        // Non-mTLS connection - apply IP-based restrictions
        const clientIp = connection.clientIp;

        // Only allow non-mTLS from specific IP ranges
        if (clientIp.startsWith("203.0.113.") || clientIp.startsWith("198.51.100.")) {
            connection.logCustomData(`NON_MTLS_ALLOWED:${clientIp}`);
            console.log(`Non-mTLS connection allowed from: ${clientIp}`);
            return connection.allow();
        }

        connection.logCustomData(`NON_MTLS_DENIED:${clientIp}`);
        return connection.deny();
    }
}
```

Esta función proporciona una seguridad mejorada para los clientes con certificados y, al mismo tiempo, mantiene la compatibilidad con los clientes antiguos de rangos de IP fiables.

Prueba de las funciones de conexión de CloudFront antes de la implementación

Puede probar las funciones de conexión de CloudFront en la etapa de DESARROLLO mediante la operación de la API TestConnectionFunction. Las pruebas permiten validar la lógica de la función con ejemplos de eventos de conexión antes de publicarlos en la etapa ACTIVA.

Temas

- Proceso de prueba
- Resultados de la prueba

- Objeto de prueba de conexión

Proceso de prueba

Para probar una función de conexión:

1. Cree una función de conexión en la etapa de DESARROLLO.
2. Prepare un objeto de conexión de prueba que represente el evento de conexión de TLS.
3. Utilice la operación de la API TestConnectionFunction para ejecutar la función con los datos de prueba.
4. Revise los resultados de la prueba, incluidos los resultados de las funciones, los registros de ejecución y cualquier mensaje de error.
5. Actualice el código de función según sea necesario y repita el proceso de prueba.

Resultados de la prueba

Al probar una función de conexión, los resultados incluyen:

- Resumen de la función: metadatos sobre la función que se probó
- Utilización del cómputo: métricas de rendimiento que muestran el uso de los recursos
- Registros de ejecución: resultados de la consola de la función, incluidas las instrucciones de registro
- Resultado de la función: el resultado devuelto por la función
- Mensajes de error: cualquier error o excepción de tiempo de ejecución que se haya producido durante la ejecución

Objeto de prueba de conexión

El objeto de prueba de conexión es un blob binario (hasta 40 KB) que representa el evento de conexión de TLS que procesará la función. Este objeto contiene el certificado y la información de conexión que la función utiliza para tomar decisiones de autenticación.

> **Note**
>
> El tiempo de ejecución de funciones de conexión de CloudFront define la estructura y el formato específicos del objeto de prueba de conexión. Consulte la documentación de

CloudFront Functions o contacte con AWS Support para obtener información sobre cómo crear los objetos de prueba adecuados para el caso de uso.

Tras crear la función de conexión, puede:

- Probar la función: utilice la funcionalidad de prueba de la consola o la CLI para validar la función con ejemplos de eventos de conexión. Para obtener más información, consulte Pruebas de funciones de conexión.
- Actualizar la función: modifique el código y la configuración de la función según sea necesario. Las funciones de conexión en la etapa de DESARROLLO se pueden actualizar en cualquier momento.
- Publicar la función: cuando esté lista para la producción, publique la función para pasarla de la etapa de DESARROLLO a la etapa ACTIVA. Para obtener más información, consulte asociación de funciones de conexión.
- Asociar con una distribución: asocie la función publicada con la distribución compatible con MTLS para gestionar las conexiones en directo. Para obtener más información, consulte asociación de funciones de conexión.

Asociación de funciones de conexión con distribuciones

Tras publicar una función de conexión en la etapa ACTIVA, debe asociarla a una distribución compatible con mTLS para gestionar las conexiones en directo. Las funciones de conexión se asocian por distribución, a diferencia de las funciones de solicitud y respuesta del espectador, que están asociadas a los comportamientos de la memoria caché.

Temas

- Requisitos de asociación
- Organización de funciones con filtros
- Consideraciones sobre la implementación

Requisitos de asociación

Asociación de una función de conexión con una distribución:

- La función debe estar en la etapa ACTIVA
- La distribución debe tener habilitado mTLS

- La distribución debe tener un almacén de confianza válido configurado
- Solo puede asociar una función de conexión por distribución

Organización de funciones con filtros

CloudFront proporciona funciones de filtrado para ayudarlo a organizar y administrar funciones de conexión:

- Filtro de ID de distribución: busque funciones asociadas a distribuciones específicas
- Filtro de almacén de valores clave: busque funciones que utilicen almacenes de valores clave específicos para la búsqueda de datos
- Filtro de etapas: muestre las funciones en las etapas DESARROLLO o ACTIVA

Utilice estos filtros cuando se administren múltiples funciones de conexión en diferentes distribuciones o entornos de desarrollo.

Consideraciones sobre la implementación

Tenga en cuenta estos factores al implementar las funciones de conexión:

- Implementación global: las funciones de conexión se implementan en todas las ubicaciones periféricas de CloudFront del mundo, lo que puede tardar varios minutos
- Administración de versiones: cada versión publicada crea una nueva función ACTIVA que reemplaza a la versión anterior
- Estrategia de reversión: planifique la reversión conservando las versiones anteriores del código de la función que funcionaban
- Pruebas en producción: considere la posibilidad de utilizar distribuciones independientes para los entornos de ensayo y producción

Implementación de la revocación de certificados para TLS mutua (espectador) con CloudFront Functions y KeyValueStore

Puede utilizar funciones de conexión de CloudFront con KeyValueStore para implementar la comprobación de revocación de certificados. Esto permite mantener una lista de números de serie de los certificados revocados y comparar los certificados de los clientes con esta lista durante el establecimiento de comunicación de TLS.

Para implementar la revocación de certificados, necesita estos componentes:

- Una distribución configurada con un mTLS de espectador
- Un KeyValueStore que contenga números de serie de certificados revocados
- Una función de conexión que consulta el KeyValueStore para comprobar el estado del certificado

Cuando un cliente se conecta, CloudFront valida el certificado con el almacén de confianza y, a continuación, ejecuta la función de conexión. La función compara el número de serie del certificado con el KeyValueStore y permite o deniega la conexión.

Temas

- Paso 1: crear un KeyValueStore para los certificados revocados
- Paso 2: crear la función de conexión de revocación
- Paso 3: probar la función de revocación
- Paso 4: asocie la función a la distribución
- Escenarios de revocación avanzada

Paso 1: crear un KeyValueStore para los certificados revocados

Cree un KeyValueStore para almacenar los números de serie de los certificados revocados que la función de conexión pueda comprobar durante las conexiones de mTLS.

En primer lugar, prepare los números de serie de los certificados revocados en formato JSON:

```
{
  "data": [
    {
      "key": "ABC123DEF456",
      "value": ""
    },
    {
      "key": "789XYZ012GHI",
      "value": ""
    }
  ]
}
```

Cargue este archivo JSON en un bucket de S3 y, a continuación, cree el KeyValueStore:

```
aws s3 cp revoked-serials.json s3://your-bucket-name/revoked-serials.json
aws cloudfront create-key-value-store \
  --name revoked-serials-kvs \
  --import-source '{
    "SourceType": "S3",
    "SourceARN": "arn:aws:s3:::your-bucket-name/revoked-serials.json"
  }'
```

Espere a que el KeyValueStore termine de aprovisionarse. Compruebe el estado con:

```
aws cloudfront get-key-value-store --name "revoked-serials-kvs"
```

Paso 2: crear la función de conexión de revocación

Cree una función de conexión que compruebe los números de serie de los certificados con los de KeyValueStore para determinar si los certificados se revocan.

Cree una función de conexión que compruebe los números de serie de los certificados con el KeyValueStore:

```
aws cloudfront create-connection-function \
  --name "revocation-control" \
  --connection-function-config file://connection-function-config.json \
  --connection-function-code file://connection-function-code.txt
```

El archivo de configuración especifica la asociación de KeyValueStore:

```
{
  "Runtime": "cloudfront-js-2.0",
  "Comment": "A function that implements revocation control via KVS",
  "KeyValueStoreAssociations": {
    "Quantity": 1,
    "Items": [
      {
        "KeyValueStoreArn": "arn:aws:cloudfront::account-id:key-value-store/kvs-id"
      }
    ]
  }
}
```

El código de la función de conexión comprueba KeyValueStore por si hay certificados revocados:

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Get parsed client serial number from client certificate
    const clientSerialNumber = connection.clientCertInfo.serialNumber;

    // Check KVS to see if serial number exists as a key
    const serialNumberExistsInKvs = await kvsHandle.exists(clientSerialNumber);

    // Deny connection if serial number exists in KVS
    if (serialNumberExistsInKvs) {
        console.log("Connection denied - certificate revoked");
        return connection.deny();
    }

    // Allow connections that don't exist in kvs
    console.log("Connection allowed");
    return connection.allow();
}
```

Paso 3: probar la función de revocación

Utilice la consola de CloudFront para probar la función de conexión con certificados de ejemplo. Navegue hasta la función de conexión en la consola y utilice la pestaña Probar.

Prueba con certificados de ejemplo

1. Pegue un certificado de ejemplo en formato PEM en la interfaz de prueba.
2. Si lo desea, especifique una dirección IP de cliente para probar la lógica basada en IP.
3. Elija Función de prueba para consultar los resultados de ejecución.
4. Revise los registros de ejecución para verificar la lógica de la función.

Realice pruebas con certificados válidos y revocados para asegurarse de que la función gestiona ambos escenarios correctamente. Los registros de ejecución muestran el resultado de console.log y cualquier error que se produzca durante la ejecución de la función.

Paso 4: asocie la función a la distribución

Una vez que publique la función de conexión, asóciela a la distribución compatible con mTLS para activar la comprobación de revocación de certificados.

Puede asociar la función desde la página de configuración de distribución o desde la tabla de distribuciones asociadas a la función de conexión. Vaya a la configuración de distribución, vaya a la sección Autenticación mutua del espectador (mTLS), seleccione la función de conexión y guarde los cambios.

Escenarios de revocación avanzada

Para requisitos de revocación de certificados más complejos, considere estas configuraciones adicionales:

Temas

- Convierta las listas de revocación de certificados (CRL) al formato KeyValueStore.
- Gestión de varias autoridades de certificación
- Agregación de datos personalizados a los registros de conexión
- Actualizaciones de CRL administradas
- Planificación de la capacidad de KeyValueStore

Convierta las listas de revocación de certificados (CRL) al formato KeyValueStore.

Si tiene un archivo de lista de revocación de certificados (CRL), puede convertirlo al formato JSON de KeyValueStore mediante OpenSSL y jq:

Convierta el CRL al formato KeyValueStore

Extraiga los números de serie del archivo CRL:

```
openssl crl -text -noout -in rfc5280_CRL.crl | \
  awk '/Serial Number:/ {print $3}' | \
  cut -d'=' -f2 | \
  sed 's/../&:/g;s/:$//' >> serialnumbers.txt
```

Convierta los números de serie al formato JSON de KeyValueStore:

```
jq -R -s 'split("\n") | map(select(length > 0)) | {data: map({"key": ., "value": ""})}'
 \
  serialnumbers.txt >> serialnumbers_kvs.json
```

Cargue el archivo formateado en S3 y cree el KeyValueStore tal y como se describe en el paso 1.

Gestión de varias autoridades de certificación

Si su TrustStore contiene varias autoridades de certificación (CA), incluya la información del emisor en las claves de KeyValueStore para evitar conflictos entre certificados de distintas autoridades de certificación que puedan tener el mismo número de serie.

En escenarios con varias autoridades de certificación, utilice como clave una combinación del hash SHA1 del emisor y el número de serie:

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();
    const clientCert = connection.clientCertInfo;

    // Create composite key with issuer hash and serial number
    const issuer = clientCert.issuer.replace(/[^a-zA-Z0-9]/g, '').substring(0, 20);
    const serialno = clientCert.serialNumber;
    const compositeKey = `${issuer}_${serialno}`;

    const cert_revoked = await kvsHandle.exists(compositeKey);

    if (cert_revoked) {
        console.log(`Blocking revoked cert: ${serialno} from issuer: ${issuer}`);
        connection.deny();
    } else {
        connection.allow();
    }
}
```

> **Note**
>
> Al utilizar el identificador del emisor y el número de serie, se crean claves más largas, lo que puede reducir el número total de entradas que puede almacenar en KeyValueStore.

Agregación de datos personalizados a los registros de conexión

Las funciones de conexión pueden agregar datos personalizados a los registros de conexión de CloudFront mediante el método logCustomData. Esto permite incluir los resultados de las comprobaciones de revocación, la información sobre los certificados u otros datos relevantes en los registros.

```
async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();
    const clientSerialNumber = connection.clientCertInfo.serialNumber;
    const serialNumberExistsInKvs = await kvsHandle.exists(clientSerialNumber);

    if (serialNumberExistsInKvs) {
        // Log revocation details to connection logs
        connection.logCustomData(`REVOKED:${clientSerialNumber}:DENIED`);
        console.log("Connection denied - certificate revoked");
        return connection.deny();
    }

    // Log successful validation
    connection.logCustomData(`VALID:${clientSerialNumber}:ALLOWED`);
    console.log("Connection allowed");
    return connection.allow();
}
```

Los datos personalizados están limitados a 800 bytes de texto UTF-8 válido. Si supera este límite, CloudFront trunca los datos hasta el límite UTF-8 válido más cercano.

> **Note**
>
> El registro de datos personalizado solo funciona cuando los registros de conexión están habilitados para la distribución. Si los registros de conexión no están configurados, el método logCustomData no es operativo.

Actualizaciones de CRL administradas

Las autoridades de certificación pueden emitir dos tipos de CRL:

- CRL completas: contienen una lista completa de todos los certificados revocados
- CRL de Delta: solo se muestran los certificados revocados desde la última CRL completa

Para obtener actualizaciones completas de la CRL, cree un KeyValueStore nuevo con los datos actualizados y redirija la asociación de la función de conexión al nuevo KeyValueStore. Este enfoque es más sencillo que calcular las diferencias y realizar actualizaciones incrementales.

Para las actualizaciones de CRL delta, utilice el comando update-keys para agregar nuevos certificados revocados al KeyValueStore existente:

```
aws cloudfront update-key-value-store \
  --name "revoked-serials-kvs" \
  --if-match "current-etag" \
  --put file://delta-revoked-serials.json
```

Planificación de la capacidad de KeyValueStore

KeyValueStore tiene un límite de tamaño total de 5 MB y admite hasta 10 millones de pares clave-valor. Planifique la capacidad de la lista de revocación en función del formato de la clave y del tamaño de los datos:

- Solo número de serie: almacenamiento eficiente para una comprobación sencilla de las revocaciones
- Identificador del emisor + número de serie: claves más largas para entornos con varias autoridades de certificación

En el caso de listas de revocación de gran tamaño, considere la posibilidad de implementar un enfoque escalonado en el que mantenga almacenes KeyValueStores independientes para diferentes categorías de certificados o periodos de tiempo.

Personalización en la periferia con Lambda@Edge

Lambda@Edge es una extensión de AWS Lambda. Lambda@Edge es un servicio informático que le permite ejecutar funciones que personalizan el contenido que entrega Amazon CloudFront. Puede crear funciones de Node.js o Python en la consola de Lambda en una sola Región de AWS, Este de EE. UU. (Norte de Virginia).

Después de crear la función, puede agregar desencadenadores con la consola de Lambda o la de CloudFront que hacen que las funciones se ejecuten en ubicaciones de AWS que están más cerca del espectador, sin necesidad de aprovisionar ni administrar servidores. Si lo desea, puede utilizar las operaciones de las API de Lambda y CloudFront para configurar las funciones y los desencadenadores mediante programación.

Lambda@Edge se escala automáticamente, desde unas pocas solicitudes al día a miles de solicitudes por segundo. Procesar solicitudes en ubicaciones de AWS más cercanas al espectador en lugar de en servidores de origen reduce significativamente la latencia y mejora la experiencia del usuario.

> **Note**
>
> Lambda@Edge no es compatible con las solicitudes de gRPC. Para obtener más información, consulte Uso de gRPC con distribuciones de CloudFront.

Temas

- Cómo funciona Lambda@Edge con las solicitudes y las respuestas
- Formas de utilizar Lambda@Edge
- Introducción a las funciones de Lambda@Edge (consola)
- Configuración de permisos y roles de IAM para Lambda@Edge
- Escritura y creación de una función de Lambda@Edge
- Adición de desencadenadores para una función de Lambda@Edge
- Prueba y depuración de funciones de Lambda@Edge
- Eliminación de réplicas y funciones de Lambda@Edge
- Estructura de eventos de Lambda@Edge
- Trabajo con solicitudes y respuestas
- Funciones de ejemplo de Lambda@Edge

Cómo funciona Lambda@Edge con las solicitudes y las respuestas

Cuando asocia una distribución de CloudFront con una función de Lambda@Edge, CloudFront intercepta solicitudes y respuestas en ubicaciones de borde de CloudFront. Puede ejecutar funciones de Lambda cuando se producen los siguientes eventos de CloudFront:

- Cuando CloudFront reciba una solicitud de un espectador (solicitud del espectador)
- Antes de que CloudFront reenvíe una solicitud al origen (solicitud al origen)
- Cuando CloudFront reciba una respuesta del origen (respuesta del origen)

- Antes de que CloudFront devuelva la respuesta al espectador (respuesta al espectador)

Si utiliza AWS WAF, la solicitud del espectador de Lambda@Edge se ejecuta después de aplicar cualquier regla de AWS WAF.

Para obtener más información, consulte Trabajo con solicitudes y respuestas y Estructura de eventos de Lambda@Edge.

Formas de utilizar Lambda@Edge

Existe una gran variedad de usos para el procesamiento con Lambda@Edge con su distribución de Amazon CloudFront, como en los siguientes ejemplos:

- Una función de Lambda puede inspeccionar las cookies y reescribir URL, a fin de que los usuarios vean distintas versiones de un sitio para pruebas A/B.
- CloudFront puede devolver diferentes objetos a lectores en función del dispositivo que estén utilizando comprobando el encabezado `User-Agent`, que incluye información acerca de los dispositivos. Por ejemplo, CloudFront puede devolver imágenes diferentes en función del tamaño de las pantallas de su dispositivo. Del mismo modo, la función podría tener en cuenta el valor del encabezado `Referer` y hacer que CloudFront devuelva a bots las imágenes con la menor resolución disponible.
- O bien, podría comprobar las cookies para otros criterios. Por ejemplo, en un sitio web minorista que vende ropa, si utiliza cookies para indicar el color de chaqueta que eligió un usuario, la función de Lambda puede cambiar la solicitud para que CloudFront devuelva la imagen de una chaqueta del color seleccionado.
- Una función de Lambda puede generar respuestas HTTP cuando ocurran eventos de solicitudes al origen o del lector de CloudFront.
- Una función puede inspeccionar encabezados o tokens de autorización e insertar un encabezado para controlar el acceso a su contenido antes de que CloudFront reenvíe una solicitud a su origen.
- Una función de Lambda también puede realizar llamadas de red a recursos externos para confirmar credenciales de usuarios o buscar contenido adicional para personalizar una respuesta.

Para obtener más información, incluido código de ejemplo, consulte Funciones de ejemplo de Lambda@Edge.

Para obtener más información acerca de cómo configurar Lambda@Edge en la consola, consulte Tutorial: Creación de una función de Lambda@Edge básica (consola).

Introducción a las funciones de Lambda@Edge (consola)

Con Lambda@Edge, puede utilizar desencadenadores de CloudFront para invocar una función de Lambda. Cuando asocia una distribución de CloudFront con una función de Lambda, CloudFront intercepta solicitudes y respuestas en ubicaciones de borde de CloudFront y ejecuta la función. Las funciones de Lambda pueden mejorar la seguridad o personalizar la información según la ubicación de los lectores, para mejorar el rendimiento.

En la siguiente lista se ofrece información general básica sobre cómo crear y utilizar funciones de Lambda con CloudFront.

Información general: Creación y uso de funciones de Lambda con CloudFront

1. Cree una función de Lambda en la región Este de EE. UU. (Norte de Virginia).
2. Guarde y publique una versión numerada de la función.

   Si desea cambiar la función, debe editar la versión $LATEST de la función en la región EE. UU. Este (Norte de Virginia). A continuación, antes de configurarla para usarla con CloudFront, publique una nueva versión numerada.
3. Asocie la función a un comportamiento de distribución y caché de CloudFront. A continuación, especifique uno o varios eventos de CloudFront (desencadenadores) que provoquen la ejecución de la función. Por ejemplo, puede crear un desencadenador para que la función se ejecute cuando CloudFront reciba una solicitud de un lector.
4. Cuando crea un desencadenador, Lambda crea réplicas de la función en ubicaciones de AWS de todo el mundo.

> **Tip**
>
> Para obtener más información, consulte creación y actualización de funciones, la estructura de los eventos y la agregación de desencadenadores de CloudFront. También puede encontrar más ideas y obtener ejemplos de código en Funciones de ejemplo de Lambda@Edge.

Para ver un tutorial paso a paso, consulte el tema siguiente:

Temas

- Tutorial: Creación de una función de Lambda@Edge básica (consola)

Tutorial: Creación de una función de Lambda@Edge básica (consola)

En este tutorial, se muestra cómo comenzar a utilizar Lambda@Edge mediante la creación y configuración de una función de Node.js de ejemplo que se ejecuta en CloudFront. En el ejemplo se agregan encabezados HTTP de seguridad a una respuesta cuando CloudFront recupera un archivo. (Esto puede mejorar la seguridad y la privacidad de un sitio web).

No necesita su propio sitio web para este tutorial. Sin embargo, si decide crear su propia solución de Lambda@Edge, seguirá pasos similares y elegirá entre las mismas opciones.

Temas

- Paso 1: Regístrese para obtener una Cuenta de AWS
- Paso 2: Cree una distribución de CloudFront
- Paso 3: Cree su función
- Paso 4: Agregue un desencadenador de CloudFront para ejecutar la función
- Paso 5: Verifique que la función se ejecuta
- Paso 6: Solucione problemas
- Paso 7: Elimine los recursos del ejemplo
- Información relacionada

Paso 1: Regístrese para obtener una Cuenta de AWS

Si aún no lo ha hecho, regístrese para conseguir una Cuenta de AWS. Para obtener más información, consulte Cómo crear una Cuenta de AWS.

Paso 2: Cree una distribución de CloudFront

Antes de crear la función de Lambda@Edge de ejemplo, debe tener un entorno de CloudFront con el que trabajar que incluya un origen para distribuir contenido.

En este ejemplo, creará una distribución de CloudFront que utilice un bucket de Amazon S3 como origen de la distribución. Si ya dispone de un entorno, puede omitir este paso.

Para crear una distribución de CloudFront con un origen de Amazon S3

1. Cree un bucket de Amazon S3 con un archivo o dos, como, por ejemplo, archivos de imágenes para usarlos como contenido de muestra. Puede seguir los pasos que se detallan en Cargar

su contenido en Amazon S3. Asegúrese de que establece permisos para conceder acceso de lectura público a los objetos del bucket.

2. Cree una distribución de CloudFront y agregue el bucket de S3 como un origen, siguiendo los pasos que se describen Crear una distribución web de CloudFront. Si ya tiene una distribución, solo es necesario que añada el bucket como origen para esa distribución.

> **Tip**
>
> Tome nota del ID de distribución. Más adelante en este tutorial, al agregar un desencadenador de CloudFront para la función, debe elegir el ID de la distribución en una lista desplegable, por ejemplo, `E653W22221KDDL`.

Paso 3: Cree su función

En este paso, se crea una función de Lambda a partir de una plantilla de esquema en la consola de Lambda. La función agrega código para actualizar los encabezados de seguridad de su distribución de CloudFront.

Para crear una función Lambda, realice el siguiente procedimiento:

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.

> **Important**
>
> Asegúrese de que está en la Región de AWS Este de EE. UU.-1 (Norte de Virginia) (us-east-1). Debe estar en esta región para crear funciones de Lambda@Edge.

2. Elija Create function (Crear función).
3. En la página Create function (Crear función), elija Use a blueprint (Usar un proyecto) y, a continuación, filtre los proyectos de CloudFront especificando **`cloudfront`** en el campo de búsqueda.

> **Note**
>
> Los proyectos de CloudFront solo están disponibles en la región US-East-1 (N. Virginia) (EE. UU. Este (Norte de Virginia) (us-east-1).

4. Elija el esquema Modificar encabezado de respuesta HTTP como la plantilla para la función.
5. Escriba la siguiente información sobre su función:
   - Nombre de la función: ingrese un nombre para la función.
   - Rol de ejecución: elija cómo se deben establecer los permisos para la función. Para utilizar la plantilla de política de permisos de Lambda@Edge básica recomendada, elija Create a new role from policy templates (Crear un nuevo rol a partir de plantillas de política de AWS).
   - Nombre de rol: ingrese un nombre para el rol que crea la plantilla de política.
   - Plantillas de política: Lambda agrega automáticamente la plantilla de política Permisos básicos de Lambda@Edge porque ha elegido un esquema de CloudFront como base de la función. Esta plantilla de política agrega permisos de rol de ejecución que permiten a CloudFront ejecutar su función de Lambda en ubicaciones de CloudFront en todo el mundo. Para obtener más información, consulte Configuración de permisos y roles de IAM para Lambda@Edge.
6. Elija Crear función en la parte inferior de la página.
7. En el panel Implementar en Lambda@Edge que aparece, elija Cancelar. (Para este tutorial, debe modificar el código de la función antes de implementarla en Lambda@Edge).
8. Desplácese hacia abajo hasta la sección Código fuente.
9. Reemplace el código de la plantilla por una función que modifique los encabezados de seguridad que devuelve el origen. Por ejemplo, puede utilizar código similar al siguiente:

```
'use strict';
export const handler = (event, context, callback) => {

    //Get contents of response
    const response = event.Records[0].cf.response;
    const headers = response.headers;

    //Set new headers
    headers['strict-transport-security'] = [{key: 'Strict-Transport-Security',
 value: 'max-age= 63072000; includeSubdomains; preload'}];
    headers['content-security-policy'] = [{key: 'Content-Security-Policy', value:
 "default-src 'none'; img-src 'self'; script-src 'self'; style-src 'self'; object-
src 'none'"}];
    headers['x-content-type-options'] = [{key: 'X-Content-Type-Options', value:
 'nosniff'}];
    headers['x-frame-options'] = [{key: 'X-Frame-Options', value: 'DENY'}];
    headers['x-xss-protection'] = [{key: 'X-XSS-Protection', value: '1;
 mode=block'}];
```

```
    headers['referrer-policy'] = [{key: 'Referrer-Policy', value: 'same-origin'}];

    //Return modified response
    callback(null, response);
};
```

10. Elija Archivo, Guardar para guardar el código actualizado.
11. Elija Implementar.

Continúe con la siguiente sección para agregar un desencadenador de CloudFront para ejecutar la función.

Paso 4: Agregue un desencadenador de CloudFront para ejecutar la función

Ahora que tiene una función de Lambda para actualizar los encabezados de seguridad, configure el desencadenador de CloudFront para ejecutar la función que va a agregar los encabezados a cualquier respuesta que CloudFront reciba desde el origen de la distribución.

Para configurar el desencadenador CloudFront para su función

1. En la consola de Lambda, en la página Información general de la función de la función, seleccione Agregar desencadenador.
2. En Configuración del desencadenador, elija CloudFront.
3. Elija Implementar en Lambda @Edge.
4. En el panel Implementar en Lambda@Edge, en Configurar desencadenador de CloudFront, escriba lo siguiente:
   - Distribución: el ID de distribución de CloudFront que se debe asociar a la función. En la lista desplegable, elija el ID de distribución.
   - Comportamiento de la caché: el comportamiento de la caché que se debe utilizar con el desencadenador. En este ejemplo, deje el valor establecido en *, es decir, el comportamiento de caché predeterminado de la distribución. Para obtener más información, consulte Configuración del comportamiento de la caché en el tema Referencia de toda la configuración de distribución.
   - Evento de CloudFront: el desencadenador que especifica cuándo se ejecutará la función. Queremos que la función de encabezados de seguridad se ejecute siempre que CloudFront devuelva una respuesta desde el origen. En la lista desplegable, elija Respuesta de origen.

Para obtener más información, consulte Adición de desencadenadores para una función de Lambda@Edge.

5. Seleccione la casilla de verificación Confirmar implementación en Lambda @Edge.
6. Seleccione Deploy (Implementar) para añadir el desencadenador y replicar la función a ubicaciones de AWS en todo el mundo.
7. Espere a que la función se replique. Esta operación suele tardar varios minutos.

   Para comprobar si la replicación ha terminado, vaya a la consola de CloudFront y consulte la distribución. Espere a que el estado de la distribución cambie de Implementando a una fecha y hora, lo que significa que la función se ha replicado. Para comprobar que la función es correcta, realice los pasos de la siguiente sección.

Paso 5: Verifique que la función se ejecuta

Ahora que ha creado la función de Lambda y que ha configurado un desencadenador para que la ejecute en una distribución de CloudFront, asegúrese de que la función se comporta según lo previsto. En este ejemplo, comprobamos los encabezados HTTP que devuelve CloudFront, para asegurarnos de que se agregan los encabezados de seguridad.

Para verificar que la función de Lambda@Edge añade los encabezados de seguridad

1. En un navegador, escriba la dirección URL de un archivo de su bucket de S3. Por ejemplo, puede utilizar una URL similar a `https://d111111abcdef8.cloudfront.net/image.jpg`.

   Para obtener más información sobre el nombre de dominio de CloudFront que se debe utilizar en la URL del archivo, consulte Personalización del formato de URL para archivos en CloudFront.
2. Abra la barra de herramientas para desarrolladores web del navegador. Por ejemplo, en la ventana del navegador Chrome, abra el menú contextual (haga clic con el botón derecho) y, a continuación, elija Inspeccionar.
3. Elija la pestaña Network (Red).
4. Vuelva a cargar la página para ver la imagen y, a continuación, elija una solicitud HTTP en el panel izquierdo. Verá que los encabezados HTTP se muestran en un panel independiente.
5. Examine la lista de encabezados HTTP para verificar que incluye los encabezados de seguridad esperados. Por ejemplo, es posible que vea encabezados similares a los que se muestran en la siguiente captura de pantalla.

Si los encabezados de seguridad se incluyen en la lista de encabezados, ¡estupendo! Significa que ha creado correctamente su primera función de Lambda@Edge. Si CloudFront devuelve algún error o hay otros problemas, continúe con el paso siguiente para solucionar los problemas.

Paso 6: Solucione problemas

Si CloudFront devuelve errores o no agrega los encabezados de seguridad según lo previsto, puede investigar la ejecución de la función consultando los CloudWatch Logs. Asegúrese de utilizar los registros almacenados en la ubicación de AWS más cercana a la ubicación en que se ejecuta la función.

Por ejemplo, si ve el archivo desde Londres, pruebe a cambiar la región en la consola de CloudWatch a UE (Londres).

Para examinar los registros de CloudWatch para su función de Lambda@Edge

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Cambie Región (Región) a la ubicación que se muestra al ver el archivo en el navegador. Aquí es donde se está ejecutando la función.

3. En el panel izquierdo, elija Logs para ver los logs de la distribución.

Para obtener más información, consulte Supervisión de métricas de CloudFront con Amazon CloudWatch.

Paso 7: Elimine los recursos del ejemplo

Si ha creado un bucket de Amazon S3 y una distribución de CloudFront solo para este tutorial, elimine los recursos de AWS asignados para que no se le apliquen cargos. Después de eliminar los recursos de AWS, el contenido que haya añadido dejará de estar disponible.

Tareas

- Elimine el bucket de S3
- Para eliminar la función de Lambda
- Eliminar la distribución de CloudFront

Elimine el bucket de S3

Antes de eliminar su bucket de Amazon S3, asegúrese de que la función de registro esté desactivada para el bucket. De lo contrario, AWS seguirá escribiendo logs en el bucket mientras lo elimina.

Para deshabilitar el registro en el bucket

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Seleccione el bucket y, luego, seleccione Properties (Propiedades).
3. En Properties (Propiedades), elija Logging (Registro).
4. Elimine la selección del recuadro Enabled (Habilitado).
5. Seleccione Guardar.

Ahora ya puede eliminar el bucket. Para obtener más información, consulte Eliminación de un bucket en la Guía del usuario de la consola de Amazon Simple Storage Service.

Para eliminar la función de Lambda

Para obtener instrucciones sobre cómo eliminar la asociación de función de Lambda y, opcionalmente, la propia función, consulte Eliminación de réplicas y funciones de Lambda@Edge.

Eliminar la distribución de CloudFront

Antes de eliminar una distribución de CloudFront, debe desactivarla. Una distribución deshabilitada ya no es funcional y no acumula cargos. Puede habilitar una distribución deshabilitada en cualquier momento. Después de eliminar una distribución deshabilitada, esta deja de estar disponible.

Para desactivar y eliminar una distribución de CloudFront, realice las siguientes acciones:

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Seleccione la distribución que desea deshabilitar y elija Disable (Deshabilitar).
3. Cuando se le indique que confirme, seleccione Yes, Disable (Sí, deshabilitar).
4. Seleccione la distribución desactivada y después Delete (Eliminar).
5. Cuando se le indique que confirme, seleccione Yes, Delete.

Información relacionada

Ahora que tiene una idea básica de cómo funcionan las funciones de Lambda@Edge, puede obtener más información leyendo los temas siguientes:

- Funciones de ejemplo de Lambda@Edge
- Prácticas recomendadas de diseño de Lambda@Edge
- Reducción de la latencia y traslado de cómputo al borde con Lambda@Edge

Configuración de permisos y roles de IAM para Lambda@Edge

Para configurar Lambda@Edge, debe tener los siguientes permisos y roles de IAM para AWS Lambda:

- Permisos de IAM: estos permisos le permiten crear la función de Lambda y asociarla a la distribución de CloudFront.
- Un rol de ejecución de una función de Lambda (rol de IAM): las entidades principales de servicio de Lambda asumen este rol para ejecutar la función.
- Roles vinculados a servicios para Lambda@Edge: los roles vinculados a servicios permiten a Servicios de AWS específicos replicar funciones de Lambda en Regiones de AWS y permitir que CloudWatch utilice archivos de registro de CloudFront.

Permisos de IAM necesarios para asociar funciones de Lambda@Edge con distribuciones de CloudFront

Además de los permisos de IAM necesarios para Lambda, necesita los siguientes permisos para asociar funciones de Lambda a las distribuciones de CloudFront:

- `lambda:GetFunction`: concede permisos para obtener información de configuración para la función de Lambda y una URL prefirmada para descargar un archivo `.zip` que contiene la función.
- `lambda:EnableReplication*`: concede permisos a la política de recursos de modo que el servicio de replicación de Lambda pueda obtener una configuración y un código de función.
- `lambda:DisableReplication*`: concede permisos a la política de recursos de modo que el servicio de replicación de Lambda pueda eliminar la función.

> **Important**
>
> Debe agregar el asterisco (`*`) al final de las acciones `lambda:EnableReplication*` y `lambda:DisableReplication*`.

- Para el recurso, especifique el ARN de la versión de la función que desea ejecutar cuando se produzca un evento de CloudFront, como en el ejemplo siguiente:

  `arn:aws:lambda:us-east-1:123456789012:function:TestFunction:2`

- `iam:CreateServiceLinkedRole`: concede permiso para crear un rol vinculado a un servicio que utiliza Lambda@Edge para replicar funciones de Lambda en CloudFront. Después de configurar Lambda@Edge por primera vez, el rol vinculado a un servicio se crea automáticamente. No es necesario agregar este permiso a otras distribuciones que utilizan Lambda@Edge.

- `cloudfront:UpdateDistribution` o `cloudfront:CreateDistribution`: concede permiso para actualizar o crear una distribución.

Para obtener más información, consulte los temas siguientes:

- Identity and Access Management para Amazon CloudFront
- Permisos de acceso a recursos de Lambda en la Guía para desarrolladores de AWS Lambda

Rol de ejecución de funciones para las entidades principales del servicio

Debe crear un rol de IAM que las entidades principales de servicio `lambda.amazonaws.com` y `edgelambda.amazonaws.com` puedan asumir cuando ejecuten su función.

> **Tip**
>
> Cuando crea la función en la consola de Lambda, puede elegir crear un nuevo rol de ejecución utilizando una plantilla de políticas de AWS. En este paso, se agregan automáticamente los permisos de Lambda@Edge necesarios para ejecutar la función. Consulte el Paso 5 del tutorial: creación de una función de Lambda@Edge sencilla.

Para obtener más información sobre cómo crear un rol de IAM manualmente, consulte Creación de roles y asociación de políticas (consola) en la Guía del usuario de IAM.

Example Ejemplo: Política de confianza de rol

Puede agregar este rol en la pestaña Relación de confianza en la consola de IAM. No agregue esta política en la pestaña Permisos.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "lambda.amazonaws.com",
               "edgelambda.amazonaws.com"
            ]
         },
         "Action": "sts:AssumeRole"
      }
   ]
}
```

Para obtener más información sobre los permisos que debe conceder al rol de ejecución, consulte Permisos de acceso a recursos de Lambda en la Guía para desarrolladores de AWS Lambda.

> **Notas**
>
> - De forma predeterminada, siempre que un evento de CloudFront desencadene una función de Lambda, los datos se escriben en CloudWatch Logs. Si desea utilizar estos registros, el rol de ejecución necesita permiso para escribir datos en CloudWatch Logs. Puede utilizar la política predefinida AWSLambdaBasicExecutionRole para conceder permisos al rol de ejecución.
>
> Para obtener más información acerca de Registros de CloudWatch, consulte the section called “Registros de funciones perimetrales”.
> - Si el código de la función de Lambda tiene acceso a otros recursos de AWS, como, por ejemplo, la lectura de un objeto de un bucket de S3, el rol de ejecución necesita permiso para realizar esa acción.

Roles vinculados a servicios para Lambda@Edge

Lambda@Edge utiliza roles vinculados a servicios de IAM. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un servicio. Los roles vinculados a servicios están predefinidos por el servicio e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Lambda@Edge usa los siguientes roles vinculados a servicios de IAM:

- AWSServiceRoleForLambdaReplicator – Lambda@Edge utiliza este rol para permitir que Lambda@Edge replique funciones en Regiones de AWS.

  Cuando se agrega un desencadenador de Lambda@Edge por primera vez en CloudFront, se crea automáticamente un rol denominado AWSServiceRoleForLambdaReplicator para permitir que Lambda@Edge replique funciones en Regiones de AWS. Este rol es necesario para utilizar las funciones de Lambda@Edge. El ARN del rol AWSServiceRoleForLambdaReplicator tiene el aspecto del siguiente ejemplo:

  ```
  arn:aws:iam::123456789012:role/aws-service-role/
  replicator.lambda.amazonaws.com/AWSServiceRoleForLambdaReplicator
  ```

- AWSServiceRoleForCloudFrontLogger – CloudFront utiliza este rol para insertar archivos de registro en CloudWatch. Puede usar archivos de registro para depurar los errores de validación de Lambda@Edge.

  El rol AWSServiceRoleForCloudFrontLogger se crea automáticamente al agregar una asociación de función de Lambda@Edge para permitir que CloudFront envíe archivos de registro de errores de Lambda@Edge a CloudWatch. El ARN del rol AWSServiceRoleForCloudFrontLogger tiene este aspecto:

  ```
  arn:aws:iam::account_number:role/aws-service-role/
  logger.cloudfront.amazonaws.com/AWSServiceRoleForCloudFrontLogger
  ```

Los roles vinculados a servicios simplifican la configuración y el uso de Lambda@Edge porque no será necesario añadir manualmente los permisos necesarios. Lambda@Edge define los permisos de sus roles vinculados a servicios y solo Lambda@Edge puede asumir estos roles. Los permisos definidos incluyen la política de confianza y la política de permisos. No se puede adjuntar la política de permisos a ninguna otra entidad de IAM.

Debe eliminar los recursos de CloudFront o de Lambda@Edge asociados para poder eliminar un rol vinculado a servicio. Esto ayuda a proteger sus recursos de Lambda@Edge de modo que no elimine un rol vinculado a un servicio que sigue siendo necesario para obtener acceso a los recursos activos.

Para obtener más información acerca de los roles vinculados a servicios, consulte Roles vinculados a servicios para CloudFront.

Permisos de roles vinculados a servicios para Lambda@Edge

Lambda@Edge utiliza dos roles vinculados a servicios, denominados AWSServiceRoleForLambdaReplicator y AWSServiceRoleForCloudFrontLogger. En las siguientes secciones se describen los permisos de cada uno de estos roles.

Contenido

- Permisos del rol vinculado a servicio para el replicador de Lambda
- Permisos de rol vinculado a servicio para el registrador de CloudFront

Permisos del rol vinculado a servicio para el replicador de Lambda

Este rol vinculado a servicio permite que Lambda replique las funciones de Lambda@Edge en Regiones de AWS.

El rol vinculado a servicios AWSServiceRoleForLambdaReplicator confía en el servicio `replicator.lambda.amazonaws.com` para asumir el rol.

La política de permisos del rol permite que Lambda@Edge realice las siguientes acciones en los recursos especificados:

- `lambda:CreateFunction` en `arn:aws:lambda:*:*:function:*`
- `lambda:DeleteFunction` en `arn:aws:lambda:*:*:function:*`
- `lambda:DisableReplication` en `arn:aws:lambda:*:*:function:*`
- `iam:PassRole` en `all AWS resources`
- `cloudfront:ListDistributionsByLambdaFunction` en `all AWS resources`

Permisos de rol vinculado a servicio para el registrador de CloudFront

Este rol vinculado a un servicio permite que CloudFront envíe archivos de registro a CloudWatch de modo que pueda depurar errores de validación de Lambda@Edge.

El rol vinculado a servicios AWSServiceRoleForCloudFrontLogger confía en el servicio `logger.cloudfront.amazonaws.com` para asumir el rol.

La política de permisos de rol permite que Lambda@Edge realice las siguientes acciones en el recurso de `arn:aws:logs:*:*:log-group:/aws/cloudfront/*` especificado:

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Debe configurar permisos para permitir que una entidad de IAM (como un usuario, grupo o rol) elimine los roles vinculados a servicios de Lambda@Edge. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de roles vinculados a servicios para Lambda@Edge

Normalmente no es necesario crear manualmente los roles vinculados a servicios para Lambda@Edge. El servicio crea los roles automáticamente en los siguientes casos:

- Cuando se crea un desencadenador por primera vez, el servicio crea el rol AWSServiceRoleForLambdaReplicator (si aún no existe). Este rol permite que Lambda replique las funciones de Lambda@Edge en Regiones de AWS.

  Si elimina el rol vinculado a servicio, el rol se creará de nuevo al añadir un nuevo disparador para Lambda@Edge en una distribución.
- Cuando se actualiza o se crea una distribución de CloudFront que tiene una asociación de Lambda@Edge, el servicio crea un rol AWSServiceRoleForCloudFrontLogger (si no existe ya). Este rol permite a CloudFront insertar sus archivos de registro en CloudWatch.

  Si elimina el rol vinculado al servicio, el rol se creará de nuevo al actualizar o crear una distribución de CloudFront que tiene una asociación de Lambda@Edge.

Para crear manualmente estos roles vinculados a servicios, ejecute los siguientes comandos de la AWS Command Line Interface (AWS CLI):

Para crear el rol de AWSServiceRoleForLambdaReplicator

- Ejecute el siguiente comando.

```
aws iam create-service-linked-role --aws-service-name
 replicator.lambda.amazonaws.com
```

Para crear el rol de AWSServiceRoleForCloudFrontLogger

- Ejecute el siguiente comando.

```
aws iam create-service-linked-role --aws-service-name
 logger.cloudfront.amazonaws.com
```

Edición de roles vinculados a servicios de Lambda@Edge

Lambda@Edge no permite editar los roles vinculados a servicios AWSServiceRoleForLambdaReplicator o AWSServiceRoleForCloudFrontLogger. Una vez que el servicio ha creado un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede utilizar IAM para editar la descripción

del rol. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones de AWS compatibles con roles vinculados a servicios de Lambda@Edge

CloudFront admite el uso de roles vinculados a servicios para Lambda@Edge en las siguientes Regiones de AWS:

- Este de EE. UU. (Norte de Virginia) – `us-east-1`
- Este de EE. UU. (Ohio) – `us-east-2`
- Oeste de EE. UU. (Norte de California) – `us-west-1`
- Oeste de EE. UU. (Oregón) – `us-west-2`
- Asia-Pacífico (Bombay) – `ap-south-1`
- Asia-Pacífico (Seúl) – (`ap-northeast-2`)
- Asia Pacífico (Singapur) – `ap-southeast-1`
- Asia-Pacífico (Sídney) – `ap-southeast-2`
- Asia-Pacífico (Tokio) – `ap-northeast-1`
- Europa (Fráncfort) – `eu-central-1`
- Europa (Irlanda) – `eu-west-1`
- Europa (Londres) – `eu-west-2`
- América del Sur (São Paulo) – `sa-east-1`

Escritura y creación de una función de Lambda@Edge

Para usar Lambda@Edge, debe escribir el código de la función de AWS Lambda. Para ayudarle a escribir funciones de Lambda@Edge, consulte los siguientes recursos:

- Estructura de eventos de Lambda@Edge: comprensión de la estructura de eventos que se va a utilizar con Lambda@Edge.
- Funciones de ejemplo de Lambda@Edge: funciones de ejemplo, como pruebas A/B y generación de un redireccionamiento HTTP.

El modelo de programación para utilizar Node.js o Python con Lambda@Edge es el mismo que para utilizar Lambda en una Región de AWS. Para obtener más información, consulte Creación de

funciones de Lambda con Node.js o Creación de funciones de Lambda con Python en la Guía del desarrollador de AWS Lambda.

En su función de Lambda@Edge, incluya el parámetro `callback` y devuelva el objeto correspondiente para eventos de solicitud o de respuesta:

- Eventos de solicitud: incluya el objeto `cf.request` en la respuesta.

  Si está generando una respuesta, incluya el objeto `cf.response` en ella. Para obtener más información, consulte Generación de respuestas HTTP en los desencadenadores de solicitud.
- Eventos de respuesta: incluya el objeto `cf.response` en la respuesta.

Tras escribir su propio código o utilizar uno de los ejemplos, cree la función en Lambda. Para crear una función o editar una ya existente, consulte los temas siguientes:

Temas

- Creación de una función de Lambda@Edge
- Edición de una función de Lambda

Después de crear la función en Lambda, se configura Lambda para ejecutar la función según los eventos de CloudFront específicos, que se denominan desencadenadores. Para obtener más información, consulte Adición de desencadenadores para una función de Lambda@Edge.

Creación de una función de Lambda@Edge

Para configurar AWS Lambda para que ejecute funciones Lambda basadas en eventos de CloudFront, siga este procedimiento.

Para crear una función de Lambda@Edge

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.
2. Si ya tiene una o varias funciones de Lambda, elija Create function (Crear función).

   Si no tiene ninguna función, elija Get Started Now (Comenzar ahora).
3. En la lista Región de la parte superior de la página, elija US East (N. Virginia) (EE. UU. Este (Norte de Virginia)).

4. Cree una función mediante su propio código o cree una función a partir de un proyecto de CloudFront.

   - Para crear una función utilizando su propio código, elija Author from scratch (Crear desde cero).
   - Para mostrar una lista de esquemas de CloudFront, ingrese cloudfront en el campo de filtro y, a continuación, elija Intro.

     Si encuentra un proyecto que desee utilizar, elija el nombre del proyecto.

5. En la sección Basic information (Información básica), especifique los siguientes valores:

   a. Nombre: escriba un nombre para la función.

   b. Rol: para empezar rápidamente, seleccione Crear un rol nuevo desde las plantillas. También puede seleccionar Elegir un rol existente o Crear un rol personalizado y, a continuación, seguir las indicaciones para completar la información de esta sección.

   c. Nombre del rol: escriba un nombre para el rol.

   d. Plantillas de políticas: elija Permisos básicos de Edge Lambda.

6. Si eligió Author from scratch (Crear desde cero) en el paso 4, vaya al paso 7.

   Si eligió un proyecto en el paso 4, la sección cloudfront le permite crear un desencadenador, que asocia esta función con una memoria caché en una distribución de CloudFront y un evento de CloudFront. Le recomendamos que elija Remove (Eliminar) en este punto, por lo que no habrá un disparador para la función cuando esta se cree. Podrá añadir disparadores más adelante.

   > **Tip**
   >
   > Le recomendamos que pruebe y depure la función antes de agregar desencadenadores. Si agrega un desencadenador ahora, la función se ejecutará en cuanto la cree y terminará de replicarse en las ubicaciones de AWS en todo el mundo; además, se implementará la distribución correspondiente.

7. Elija Create function (Crear función).

   Lambda crea dos versiones de su función: $LATEST y Version 1. Solo puede editar la versión $LATEST, pero la consola muestra inicialmente Version 1.

8. Para editar la función, elija Version 1 (Versión 1) cerca de la parte superior de la página, bajo el ARN de la función. A continuación, en la pestaña Versions (Versiones), elija $LATEST.

(Si abandona la función y vuelve a ella más tarde, el botón de etiqueta será Qualifiers (Cualificadores)).

9. En la pestaña Configuration (Configuración), elija el valor correspondiente para Code entry type (Tipo de entrada de código). A continuación, siga las instrucciones para editar o cargar el código.
10. En Runtime (Tiempo de ejecución), elija el valor según el código de la función.
11. En la sección Tags (Etiquetas), añada todas las etiquetas aplicables.
12. Elija Actions (Acciones) y, a continuación, Publish new version (Publicar nueva versión).
13. Ingrese una descripción para la nueva versión de la función.
14. Elija Publish.
15. Pruebe y depure la función. Para obtener más información sobre las pruebas en la consola de Lambda, consulte Invocar una función de Lambda con la consola en la Guía para desarrolladores de AWS Lambda.
16. Cuando esté listo para que la función se ejecute para eventos de CloudFront, publique otra versión y edite la función para agregar desencadenadores. Para obtener más información, consulte Adición de desencadenadores para una función de Lambda@Edge.

Edición de una función de Lambda

Después de crear una función de Lambda@Edge, puede utilizar la consola de Lambda para editarla.

Notas

- La versión original se denomina $LATEST.
- Solo puede editar la versión $LATEST.
- Cada vez que edite la versión $LATEST, debe publicar una nueva versión numerada.
- No puede crear disparadores para $LATEST.
- Cuando se publica una nueva versión de una función, Lambda no copia automáticamente los desencadenadores de la versión anterior a la nueva. Debe reproducir los disparadores para la nueva versión.
- Cuando se agrega un desencadenador para un evento de CloudFront a una función, si ya existe un desencadenador para la misma distribución, comportamiento de la caché y evento para una versión anterior de la misma función, Lambda lo elimina de esta versión anterior.

- Después de realizar actualizaciones a una distribución de CloudFront, como agregar desencadenadores, debe esperar que los cambios se propaguen a ubicaciones de borde antes de que las funciones que ha especificado en los desencadenadores funcionen.

Para editar una función de Lambda

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.
2. En la lista Región de la parte superior de la página, elija US East (N. Virginia) (EE. UU. Este (Norte de Virginia)).
3. En la lista de funciones, elija el nombre de la función.

   De forma predeterminada, la consola muestra la versión $LATEST. Puede ver las versiones anteriores (elija Qualifiers (Cualificadores)), pero solo puede editar $LATEST.
4. En la pestaña Code (Código), en Code entry type (Tipo de entrada de código), elija si desea editar el código en el navegador, cargar un archivo .zip o cargar un archivo desde Amazon S3.
5. Elija Save (Guardar) o Save and test (Guardar y probar).
6. Elija Actions (Acciones) y, a continuación, Publish new version (Publicar nueva versión).
7. En el cuadro de diálogo Publish new version from $LATEST (Publicar una nueva versión desde $LATEST), introduzca una descripción de la nueva versión. Esta descripción aparece en la lista de versiones, junto con un número de versión generado de forma automática.
8. Elija Publish.

   La nueva versión se convierte automáticamente la versión más reciente. El número de versión aparece en Versión en la esquina superior izquierda de la página.

   > **Note**
   >
   > Si no ha agregado aún desencadenadores para la función, consulte Adición de desencadenadores para una función de Lambda@Edge.

9. Elija la pestaña Desencadenadores.
10. Elija Add trigger (Añadir disparador).
11. En el cuadro de diálogo Add trigger (Agregar desencadenador), elija el cuadro con puntos y, a continuación, CloudFront.

> **Note**
>
> Si ya ha creado uno o varios desencadenadores para una función, CloudFront es el servicio predeterminado.

12. Especifique los siguientes valores para indicar cuándo desea que se ejecute la función de Lambda.
    a. ID de distribución: elija el ID de la distribución donde desea añadir el desencadenador.
    b. Comportamiento de caché: elija el comportamiento de la caché que especifica los objetos en los que desea ejecutar la función.
    c. Evento de CloudFront: elija el evento de CloudFront que provoca la ejecución de la función.
    d. Activar desencadenador y replicar: seleccione esta casilla para que Lambda replique la función en las Regiones de AWS en todo el mundo.
13. Elija Submit.
14. Para añadir más disparadores para esta función, repita los pasos del 10 al 13.

Para obtener más información sobre las pruebas y la depuración de la función en la consola de Lambda, consulte Invocar una función de Lambda con la consola en la Guía para desarrolladores de AWS Lambda.

Cuando esté listo para que la función se ejecute para eventos de CloudFront, publique otra versión y edite la función para agregar desencadenadores. Para obtener más información, consulte Adición de desencadenadores para una función de Lambda@Edge.

Adición de desencadenadores para una función de Lambda@Edge

Un desencadenador de Lambda@Edge es una combinación de una distribución de CloudFront, un comportamiento de la caché y un evento que provoca la ejecución de una función. Por ejemplo, puede crear un desencadenador que provoque la ejecución de la función cuando CloudFront reciba una solicitud de un lector para un comportamiento de la caché específico que haya configurado para la distribución. Puede especificar uno o más desencadenadores de CloudFront.

> **Tip**
>
> Al crear una distribución de CloudFront, debe especificar la configuración que indica a CloudFront cómo responder al recibir distintas solicitudes. La configuración predeterminada

se denomina comportamiento de la caché predeterminado para la distribución. Puede configurar más comportamientos de la caché que definen cómo responde CloudFront en circunstancias específicas, por ejemplo, cuando recibe una solicitud para un tipo de archivo específico. Para obtener más información, consulte Configuración del comportamiento de la caché.

Cuando crea por primera vez una función de Lambda, solo puede especificar un desencadenador. Pero se pueden agregar más desencadenadores a la misma función más adelante con la consola de Lambda o editando la distribución en la consola de CloudFront.

- La consola de Lambda funciona bien si desea agregar más desencadenadores a una función para la misma distribución de CloudFront.
- La consola de CloudFront puede ser mejor si desea agregar desencadenadores para varias distribuciones, ya que es más sencillo encontrar la distribución que desea actualizar. También puede actualizar otros ajustes de CloudFront simultáneamente.

Temas

- Eventos de CloudFront que pueden desencadenar una función de Lambda@Edge
- Elección del evento para desencadenar la función
- Adición de desencadenadores a una función de Lambda@Edge

Eventos de CloudFront que pueden desencadenar una función de Lambda@Edge

Para cada comportamiento de la caché de una distribución de Amazon CloudFront, puede agregar hasta cuatro desencadenadores (asociaciones) que harán que se ejecute una función de Lambda cuando se produzcan determinados eventos de CloudFront. Los desencadenadores de CloudFront pueden basarse en uno de los cuatro eventos de CloudFront que se muestran en el siguiente diagrama.

El eventos de CloudFront que pueden utilizarse para activar funciones de Lambda@Edge son los siguientes:

Solicitud del lector

La función se ejecuta cuando CloudFront recibe una solicitud de un lector y antes de comprobar si el objeto solicitado está en la caché de CloudFront.

La función no se ejecuta en los casos siguientes:

- Cuando se devuelve una página de error personalizada.
- Cuando CloudFront redirige automáticamente una solicitud HTTP a HTTPS (cuando el valor de Política de protocolo para lectores es Redirigir HTTP a HTTPS).

Solicitud del origen

La función se ejecuta solo cuando CloudFront reenvía una solicitud a su origen. Cuando el objeto solicitado está en la caché de CloudFront, la función no se ejecuta.

Respuesta del origen

La función se ejecuta después de que CloudFront recibe una respuesta del origen y antes de almacenar el objeto en caché en la respuesta. Tenga en cuenta que la función se ejecuta aunque el origen devuelva un error.

La función no se ejecuta en los casos siguientes:

- Cuando el archivo solicitado está en la caché de CloudFront y no ha caducado.
- Cuando la respuesta se genera a partir de una función activada por un evento de solicitud al origen.

Respuesta del lector

La función se ejecuta antes de devolver el archivo solicitado al espectador. Tenga en cuenta que la función se ejecuta independientemente de si el archivo ya está en la caché de CloudFront.

La función no se ejecuta en los casos siguientes:

- Cuando el origen devuelve un código de estado HTTP 400 o superior.
- Cuando se devuelve una página de error personalizada.
- Cuando la respuesta se genera a partir de una función activada por un evento de solicitud del espectador.
- Cuando CloudFront redirige automáticamente una solicitud HTTP a HTTPS (cuando el valor de Política de protocolo para lectores es Redirigir HTTP a HTTPS).

Si añade varios disparadores al mismo comportamiento de la caché, puede utilizarlos para ejecutar la misma función o distintas funciones para cada disparador. También puede asociar la misma función a más de una distribución.

> **Note**
>
> Cuando un evento de CloudFront desencadena la ejecución de una función de Lambda, la función debe finalizar antes de que CloudFront pueda continuar.
> Por ejemplo, si una función Lambda se activa por medio de un evento de solicitud del espectador de CloudFront, CloudFront no devolverá una respuesta al lector ni reenviará la solicitud al origen hasta que la función Lambda termine de ejecutarse.
> Esto significa que cada solicitud que desencadena una función de Lambda aumenta la latencia de la solicitud, por lo que es conveniente que la función se ejecute con la mayor rapidez posible.

Elección del evento para desencadenar la función

A la hora de decidir qué evento de CloudFront utilizar para desencadenar una función de Lambda, tenga en cuenta lo siguiente:

Quiero que CloudFront almacene en caché los objetos modificados por una función de Lambda

Para almacenar en caché un objeto modificado por una función de Lambda para que CloudFront pueda enviarlo desde la ubicación periférica la próxima vez que se solicite, utilice el evento de solicitud de origen o respuesta de origen.

Esto reduce la carga en el origen, la latencia de las solicitudes posteriores y los costos de invocación de Lambda@Edge en las solicitudes posteriores.

Por ejemplo, si desea agregar, eliminar o cambiar los encabezados de los objetos devueltos por el origen y que CloudFront almacene el resultado en caché, utilice el evento de respuesta del origen.

Deseo que la función se ejecute por cada solicitud

Para ejecutar la función para cada solicitud que CloudFront reciba para la distribución, utilice los eventos de solicitud del lector o de respuesta del lector.

Los eventos de solicitud al origen y respuesta del origen ocurren solo cuando un objeto solicitado no se almacena en caché en una ubicación de borde y CloudFront reenvía una solicitud al origen.

Quiero que la función cambie la clave de caché

Para cambiar un valor que está utilizando como base para el almacenamiento en caché, utilice el evento de solicitud del lector.

Por ejemplo, si una función cambia la URL para incluir una abreviatura de idioma en la ruta (por ejemplo, porque el usuario había elegido su idioma en una lista desplegable), utilice el evento de solicitud del espectador:

- URL en la solicitud del lector: https://example.com/en/index.html
- URL si la solicitud viene de una dirección IP en Alemania: https://example.com/de/index.html

También puede utilizar el evento de solicitud del espectador si está almacenando en caché en función de cookies o encabezados de solicitudes.

> **Note**
>
> Si la función cambia cookies o encabezados, configure CloudFront para reenviar la parte aplicable de la solicitud al origen. Para obtener más información, consulte los temas siguientes:

- Almacenamiento en caché de contenido en función de cookies
- Almacenamiento en caché de contenido en función de encabezados de solicitud

La función afecta a la respuesta del origen

Para cambiar la solicitud para que afecte a la respuesta del origen, utilice el evento de solicitud de origen.

Normalmente, la mayoría de los eventos de solicitud de lectores no se reenvían al origen. CloudFront responde a una solicitud con un objeto que ya está en la caché periférica. Si la función modifica la solicitud basándose en un evento de solicitud al origen, CloudFront almacena en caché la respuesta a la solicitud al origen modificada.

Adición de desencadenadores a una función de Lambda@Edge

Puede utilizar la consola de AWS Lambda o la consola de Amazon CloudFront para agregar un desencadenador a su función de Lambda@Edge.

> **Important**
>
> Solo puede crear desencadenadores para las versiones numeradas de su función (no para las $LATEST).

Lambda console

Agregación de desencadenadores para eventos de CloudFront a una función de Lambda@Edge

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.
2. En la lista Región de la parte superior de la página, elija US East (N. Virginia) (EE. UU. Este (Norte de Virginia)).
3. En la página Functions (Funciones), elija el nombre de la función a la que desee añadir disparadores.
4. En la página Información general de la función, elija la pestaña Versiones.
5. Elija la versión a la que desea añadir disparadores.

Una vez elegida una versión, el nombre del botón cambia a Version: $LATEST (Versión: $LATEST) o Version: número de versión.

6. Elija la pestaña Desencadenadores.
7. Elija Add trigger (Añadir disparador).
8. En Configuración del desencadenador, elija Seleccionar un origen, introduzca **`cloudfront`** y, a continuación, elija CloudFront.

> **Note**
>
> Si ya ha creado uno o varios desencadenadores, CloudFront es el servicio predeterminado.

9. Especifique los siguientes valores para indicar cuándo desea que se ejecute la función de Lambda.

   a. Distribución: elija la distribución a la que desee agregar el desencadenador.

   b. Comportamiento de caché: elija el comportamiento de la caché que especifica los objetos en los que desea ejecutar la función.

   > **Note**
   >
   > Si especifica * como comportamiento de la caché, la función de Lambda se implementa con el comportamiento predeterminado de la caché.

   c. Evento de CloudFront: elija el evento de CloudFront que provoca la ejecución de la función.

   d. Incluir cuerpo: marque esta casilla si desea obtener acceso al cuerpo de la solicitud en la función.

   e. Confirmación de la implementación en Lambda@Edge: seleccione esta casilla para que AWS Lambda replique la función en las Regiones de AWS de forma global.

10. Elija Agregar.

La función comienza a procesar solicitudes de los eventos de CloudFront especificados cuando se implementa la distribución de CloudFront actualizada. Para determinar si una distribución se ha implementado, elija Distribuciones en el panel de navegación. Cuando

una distribución se implementa, el valor de la columna Estado de la distribución cambia de Implementando a la fecha y hora de la implementación.

CloudFront console

Agregación de desencadenadores para eventos de CloudFront a una función de Lambda@Edge

1. Identifique el ARN de la función de Lambda para la que desee añadir disparadores:

   a. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.

   b. En la lista de regiones de la parte superior de la página, elija US East (N. Virginia) (EE. UU. Este (Norte de Virginia)).

   c. En la lista de funciones, seleccione el nombre de la función a la que desee añadir disparadores.

   d. En la página Información general de la función, elija la pestaña Versiones y seleccione la versión numerada a la que desea agregar desencadenadores.

   e. Elija el botón Copiar ARN para copiar el ARN en el portapapeles. El ARN de la función de Lambda tiene un aspecto similar al siguiente:

      ```
      arn:aws:lambda:us-east-1:123456789012:function:TestFunction:2
      ```

      El número del final (en este ejemplo es 2) es el número de versión de la función.

2. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.

3. En la lista de distribuciones, seleccione el ID de la distribución a la que desee añadir disparadores.

4. Elija la pestaña Behaviors (Comportamientos).

5. Seleccione comportamiento de caché al que desee agregar desencadenadores y, a continuación, elija Editar.

6. En Asociaciones de función, en la lista Tipo de función, elija Lambda@Edge para cuando desee que se ejecute la función: para solicitudes de lector, respuestas de lector, solicitudes de origen o respuestas de origen.

   Para obtener más información, consulte Elección del evento para desencadenar la función.

7. En el cuadro de texto ARN/nombre de la función, pegue el ARN de la función de Lambda que desea ejecutar cuando se produzca el evento elegido. Este es el valor que ha copiado de la consola de Lambda.
8. Seleccione Incluir cuerpo si desea obtener acceso al cuerpo de la solicitud en la función.

   Si simplemente desea reemplazar el cuerpo de la solicitud, no necesita seleccionar esta opción.
9. Para ejecutar la misma función con más tipos de eventos, repita los pasos 6 y 7.
10. Seleccione Save changes (Guardar cambios).
11. Para agregar desencadenadores a más comportamientos de caché para esa distribución, repita los pasos del 5 al 10.

    La función comienza a procesar solicitudes de los eventos de CloudFront especificados cuando se implementa la distribución de CloudFront actualizada. Para determinar si una distribución se ha implementado, elija Distribuciones en el panel de navegación. Cuando una distribución se implementa, el valor de la columna Estado de la distribución cambia de Implementando a la hora y fecha de la implementación.

Prueba y depuración de funciones de Lambda@Edge

Es importante probar el código de la función de Lambda@Edge de forma independiente, para asegurarse de que completa la tarea prevista, y realizar pruebas de integración, para asegurarse de que la funciona correctamente con CloudFront.

Durante las pruebas de integración o una vez implementada su función, es posible que deba depurar errores de CloudFront, como errores HTTP 5xx. Los errores pueden ser una respuesta no válida que devuelve la función de Lambda, errores de ejecución cuando se desencadena la función o errores debido a limitación controlada de ejecución por parte del servicio de Lambda. En las secciones de este tema se explican estrategias para determinar qué tipo de error es la causa del problema y, a continuación, se ofrecen pasos que puede seguir para corregir el problema.

> **Note**
>
> Al examinar las métricas o los archivos de registro de CloudWatch durante la solución de problemas, tenga en cuenta que se muestran o almacenan en la Región de AWS más cercana a la ubicación donde se ejecutó la función. Por lo tanto, si tiene un sitio web o una aplicación web con usuarios en el Reino Unido y tiene una función de Lambda asociada a

su distribución, por ejemplo, debe cambiar la región para ver las métricas o los archivos de registro de CloudWatch para la Región de AWS de Londres. Para obtener más información, consulte the section called “Determinación de la región de Lambda@Edge”.

Temas

- Prueba de funciones de Lambda@Edge
- Identificación de errores de funciones de Lambda@Edge en CloudFront
- Solución de problemas de respuestas no válidas de funciones de Lambda@Edge (errores de validación)
- Solución de problemas de errores de ejecución de funciones de Lambda@Edge
- Determinación de la región de Lambda@Edge
- Determinación de si la cuenta inserta registros en CloudWatch

Prueba de funciones de Lambda@Edge

Hay dos pasos para probar la función de Lambda: pruebas independientes y pruebas de integración.

Probar la funcionalidad independiente

Antes de agregar su función de Lambda a CloudFront, asegúrese de probar primero la funcionalidad mediante las capacidades de prueba de la consola de Lambda o mediante otros métodos. Para obtener más información sobre las pruebas en la consola de Lambda, consulte Invocar una función de Lambda con la consola en la Guía para desarrolladores de AWS Lambda.

Probar la operación de la función en CloudFront

Es importante realizar pruebas de integración, donde la función está asociada a una distribución y se ejecuta en función de un evento de CloudFront. Asegúrese de que la función se activa para el evento adecuado y devuelve una respuesta que es válida y correcta para CloudFront. Por ejemplo, asegúrese de que la estructura del evento es correcta, que solo se incluyen encabezados válidos, etc.

Mientras realiza la iteración en las pruebas de integración con la función en la consola de Lambda, consulte los pasos que se indican en el tutorial de Lambda@Edge a medida que modifica el código o cambia el desencadenador de CloudFront que llama a su función. Por ejemplo, asegúrese de que está trabajando en una versión numerada de su función, tal y como

se describe en este paso del tutorial: Paso 4: Agregue un desencadenador de CloudFront para ejecutar la función.

A medida que realiza cambios y los implementa, tenga en cuenta que pasarán varios minutos hasta que su función actualizada y los desencadenadores de CloudFront se repliquen en todas las regiones. Esto suele hacerse en unos minutos, pero puede tardar hasta 15 minutos.

Para comprobar si la replicación ha terminado, vaya a la consola de CloudFront y consulte la distribución.

Comprobación de la finalización de la implementación de la replicación

1. Abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija el nombre de la distribución.
3. Compruebe que el estado de la distribución cambia de En curso a Implementada, lo que significa que la función se ha replicado. A continuación, siga los pasos de la sección siguiente para verificar el funcionamiento de la función.

Tenga en cuenta que las pruebas en la consola solo validan la lógica de la función, pero no aplican cuotas (antes denominadas límites) de servicio específicas de Lambda@Edge.

Identificación de errores de funciones de Lambda@Edge en CloudFront

Una vez que haya verificado que la lógica de la función funciona correctamente, es posible que sigan apareciendo errores HTTP 5xx cuando la función se ejecuta en CloudFront. Los errores HTTP 5xx se pueden devolver por diversas razones, que puede incluir errores de las funciones de Lambda u otros problemas en CloudFront.

- Si utiliza las funciones de Lambda@Edge, puede utilizar gráficos en la consola de CloudFront para ayudar a localizar lo que está provocando el error y, a continuación, trabajar para solucionarlo. Por ejemplo, puede ver si los errores HTTP 5xx están provocados por CloudFront o funciones de Lambda y, a continuación, en el caso de funciones específicas, puede ver los archivos de registro relacionados para investigar el problema.
- Para solucionar los errores HTTP en general en CloudFront, consulte los pasos de solución de problemas en el siguiente tema: Solución de problemas de códigos de estado de respuesta a errores en CloudFront.

Causa de los errores de función de Lambda@Edge en CloudFront

Existen varias razones por las que una función de Lambda puede provocar un error HTTP 5xx y los pasos de solución de problemas que lleve a cabo dependerán del tipo de error. Los errores pueden clasificarse como los siguientes:

Un error de ejecución de la función de Lambda

Un error de ejecución se produce cuando CloudFront no obtiene ninguna respuesta de Lambda porque hay excepciones no controladas en la función o hay un error en el código. Por ejemplo, si el código incluye callback(Error).

Se devuelve a CloudFront una respuesta de función de Lambda no válida

Después de ejecutar la función, CloudFront recibe una respuesta de Lambda. Se devuelve un error si la estructura de objetos de la respuesta no se ajusta a la Estructura de eventos de Lambda@Edge o si la respuesta contiene encabezados no válidos u otros campos no válidos.

La ejecución en CloudFront se limita debido a las cuotas de servicio de Lambda (anteriormente conocidas como límites)

El servicio de Lambda limita las ejecuciones en cada región y devuelve un error si se supera la cuota. Para obtener más información, consulte Cuotas de Lambda@Edge.

Cómo determinar el tipo de error

Para ayudarle a decidir dónde centrarse a medida que depura y trabaja para resolver errores que devuelve CloudFront, es útil identificar por qué CloudFront devuelve un error HTTP. Para empezar, puede usar los gráficos proporcionados en la sección Monitoring (Monitoreo) de la consola de CloudFront en la Consola de administración de AWS. Para empezar, puede usar los gráficos proporcionada en la sección Monitoring (Monitoreo) de la consola de CloudFront, consulte Supervisión de métricas de CloudFront con Amazon CloudWatch.

Los siguientes gráficos pueden resultar especialmente útiles cuando desea realizar un seguimiento de los errores devueltos por orígenes o por una función de Lambda y para acotar el tipo de problema cuando se trata de un error de una función de Lambda.

Gráfico de índices de error

Uno de los gráficos que puede ver en la pestaña Overview (Descripción general) de cada una de las distribuciones es un gráfico de Error rates (Índices de error). Este gráfico muestra la tasa

de errores como porcentaje de las solicitudes totales próximas a su distribución. El gráfico se muestra la tasa de error total, errores 4xx totales, errores 5xx totales y errores 5xx totales de funciones Lambda. En función del tipo de error y del volumen, puede seguir los pasos para investigar y solucionar la causa.

- Si ve errores de Lambda, puede seguir investigando mirando los tipos de error específicos que devuelve la función. La pestaña Lambda@Edge errors (Errores de Lambda@Edge) incluye gráficos que clasifican los errores de función por tipo para ayudar a identificar el problema para una función específica.
- Si ve errores de CloudFront, puede solucionar el problema y trabajar para corregir los errores de origen o cambiar la configuración de CloudFront. Para obtener más información, consulte Solución de problemas de códigos de estado de respuesta a errores en CloudFront.

Gráficos de respuestas de función no válida y errores de ejecución

La pestaña Lambda@Edge errors (Errores de Lambda@Edge) incluye gráficos que clasifican los errores de Lambda@Edge de una distribución específica, por tipo. Por ejemplo, un gráfico muestra todos los errores de ejecución por Región de AWS.

Para facilitar la resolución de problemas, puede buscar problemas específicos abriendo y examinando los archivos de registro de funciones específicas por región.

Visualización de los archivos de registro de una función específica por región

1. En la pestaña Errores de Lambda@Edge, en Funciones de Lambda@Edge asociadas, elija el nombre de la función y, a continuación, Ver métricas.
2. A continuación, en la página con el nombre de la función, en la esquina superior derecha, seleccione Ver registros de funciones y, a continuación, elija una región.

   Por ejemplo, si ve problemas en el gráfico Errores de la región Oeste de EE. UU. (Oregón), elija esa región en la lista desplegable. Se abrirá la consola de Amazon CloudWatch.

3. En la consola de CloudWatch de esa región, en Flujos de registro, seleccione un flujo de registro para ver los eventos de la función.

Además, lea las siguientes secciones de este capítulo para obtener más recomendaciones acerca de la solución de problemas y la corrección de errores.

Gráfico de limitaciones

La pestaña Lambda@Edge errors (Errores de Lambda@Edge) incluye además un gráfico Throttles (Limitaciones). A veces, el servicio de Lambda limita las invocaciones de la función por región, si se alcanza la cuota (antes denominada límite) de simultaneidad regional. Si aparece un error limit exceeded (límite superado), su función ha alcanzado una cuota que el servicio Lambda impone a las ejecuciones en una región. Para obtener más información, incluido cómo solicitar un aumento de la cuota, consulte Cuotas de Lambda@Edge.

Para ver un ejemplo sobre cómo utilizar esta información en la solución de problemas de errores HTTP, consulte Cuatro pasos para depurar la entrega de contenido en AWS.

Solución de problemas de respuestas no válidas de funciones de Lambda@Edge (errores de validación)

Si identifica que el problema es un error de validación de Lambda, significa que su función de Lambda devuelve una respuesta no válida a CloudFront. Siga las indicaciones de esta sección para realizar los pasos que permiten revisar la función y asegurarse de que su respuesta se ajusta a los requisitos de CloudFront.

CloudFront valida la respuesta de una función de Lambda de dos maneras:

- La respuesta de Lambda debe ajustarse a la estructura de objetos necesaria. Estos son algunos ejemplos de estructura de objetos incorrecta: JSON que no se puede analizar, campos obligatorios que faltan y un objeto no válido en la respuesta. Para obtener más información, consulte Estructura de eventos de Lambda@Edge.
- La respuesta solo debe incluir valores de objetos válidos. Se producirá un error si la respuesta incluye un objeto válido pero tiene valores que no se admiten. Por ejemplo: añadir o actualizar encabezados que están en la lista negra o son de solo lectura (consulte Restricciones en funciones de borde en el tema Requisitos y restricciones en funciones Lambda), superar el tamaño máximo del cuerpo (consulte Restricciones en el tamaño de la respuesta generada en el tema Errores de respuesta de Lambda@Edge) y caracteres o valores no válidos (consulte Estructura de eventos de Lambda@Edge).

Cuando Lambda devuelve una respuesta no válida a CloudFront, los mensajes de error se escriben en los archivos de registro que CloudFront envía a CloudWatch en la región donde se ejecutó la función de Lambda. El comportamiento predeterminado es enviar los archivos de registro a CloudWatch cuando hay una respuesta no válida. Sin embargo, si asoció una función de Lambda con CloudFront antes de que se lanzara la funcionalidad, es posible que no esté habilitada para la función. Para obtener más información, consulte Determinación de si su cuenta inserta registros en CloudWatch más adelante en este tema.

CloudFront envía los archivos de registro a la región correspondiente donde se ejecutó la función, al grupo de registros asociado a la distribución. Los grupos de registros tienen el siguiente formato: `/aws/cloudfront/LambdaEdge/`*`DistributionId`*, donde *`DistributionId`* es el ID de la distribución. Para determinar la región donde se encuentran los archivos de registro de CloudWatch, consulte Determinación de la región de Lambda@Edge más adelante en este tema.

Si el error es reproducible, puede crear una nueva solicitud que produzca el error y, a continuación, buscar el ID de solicitud en una respuesta fallida de CloudFront (encabezado `X-Amz-Cf-Id`) para encontrar un error en los archivos de registro. La entrada del archivo de registro incluye información que puede ayudarle a identificar por qué se devuelve el error, y también muestra el ID de solicitud de Lambda correspondiente para que pueda analizar la causa raíz en el contexto de una única solicitud.

Si se trata de un error intermitente, puede utilizar los registros de acceso de CloudFront para encontrar el ID de una solicitud que ha generado un error y, a continuación, buscar en los registros de CloudWatch los mensajes de error correspondientes. Para obtener más información, consulte la sección anterior, Determinación del tipo de error.

Solución de problemas de errores de ejecución de funciones de Lambda@Edge

Si se trata de un error de ejecución de Lambda, puede ser útil crear declaraciones de registros para las funciones de Lambda, escribir mensajes en los archivos de registro de CloudWatch que monitorean la ejecución de la función en CloudFront y determinar si funciona según lo previsto. A continuación, puede buscar esas instrucciones en los archivos de registro de CloudWatch para verificar que la función está funcionando.

> **Note**
>
> Aunque no haya cambiado la función de Lambda@Edge, las actualizaciones del entorno de ejecución de la función de Lambda podrían afectar a esa función y devolver un error de ejecución. Para obtener más información sobre cómo probar y migrar a una versión posterior, consulte Próximas actualizaciones del entorno de ejecución de AWS Lambda y AWS Lambda@Edge.

Determinación de la región de Lambda@Edge

Para ver las regiones donde la función Lambda@Edge recibe tráfico, consulte las métricas de la función en la consola de CloudFront en la Consola de administración de AWS. Las métricas se muestran para cada región de AWS. En la misma página, puede elegir una región y ver los archivos de registro para dicha región a fin de poder investigar problemas. Debe revisar los archivos de registro de CloudWatch en la región correcta de AWS para ver los archivos de registro creados cuando CloudFront ejecutó su función de Lambda.

Para empezar, puede usar los gráficos proporcionada en la sección Monitoring (Monitoreo) de la consola de CloudFront, consulte Supervisión de métricas de CloudFront con Amazon CloudWatch.

Determinación de si la cuenta inserta registros en CloudWatch

De forma predeterminada, CloudFront habilita el registro de respuestas de la función de Lambda no válidas y envía los archivos de registro a CloudWatch mediante uno de los Roles vinculados a servicios para Lambda@Edge. Si ha agregado funciones de Lambda@Edge a CloudFront antes de que se lanzara la característica de registro de respuestas de funciones de Lambda, el registro estará habilitado la próxima vez que actualice la configuración de Lambda@Edge, por ejemplo, agregando un desencadenador de CloudFront.

Haga lo siguiente para verificar que el envío de los archivos de registro a CloudWatch está habilitado para su cuenta:

- Compruebe si los registros aparecen en CloudWatch: asegúrese de mirar en la región donde se ejecutó la función de Lambda@Edge. Para obtener más información, consulte Determinación de la región de Lambda@Edge.
- Determine si el rol vinculado al servicio relacionado existe en la cuenta en IAM: debe tener el rol de IAM `AWSServiceRoleForCloudFrontLogger` en la cuenta. Para obtener más información acerca de este rol, consulte Roles vinculados a servicios para Lambda@Edge.

Eliminación de réplicas y funciones de Lambda@Edge

Puede eliminar una función de Lambda@Edge solo cuando CloudFront haya eliminado las réplicas de la función. Las réplicas de una función de Lambda se eliminan automáticamente en las siguientes situaciones:

- Una vez que elimine la última asociación de la función desde todas sus distribuciones de CloudFront. Si más de una distribución utiliza una función, las réplicas se eliminan solo después de que elimine la asociación de la función desde la última distribución.
- Después de eliminar la última distribución a la que se asoció una función.

Las réplicas suelen eliminarse al cabo de unas horas. No puede eliminar manualmente las réplicas de las funciones Lambda@Edge. Esto contribuye a evitar una situación en la que se elimina una réplica que todavía está en uso, lo que daría lugar a un error.

> **Warning**
>
> No cree aplicaciones que utilicen réplicas de funciones de Lambda@Edge fuera de CloudFront. Estas réplicas se eliminan cuando se eliminan sus asociaciones con distribuciones o cuando se eliminan las propias distribuciones. La réplica de la que depende una aplicación externa puede eliminarse sin ningún tipo de advertencia, lo que provocaría un error.

Para eliminar una asociación de las funciones de Lambda@Edge de una distribución de CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija el ID de la distribución con la asociación de las funciones de Lambda@Edge que desea eliminar.
3. Elija la pestaña Comportamientos.
4. Seleccione el comportamiento de caché que tiene la asociación de la función de Lambda@Edge que desea eliminar y, a continuación, elija Editar.
5. En Asociaciones de funciones, Tipo de función, elija Sin asociación para eliminar la asociación de función de Lambda@Edge.
6. Seleccione Save changes (Guardar cambios).

Después de eliminar una asociación de la función Lambda@Edge de una distribución de CloudFront, si lo desea puede eliminar la función Lambda o la versión de la función de AWS Lambda. Espere unas horas después de eliminar la asociación de funciones para poder limpiar las réplicas de la función de Lambda @Edge. Después, puede eliminar la función mediante la consola de Lambda, la AWS CLI, la API de Lambda o un SDK de AWS.

También puede eliminar una versión específica de una función de Lambda si la versión no tiene ninguna distribución de CloudFront asociada. Cuando haya eliminado todas las asociaciones correspondientes a una versión de función de Lambda, espere unas horas. Después, puede eliminar la versión de la función.

Estructura de eventos de Lambda@Edge

En los temas siguientes se describen los objetos de evento de solicitud y respuesta que CloudFront pasa a una función de Lambda@Edge cuando se activa.

Temas

- Selección dinámica del origen
- Eventos de solicitud
- Eventos de respuesta

Selección dinámica del origen

Puede utilizar el patrón de ruta de un comportamiento de la caché para enviar las solicitudes a un origen, en función de la ruta y el nombre del objeto solicitado, como `images/*.jpg`. Lambda@Edge también le permite direccionar las solicitudes a un origen en función de otras características, como los valores de los encabezados de solicitudes.

Esta selección dinámica del origen puede resultar útil en varios casos. Por ejemplo, puede distribuir solicitudes entre orígenes de diferentes zonas geográficas para facilitar el balanceo de carga global. También puede direccionar solicitudes selectivamente a varios orígenes, cada uno de ellos con un propósito distinto: control de bots, optimización SEO, autenticación, etc. Para obtener ejemplos de código que muestran cómo utilizar esta característica, consulte Selección de origen dinámico basada en contenido: ejemplos.

En el evento de solicitud de origen de CloudFront, el objeto `origin` de la estructura de eventos contiene información sobre el origen al que se enviaría la solicitud, en función del patrón de ruta. Puede actualizar los valores del objeto `origin` para enviar una solicitud a otro origen. Al actualizar el objeto de `origin`, no es necesario definir el origen en la distribución. También puede reemplazar un objeto de origen de Amazon S3 por un objeto de origen personalizado y viceversa. Sin embargo, solo se puede especificar un único origen por solicitud, ya sea un origen personalizado o un origen de Amazon S3, pero no ambos.

Eventos de solicitud

En los temas siguientes se muestra la estructura del objeto que CloudFront pasa a una función de Lambda para los eventos de solicitud de lector y de origen. Estos ejemplos muestran una solicitud `GET` sin cuerpo. Después de los ejemplos, se muestra una lista de todos los campos posibles en eventos de solicitud de lector y de origen.

Temas

- Ejemplo de solicitud de lector
- Ejemplo de solicitud de origen
- Campos de eventos de solicitud

Ejemplo de solicitud de lector

En el ejemplo siguiente se muestra un objeto de evento de solicitud de lector.

```
{
```

```
  "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": "/"
        }
      }
    }
  ]
}
```

Ejemplo de solicitud de origen

En el ejemplo siguiente se muestra un objeto de evento de solicitud de origen.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "origin-request",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "x-forwarded-for": [
              {
                "key": "X-Forwarded-For",
                "value": "203.0.113.178"
              }
            ],
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "Amazon CloudFront"
              }
            ],
            "via": [
              {
                "key": "Via",
                "value": "2.0 2afae0d44e2540f472c0635ab62c232b.cloudfront.net
 (CloudFront)"
              }
            ],
            "host": [
              {
                "key": "Host",
                "value": "example.org"
              }
            ],
            "cache-control": [
              {
                "key": "Cache-Control",
                "value": "no-cache"
              }
```

```
            ]
          },
          "method": "GET",
          "origin": {
            "custom": {
              "customHeaders": {},
              "domainName": "example.org",
              "keepaliveTimeout": 5,
              "path": "",
              "port": 443,
              "protocol": "https",
              "readTimeout": 30,
              "responseCompletionTimeout": 30,
              "sslProtocols": [
                "TLSv1",
                "TLSv1.1",
                "TLSv1.2"
              ]
            }
          },
          "querystring": "",
          "uri": "/"
        }
      }
    }
  ]
}
```

Campos de eventos de solicitud

Los datos del objeto de evento de solicitud se incluyen en dos subobjetos: `config` (`Records.cf.config`) y `request` (`Records.cf.request`). En las listas siguientes se describen los campos de cada subobjeto.

Campos del objeto config

En la siguiente lista se describen los campos del objeto `config` (`Records.cf.config`).

`distributionDomainName` (solo lectura)

El nombre de dominio de la distribución asociada a la solicitud.

`distributionID` (solo lectura)

El ID de la distribución asociada a la solicitud.

`eventType` (solo lectura)

El tipo de desencadenador asociado a la solicitud: `viewer-request` u `origin-request`.

`requestId` (solo lectura)

Una cadena cifrada que identifica de forma inequívoca una solicitud de lector a CloudFront. El valor `requestId` también aparece en los registros de acceso de CloudFront como `x-edge-request-id`. Para obtener más información, consulte Registros de acceso (registros estándar) y Campos de un archivo de registro.

Campos del objeto de solicitud

En la siguiente lista se describen los campos del objeto `request` (`Records.cf.request`).

`clientIp` (solo lectura)

La dirección IP del espectador que ha realizado la solicitud. Si el espectador utiliza un proxy HTTP o un equilibrador de carga para enviar la solicitud, el valor es la dirección IP del proxy o del equilibrador de carga.

headers (lectura y escritura)

Los encabezados de la solicitud. Tenga en cuenta lo siguiente:

- Las claves del objeto `headers` son nombres de encabezado HTTP estándar en minúsculas. El uso de claves en minúsculas le proporciona acceso a los valores del encabezado sin diferenciar mayúsculas de minúsculas.
- Cada objeto header (por ejemplo, `headers["accept"]` o `headers["host"]`) es una matriz de pares de clave-valor. Para un encabezado determinado, la matriz contiene un par de clave-valor para cada valor de la solicitud.
- `key` contiene el nombre con distinción de mayúsculas y minúsculas del encabezado tal como aparecía en la solicitud HTTP; por ejemplo, `Host`, `User-Agent`, `X-Forwarded-For`, `Cookie`, etc.
- `value` contiene el valor del encabezado tal como aparecía en la solicitud HTTP.
- Cuando la función Lambda agrega o modifica encabezados de solicitud y no incluye el campo `key` del encabezado, Lambda@Edge inserta automáticamente un encabezado `key` usando

el nombre de encabezado que proporcione. Independientemente de cómo haya formateado el nombre del encabezado, la clave de encabezado que se inserta automáticamente se formatea con mayúscula inicial para cada parte, separada por guiones (-).

Por ejemplo, puede agregar un encabezado como el siguiente, sin la clave de encabezado `key`:

```
"user-agent": [
  {
    "value": "ExampleCustomUserAgent/1.X.0"
  }
]
```

En este ejemplo, Lambda @Edge inserta automáticamente `"key": "User-Agent"`.

Para obtener más información acerca de restricciones de uso de encabezados, consulte Restricciones en funciones de borde.

`method` (solo lectura)

El método HTTP de la solicitud.

`querystring` (lectura y escritura)

La cadena de consulta, si hay alguna, de la solicitud. Si la solicitud no incluye una cadena de consulta, el objeto del evento incluye igualmente `querystring` con un valor vacío. Para obtener más información acerca de cadenas de consulta, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta.

`uri` (lectura y escritura)

La ruta relativa del objeto solicitado. Si su función de Lambda modifica el valor `uri`, tenga en cuenta lo siguiente:

- El nuevo valor `uri` debe comenzar con una barra diagonal (/).
- Si una función cambia el valor de `uri`, se cambia el objeto que el lector solicita.
- Si una función cambia el valor de `uri`, no cambia el comportamiento de la caché de la solicitud ni del origen al que se envía la solicitud.

`body` (lectura y escritura)

El cuerpo de la solicitud HTTP. La estructura `body` puede contener los siguientes campos:

`inputTruncated` (solo lectura)

Un indicador booleano que indica si Lambda@Edge truncó el cuerpo. Para obtener más información, consulte Restricciones para el cuerpo de la solicitud con la opción Incluir cuerpo.

`action` (lectura y escritura)

La acción que va a realizar con el cuerpo. Las opciones de `action` son las siguientes:

- `read-only:` Esta es la opción predeterminada. Cuando se devuelve la respuesta de la función de Lambda, si `action` es solo lectura, Lambda@Edge omite los cambios realizados en `encoding` o `data`.
- `replace:` Especifique este valor cuando desee reemplazar el cuerpo enviado al origen.

`encoding` (lectura y escritura)

La codificación del cuerpo. Cuando Lambda@Edge expone el cuerpo a la función de Lambda, primero lo convierte a base64-encoding. Si elige `replace` en `action` para reemplazar el cuerpo, puede elegir usar la codificación `base64` o `text` (el valor predeterminado). Si especifica `encoding` como `base64` pero el cuerpo no tiene una codificación base64 válida, CloudFront devuelve un error.

`data` (lectura y escritura)

El contenido del cuerpo de la solicitud.

`origin` (lectura y escritura) (solo eventos de origen)

El origen al que se envía la solicitud. La estructura del `origin` debe contener exactamente un origen, que puede ser un origen personalizado o un origen de Amazon S3.

Según el tipo de origen que especifique (orígenes personalizados o de Amazon S3), debe especificar los siguientes campos en su solicitud:

`customHeaders` (lectura/escritura) (orígenes personalizados y de Amazon S3)

(Opcional) Si desea incluir encabezados personalizados con la solicitud, especifique un nombre de encabezado y un par de valores para cada uno de ellos. No puede agregar encabezados que no estén permitidos y un encabezado con el mismo nombre no puede estar presente en `Records.cf.request.headers`. Las notas sobre encabezados de solicitud también se aplican a los encabezados personalizados. Para obtener más información, consulte Encabezados personalizados que CloudFront no puede agregar a solicitudes de origen y Restricciones en funciones de borde.

`domainName` (lectura/escritura) (orígenes personalizados y de Amazon S3)

El nombre de dominio del origen. El nombre de dominio no puede estar vacío.

- Para orígenes personalizados: especifique un nombre de dominio DNS, como `www.example.com`. El nombre de dominio no puede incluir dos puntos (:) y no puede ser una dirección IP. El nombre de dominio puede tener una longitud de hasta 253 caracteres.
- Para orígenes de Amazon S3: especifique el nombre de dominio DNS del bucket de Amazon S3, como `amzn-s3-demo-bucket.s3.eu-west-1.amazonaws.com`. El nombre puede tener una longitud de hasta 128 caracteres y debe escribirse en letras minúsculas.

`path` (lectura/escritura) (orígenes personalizados y de Amazon S3)

La ruta de directorio del servidor donde la solicitud debería encontrar el contenido. La ruta debe comenzar con una barra diagonal (/), pero no debe terminar con una (por ejemplo, no debería terminar con `example-path/`). Solo para los orígenes personalizados: la ruta debe estar codificada como una URL y tener una longitud máxima de 255 caracteres.

`keepaliveTimeout` (lectura y escritura) (solo orígenes personalizados)

El periodo de tiempo, en segundos, que CloudFront debería intentar mantener la conexión con el origen después de recibir el último paquete de la respuesta. El valor debe ser un número del 1 al 120, ambos inclusive.

`port` (lectura y escritura) (solo orígenes personalizados)

El puerto al que CloudFront debe conectarse en el origen personalizado. Este valor debe ser 80, 443 o un número comprendido entre 1024 y 65535, ambos inclusive.

`protocol` (lectura y escritura) (solo orígenes personalizados)

El protocolo de conexión que CloudFront debe usar al conectarse a su origen. El valor puede ser `http` o `https`.

`readTimeout` (lectura/escritura) (orígenes personalizados y de Amazon S3)

El tiempo, en segundos, que CloudFront debe esperar una respuesta después de enviar una solicitud a su origen. También especifica cuánto tiempo debe esperar CloudFront después de recibir un paquete de una respuesta antes de recibir el siguiente paquete. El valor debe ser un número del 1 al 120, ambos inclusive.

Si necesita una cuota mayor, consulte Tiempo de espera de respuesta por origen.

`responseCompletionTimeout` (lectura/escritura) (orígenes personalizados y de Amazon S3)

El tiempo (en segundos) que una solicitud de CloudFront al origen puede permanecer abierta y esperar una respuesta. Si en ese tiempo no se recibe la respuesta completa del origen, CloudFront finaliza la conexión.

El valor de `responseCompletionTimeout` debe ser igual o mayor que el valor para `readTimeout`. Si establece este valor en 0, elimina cualquier valor anterior que haya establecido y vuelve al valor predeterminado. También puede conseguirlo si elimina el campo `responseCompletionTimeout` de la solicitud del evento.

`sslProtocols` (lectura y escritura) (solo orígenes personalizados)

El protocolo SSL/TLS mínimo que CloudFront puede utilizar al establecer una conexión HTTPS con su origen. Los valores pueden ser alguno de los siguientes: `TLSv1.2`, `TLSv1.1`, `TLSv1` o `SSLv3`.

`authMethod` (lectura/escritura) (solo orígenes de Amazon S3)

Si utiliza una identidad de acceso de origen (OAI), establezca este campo a `origin-access-identity`. Si no usa una OAI, establézcala a `none`. Si establece `authMethod` en `origin-access-identity`, se aplican varios requisitos:

- Debe especificar el elemento `region` (consulte el siguiente campo).
- Debe utilizar la misma OAI cuando cambie la solicitud de un origen de Amazon S3 a otro.
- No se puede utilizar una OAI cuando se cambia la solicitud de un origen personalizado a un origen de Amazon S3.

> **Note**
>
> Este campo no admite el control de acceso de origen (OAC).

`region` (lectura/escritura) (solo orígenes de Amazon S3)

La región de AWS de su bucket de Amazon S3. Esto solo es necesario cuando se establece `authMethod` en `origin-access-identity`.

Eventos de respuesta

En los temas siguientes se muestra la estructura del objeto que CloudFront pasa a una función Lambda para los eventos de respuesta de lector y de origen. Después de los ejemplos, se muestra una lista de todos los campos posibles en eventos de respuesta de lector y de origen.

Temas

- Respuesta de origen de ejemplo
- Respuesta de lector de ejemplo
- Campos del evento de respuesta

Respuesta de origen de ejemplo

En el ejemplo siguiente se muestra un objeto de evento de respuesta de origen.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "origin-response",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "x-forwarded-for": [
              {
                "key": "X-Forwarded-For",
                "value": "203.0.113.178"
              }
            ],
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "Amazon CloudFront"
              }
            ],
            "via": [
```

```
              {
                "key": "Via",
                "value": "2.0 8f22423015641505b8c857a37450d6c0.cloudfront.net
(CloudFront)"
              }
            ],
            "host": [
              {
                "key": "Host",
                "value": "example.org"
              }
            ],
            "cache-control": [
              {
                "key": "Cache-Control",
                "value": "no-cache"
              }
            ]
          },
          "method": "GET",
          "origin": {
            "custom": {
              "customHeaders": {},
              "domainName": "example.org",
              "keepaliveTimeout": 5,
              "path": "",
              "port": 443,
              "protocol": "https",
              "readTimeout": 30,
              "responseCompletionTimeout": 30,
              "sslProtocols": [
                "TLSv1",
                "TLSv1.1",
                "TLSv1.2"
              ]
            }
          },
          "querystring": "",
          "uri": "/"
        },
        "response": {
          "headers": {
            "access-control-allow-credentials": [
              {
```

```
                "key": "Access-Control-Allow-Credentials",
                "value": "true"
              }
            ],
            "access-control-allow-origin": [
              {
                "key": "Access-Control-Allow-Origin",
                "value": "*"
              }
            ],
            "date": [
              {
                "key": "Date",
                "value": "Mon, 13 Jan 2020 20:12:38 GMT"
              }
            ],
            "referrer-policy": [
              {
                "key": "Referrer-Policy",
                "value": "no-referrer-when-downgrade"
              }
            ],
            "server": [
              {
                "key": "Server",
                "value": "ExampleCustomOriginServer"
              }
            ],
            "x-content-type-options": [
              {
                "key": "X-Content-Type-Options",
                "value": "nosniff"
              }
            ],
            "x-frame-options": [
              {
                "key": "X-Frame-Options",
                "value": "DENY"
              }
            ],
            "x-xss-protection": [
              {
                "key": "X-XSS-Protection",
                "value": "1; mode=block"
```

```
              }
            ],
            "content-type": [
              {
                "key": "Content-Type",
                "value": "text/html; charset=utf-8"
              }
            ],
            "content-length": [
              {
                "key": "Content-Length",
                "value": "9593"
              }
            ]
          },
          "status": "200",
          "statusDescription": "OK"
        }
      }
    }
  ]
}
```

Respuesta de lector de ejemplo

En el ejemplo siguiente se muestra un objeto de evento de respuesta de lector.

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

Campos del evento de respuesta

Los datos del objeto de evento de respuesta se incluyen en tres subobjetos: `config` (`Records.cf.config`), `request` (`Records.cf.request`) y `response` (`Records.cf.response`). Para obtener más información acerca de los campos del objeto de solicitud, consulte Campos del objeto de solicitud. En las listas siguientes se describen los campos de los subobjetos `config` y `response`.

Campos del objeto config

En la siguiente lista se describen los campos del objeto `config` (`Records.cf.config`).

`distributionDomainName` (solo lectura)

El nombre de dominio de la distribución asociada a la respuesta.

`distributionID` (solo lectura)

El ID de la distribución asociada a la respuesta.

`eventType` (solo lectura)

El tipo de desencadenador asociado a la respuesta: `origin-response` o `viewer-response`.

`requestId` (solo lectura)

Una cadena cifrada que identifica de forma inequívoca la solicitud del lector a CloudFront a la que está asociada esta respuesta. El valor `requestId` también aparece en los registros de acceso de CloudFront como `x-edge-request-id`. Para obtener más información, consulte Registros de acceso (registros estándar) y Campos de un archivo de registro.

Campos del objeto de respuesta

En la siguiente lista se describen los campos del objeto `response` (`Records.cf.response`). Para obtener información sobre el uso de una función de Lambda @Edge para generar una respuesta HTTP, consulte Generación de respuestas HTTP en los desencadenadores de solicitud.

`headers` (lectura y escritura)

Los encabezados de la respuesta. Tenga en cuenta lo siguiente:

- Las claves del objeto `headers` son nombres de encabezado HTTP estándar en minúsculas. El uso de claves en minúsculas le proporciona acceso a los valores del encabezado sin diferenciar mayúsculas de minúsculas.
- Cada objeto header (por ejemplo, `headers["content-type"]` o `headers["content-length"]`) es una matriz de pares de clave-valor. Para un encabezado determinado, la matriz contiene un par de clave-valor para cada valor de la respuesta.
- `key` contiene el nombre con distinción de mayúsculas y minúsculas del encabezado tal como aparece en la respuesta HTTP; por ejemplo `Content-Type`, `Content-Length`, `Cookie`, etc.
- `value` contiene el valor del encabezado tal como aparece en la respuesta HTTP.
- Cuando la función Lambda agrega o modifica encabezados de respuesta y no incluye el campo `key` del encabezado, Lambda@Edge inserta automáticamente un encabezado `key` usando el nombre de encabezado que proporcione. Independientemente de cómo haya formateado el nombre del encabezado, la clave de encabezado que se inserta automáticamente se formatea con mayúscula inicial para cada parte, separada por guiones (-).

  Por ejemplo, puede agregar un encabezado como el siguiente, sin la clave de encabezado `key`:

  ```
  "content-type": [
    {
      "value": "text/html;charset=UTF-8"
    }
  ]
  ```

  En este ejemplo, Lambda @Edge inserta automáticamente `"key": "Content-Type"`.

Para obtener más información acerca de restricciones de uso de encabezados, consulte Restricciones en funciones de borde.

`status`

Código de estado HTTP de la respuesta.

`statusDescription`

La descripción del estado HTTP de la respuesta.

Trabajo con solicitudes y respuestas

Para utilizar las solicitudes y respuestas de Lambda@Edge, consulte los temas siguientes:

Temas

- Uso de funciones de Lambda@Edge con conmutación por error de origen
- Generación de respuestas HTTP en los desencadenadores de solicitud
- Actualización de respuestas HTTP en desencadenadores de respuesta de origen
- Acceso al cuerpo de la solicitud con la opción Incluir cuerpo

Uso de funciones de Lambda@Edge con conmutación por error de origen

Puede utilizar las funciones de Lambda@Edge con distribuciones de CloudFront que ha configurado con grupos de origen, por ejemplo, para conmutación por error de origen que configure para ayudar a garantizar una alta disponibilidad. Para utilizar una función de Lambda con un grupo de origen, especifique la función en una solicitud de origen o un desencadenador de respuesta de origen para un grupo de origen al crear el comportamiento de la caché.

Para obtener más información, consulte los siguientes temas:

- Creación de grupos de origen: Creación de un grupo de origen
- Cómo utilizar la conmutación por error de origen con Lambda@Edge: Utilizar la conmutación por error de origen con funciones de Lambda@Edge

Generación de respuestas HTTP en los desencadenadores de solicitud

Cuando CloudFront recibe una solicitud, es posible utilizar una función de Lambda para generar una respuesta HTTP que CloudFront devuelve directamente al lector sin enviarla al origen. La generación de respuestas HTTP reduce la carga en el origen, y normalmente también reduce la latencia para el espectador.

Entre las situaciones más comunes para generar respuestas HTTP se incluyen las siguientes:

- Devolver una pequeña página web al lector
- Devolver un código de estado HTTP 301 o 302 para redirigir al usuario a otra página web
- Devolución de un código de estado HTTP 401 al espectador si el usuario no se ha autenticado

Una función de Lambda@Edge puede generar una respuesta HTTP cuando ocurren los siguientes eventos de CloudFront:

Eventos de solicitud del espectador

Cuando un evento de solicitud del lector activa una función, CloudFront devuelve la respuesta al lector y no la almacena en caché.

Eventos de solicitud al origen

Cuando un evento de solicitud al origen activa una función, CloudFront busca en la caché de borde una respuesta generada previamente por la función.

- Si la respuesta está en la caché, la función no se ejecuta y CloudFront devuelve al lector la respuesta almacenada en la caché.
- Si la respuesta no está en la caché, la función se ejecuta, CloudFront devuelve la respuesta al lector y también la almacena en la caché.

Para ver algunos ejemplos de código para generar respuestas HTTP, consulte Funciones de ejemplo de Lambda@Edge. También puede sustituir las respuestas HTTP en disparadores de respuesta. Para obtener más información, consulte Actualización de respuestas HTTP en desencadenadores de respuesta de origen.

Modelo de programación

En esta sección se describe el modelo de programación a seguir para usar Lambda@Edge con el fin de generar respuestas HTTP.

Temas

- Objeto de respuesta
- Errores
- Campos obligatorios

Objeto de respuesta

La respuesta que devuelva como parámetro `result` del método `callback` debe tener la siguiente estructura (tenga en cuenta que solo es obligatorio el campo `status`).

```
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'
};
```

El objeto de respuesta puede incluir los siguientes valores:

`body`

El cuerpo, si lo hay, que desea que CloudFront devuelva en la respuesta generada.

`bodyEncoding`

La codificación del valor especificado en `body`. Las únicas codificaciones válidas son `text` y `base64`. Si incluye `body` en el objeto `response` pero omite `bodyEncoding`, CloudFront trata el cuerpo como texto.

Si especifica `bodyEncoding` como `base64` pero el cuerpo no tiene una codificación base64 válida, CloudFront devuelve un error.

`headers`

Los encabezados que desea que devuelva CloudFront en la respuesta generada. Tenga en cuenta lo siguiente:

- Las claves del objeto `headers` son nombres de encabezado HTTP estándar en minúsculas. El uso de claves en minúsculas le proporciona acceso a los valores del encabezado sin diferenciar mayúsculas de minúsculas.
- Cada encabezado (por ejemplo, `headers["accept"]` or `headers["host"]`) es una matriz de pares clave-valor. Para un encabezado determinado, la matriz contiene un par de clave-valor para cada valor de la respuesta generada.
- `key` (opcional) es el nombre del encabezado que diferencia mayúsculas de minúsculas tal como aparece en una solicitud HTTP; por ejemplo, `accept` u `host`.
- Especifique `value` como un valor de encabezado.

- Si no incluye la parte de clave de encabezado del par de clave-valor, Lambda@Edge insertará automáticamente una clave de encabezado utilizando el nombre de encabezado que proporcione. Independientemente de cómo haya formateado el nombre del encabezado, la clave de encabezado que se inserta automáticamente se formatea con mayúscula inicial para cada parte, separada por guiones (-).

  Por ejemplo, puede añadir un encabezado como el siguiente, sin una clave de encabezado: `'content-type': [{ value: 'text/html;charset=UTF-8' }]`

  En este ejemplo, Lambda@Edge crea la siguiente clave de encabezado: `Content-Type`.

Para obtener más información acerca de restricciones de uso de encabezados, consulte Restricciones en funciones de borde.

`status`

El código de estado HTTP. Proporcione el código de estado como una cadena. CloudFront utiliza el código de estado proporcionado para lo siguiente:

- Devolverlo en la respuesta
- Almacenarlo en la caché de borde de CloudFront cuando la respuesta la generó una función activada por un evento de solicitud al origen
- Inicie sesión en CloudFront Registros de acceso (registros estándar)

Si el valor `status` no está comprendido entre 200 y 599, CloudFront devuelve un error al lector.

`statusDescription`

La descripción que desea que CloudFront devuelva en la respuesta, y que acompañará al código de estado HTTP. No es obligatorio utilizar descripciones estándar, como `OK` en un código de estado HTTP 200.

Errores

Los siguientes son posibles errores de respuestas HTTP generadas.

La respuesta contiene un cuerpo y especifica un código de estado 204 (Sin contenido

Cuando una solicitud del lector activa una función, CloudFront devuelve un código de estado HTTP 502 (Gateway incorrecta) al lector cuando se cumplen las dos condiciones siguientes:

- El valor de `status` es 204 (Sin contenido)

- La respuesta incluye un valor para `body`

  Esto se debe a que Lambda@Edge impone la restricción opcional de RFC 2616 que establece que una respuesta `HTTP 204` no necesita contener cuerpo de mensaje.

Restricciones en el tamaño de la respuesta generada

El tamaño máximo de una respuesta generada por una función de Lambda depende del evento que desencadenó la función:

- Eventos de solicitud del lector: 40 KB
- Eventos de solicitud al origen: 1 MB

Si la respuesta supera el tamaño permitido, CloudFront devuelve un código de estado HTTP 502 (Gateway incorrecta) al lector.

Campos obligatorios

El campo `status` es obligatorio.

Todos los demás campos son opcionales.

Actualización de respuestas HTTP en desencadenadores de respuesta de origen

Cuando CloudFront recibe una respuesta HTTP desde el servidor de origen, si existe un desencadenador de respuesta del origen asociado al comportamiento de la caché, es posible modificar la respuesta HTTP para anular lo que ha devuelto el origen.

Entre las situaciones más comunes para actualizar respuestas HTTP se incluyen las siguientes:

- Cambiar el estado para establecer un código de estado HTTP 200 y crear un cuerpo con contenido estático para devolverlo al espectador cuando un origen devuelva un código de estado de error (4xx o 5xx). Para ver código de muestra, consulte Ejemplo: Uso de un desencadenador de respuesta de origen para actualizar el código de estado de error a 200.
- Cambiar el estado para establecer un código de estado HTTP 301 o 302, con objeto de redirigir al usuario a otro sitio web cuando un origen devuelve un código de estado de error (4xx o 5xx). Para ver código de muestra, consulte Ejemplo: Uso de un desencadenador de respuesta de origen para actualizar el código de estado de error a 302.

> **Note**
>
> La función debe devolver un valor de estado entre `200` y `599` (incluidos); de lo contrario, CloudFront devuelve un error al espectador.

También puede sustituir las respuestas HTTP en eventos de solicitud al origen y del espectador. Para obtener más información, consulte Generación de respuestas HTTP en los desencadenadores de solicitud.

Cuando trabaja con la respuesta HTTP, Lambda@Edge no expone el cuerpo que devuelve el servidor de origen al desencadenador de respuesta del origen. Puede generar un cuerpo con contenido estático estableciéndolo en el valor deseado, o eliminar el cuerpo dentro de la función estableciendo un valor vacío. Si no actualiza el campo de cuerpo de la función, se devolverá al espectador el cuerpo original devuelto por el servidor de origen.

Acceso al cuerpo de la solicitud con la opción Incluir cuerpo

A partir de ahora, puede hacer que Lambda@Edge exponga el cuerpo de una solicitud en los métodos HTTP que permiten la escritura (POST, PUT, DELETE, etc.) para que puede tener acceso a él en la función de Lambda. Puede elegir acceso de solo lectura o puede especificar que sustituirá el cuerpo.

Para habilitar esta opción, elija Incluir cuerpo al crear un desencadenador de CloudFront para la función que corresponde a un evento de solicitud al origen o del lector. Para obtener más información, consulte Adición de desencadenadores para una función de Lambda@Edge; para obtener información acerca de cómo utilizar Incluir cuerpo con su función, consulte Estructura de eventos de Lambda@Edge.

Entre los escenarios en los que es conveniente utilizar esta característica se incluyen los siguientes:

- Procesamiento de formularios web, como formularios de tipo "póngase en contacto con nosotros", sin devolver los datos de entrada de los clientes a los servidores de origen.
- Recopilación de datos de balizas web enviados por los navegadores de los espectadores y que se procesan en el borde.

Para ver código de muestra, consulte Funciones de ejemplo de Lambda@Edge.

> **Note**
>
> Si el cuerpo de la solicitud es grande, Lambda@Edge lo trunca. Para obtener información detallada sobre el tamaño máximo y el truncamiento, consulte Restricciones para el cuerpo de la solicitud con la opción Incluir cuerpo.

Funciones de ejemplo de Lambda@Edge

Consulte los ejemplos siguientes para usar funciones de Lambda con Amazon CloudFront.

> **Note**
>
> Si elige el tiempo de ejecución Node.js 18 o una versión posterior para la función Lambda@Edge, se creará automáticamente un archivo `index.mjs`. Para usar los siguientes ejemplos de código, cambie el nombre del archivo `index.mjs` a `index.js`.

Temas

- Ejemplos generales
- Generación de respuestas: ejemplos
- Cadenas de consulta: ejemplos
- Personalización de contenido por encabezados de tipo de dispositivo o país: ejemplos
- Selección de origen dinámico basada en contenido: ejemplos
- Actualización de estados de error: ejemplos
- Acceso al cuerpo de la solicitud: ejemplos

Ejemplos generales

Los ejemplos siguientes muestran formas habituales de usar Lambda@Edge en CloudFront.

Temas

- Ejemplo: prueba A/B
- Ejemplo: Sobrescritura de un encabezado de respuesta

Ejemplo: prueba A/B

Puede utilizar el siguiente ejemplo para probar dos versiones diferentes de una imagen sin crear redirecciones ni cambiar la dirección URL. En este ejemplo se leen las cookies de la solicitud del lector y se modifica la URL de la solicitud en consecuencia. Si el espectador no envía una cookie con uno de los valores esperados, el ejemplo asigna aleatoriamente al espectador una de las URL.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const headers = request.headers;

    if (request.uri !== '/experiment-pixel.jpg') {
        // do not process if this is not an A-B test request
        callback(null, request);
        return;
    }

    const cookieExperimentA = 'X-Experiment-Name=A';
    const cookieExperimentB = 'X-Experiment-Name=B';
    const pathExperimentA = '/experiment-group/control-pixel.jpg';
    const pathExperimentB = '/experiment-group/treatment-pixel.jpg';

    /*
     * Lambda at the Edge headers are array objects.
     *
     * Client may send multiple Cookie headers, i.e.:
     * > GET /viewerRes/test HTTP/1.1
     * > User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1
 OpenSSL/1.0.1u zlib/1.2.3
     * > Cookie: First=1; Second=2
     * > Cookie: ClientCode=abc
     * > Host: example.com
     *
     * You can access the first Cookie header at headers["cookie"][0].value
     * and the second at headers["cookie"][1].value.
     *
     * Header values are not parsed. In the example above,
     * headers["cookie"][0].value is equal to "First=1; Second=2"
     */
```

```
    let experimentUri;
    if (headers.cookie) {
        for (let i = 0; i < headers.cookie.length; i++) {
            if (headers.cookie[i].value.indexOf(cookieExperimentA) >= 0) {
                console.log('Experiment A cookie found');
                experimentUri = pathExperimentA;
                break;
            } else if (headers.cookie[i].value.indexOf(cookieExperimentB) >= 0) {
                console.log('Experiment B cookie found');
                experimentUri = pathExperimentB;
                break;
            }
        }
    }

    if (!experimentUri) {
        console.log('Experiment cookie has not been found. Throwing dice...');
        if (Math.random() < 0.75) {
            experimentUri = pathExperimentA;
        } else {
            experimentUri = pathExperimentB;
        }
    }

    request.uri = experimentUri;
    console.log(`Request uri set to "${request.uri}"`);
    callback(null, request);
};
```

Python

```
import json
import random

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    headers = request['headers']

    if request['uri'] != '/experiment-pixel.jpg':
        # Not an A/B Test
        return request
```

```
    cookieExperimentA, cookieExperimentB = 'X-Experiment-Name=A', 'X-Experiment-
Name=B'
    pathExperimentA, pathExperimentB = '/experiment-group/control-pixel.jpg', '/
experiment-group/treatment-pixel.jpg'

    '''
    Lambda at the Edge headers are array objects.

    Client may send multiple cookie headers. For example:
    > GET /viewerRes/test HTTP/1.1
    > User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1
 OpenSSL/1.0.1u zlib/1.2.3
    > Cookie: First=1; Second=2
    > Cookie: ClientCode=abc
    > Host: example.com

    You can access the first Cookie header at headers["cookie"][0].value
    and the second at headers["cookie"][1].value.

    Header values are not parsed. In the example above,
    headers["cookie"][0].value is equal to "First=1; Second=2"
    '''

    experimentUri = ""

    for cookie in headers.get('cookie', []):
        if cookieExperimentA in cookie['value']:
            print("Experiment A cookie found")
            experimentUri = pathExperimentA
            break
        elif cookieExperimentB in cookie['value']:
            print("Experiment B cookie found")
            experimentUri = pathExperimentB
            break

    if not experimentUri:
        print("Experiment cookie has not been found. Throwing dice...")
        if random.random() < 0.75:
            experimentUri = pathExperimentA
        else:
            experimentUri = pathExperimentB

    request['uri'] = experimentUri
    print(f"Request uri set to {experimentUri}")
```

```
    return request
```

Ejemplo: Sobrescritura de un encabezado de respuesta

En el ejemplo siguiente, se muestra cómo cambiar el valor de un encabezado de respuesta según el valor de otro encabezado.

Node.js

```
export const handler = async (event) => {
    const response = event.Records[0].cf.response;
    const headers = response.headers;

    const headerNameSrc = 'X-Amz-Meta-Last-Modified';
    const headerNameDst = 'Last-Modified';

    if (headers[headerNameSrc.toLowerCase()]) {
        headers[headerNameDst.toLowerCase()] = [{
            key: headerNameDst,
            value: headers[headerNameSrc.toLowerCase()][0].value,
        }];
        console.log(`Response header "${headerNameDst}" was set to ` +
                    `"${headers[headerNameDst.toLowerCase()][0].value}"`);
    }

    return response;
};
```

Python

```
import json

def lambda_handler(event, context):
    response = event['Records'][0]['cf']['response']
    headers = response['headers']

    header_name_src = 'X-Amz-Meta-Last-Modified'
    header_name_dst = 'Last-Modified'

    if headers.get(header_name_src.lower()):
        headers[header_name_dst.lower()] = [{
            'key': header_name_dst,
```

```
            'value': headers[header_name_src.lower()][0]['value']
        }]
        print(f'Response header "{header_name_dst}" was set to '
              f'"{headers[header_name_dst.lower()][0]["value"]}"')

    return response
```

Generación de respuestas: ejemplos

En los ejemplos siguientes se muestra cómo puede usar Lambda@Edge para generar respuestas.

Temas

- Ejemplo: Envío de contenido estático (respuesta generada)
- Ejemplo: Generación de un redireccionamiento HTTP (respuesta generada)

Ejemplo: Envío de contenido estático (respuesta generada)

En el siguiente ejemplo se muestra cómo utilizar una función de Lambda para enviar contenido de sitio web estático, lo que reduce la carga en el servidor de origen y la latencia total.

> **Note**
>
> Puede generar respuestas HTTP para los eventos de solicitud del espectador y al origen. Para obtener más información, consulte the section called “Generación de respuestas HTTP en los desencadenadores de solicitud”.
> También puede sustituir o quitar el cuerpo de la respuesta HTTP en eventos de respuesta de origen. Para obtener más información, consulte the section called “Actualización de respuestas HTTP en desencadenadores de respuesta de origen”.

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
```

Ejemplo: Generación de un redireccionamiento HTTP (respuesta generada)

En el siguiente ejemplo se muestra cómo generar una redirección HTTP.

> **Note**
>
> Puede generar respuestas HTTP para los eventos de solicitud del espectador y al origen. Para obtener más información, consulte Generación de respuestas HTTP en los desencadenadores de solicitud.

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
```

Cadenas de consulta: ejemplos

En los ejemplos siguientes se muestran formas de usar Lambda@Edge con cadenas de consulta.

Temas

- Ejemplo: Adición de un encabezado en función de un parámetro de la cadena de consulta
- Ejemplo: Normalización de parámetros de cadenas de consulta para mejorar la tasa de aciertos de caché
- Ejemplo: Redireccionamiento de los usuarios no autenticados a una página de inicio de sesión

Ejemplo: Adición de un encabezado en función de un parámetro de la cadena de consulta

El siguiente ejemplo muestra cómo obtener el par clave-valor de un parámetro de la cadena de consulta y, a continuación, añadir un encabezado en función de dichos valores.

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
```

Ejemplo: Normalización de parámetros de cadenas de consulta para mejorar la tasa de aciertos de caché

El siguiente ejemplo muestra cómo mejorar la tasa de acceso a la caché haciendo los siguientes cambios en las cadenas de consulta antes de que CloudFront reenvíe las solicitudes a su origen:

- Alfabetizar los pares de clave-valor por el nombre del parámetro.
- Cambiar a minúsculas el modelo de mayúsculas y minúsculas de los pares de clave-valor.

Para obtener más información, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta.

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
```

Ejemplo: Redireccionamiento de los usuarios no autenticados a una página de inicio de sesión

El siguiente ejemplo muestra cómo redirigir a los usuarios una página de inicio de sesión si no ha introducido sus credenciales.

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
```

Personalización de contenido por encabezados de tipo de dispositivo o país: ejemplos

En los ejemplos siguientes se muestra cómo puede usar Lambda@Edge para personalizar el comportamiento en función de la ubicación o el tipo de dispositivo que usa el lector.

Temas

- Ejemplo: Redireccionamiento de solicitudes de espectadores a una URL específica de un país
- Ejemplo: Envío de distintas versiones de un objeto en función del dispositivo

Ejemplo: Redireccionamiento de solicitudes de espectadores a una URL específica de un país

El siguiente ejemplo muestra cómo generar una respuesta de redireccionamiento HTTP con una URL específica del país y devolver la respuesta al espectador. Esto resulta útil cuando se quiere proporcionar respuestas específicas del país. Por ejemplo:

- Si tiene subdominios específicos de un país, como us.ejemplo.com y tw.ejemplo.com, puede generar una respuesta de redireccionamiento cuando un espectador solicite ejemplo.com.
- Si está haciendo streaming de video, pero no tiene derechos para transmitir el contenido en un país determinado, puede redirigir a los usuarios de dicho país a una página en la que se explica por qué no pueden ver el video.

Tenga en cuenta lo siguiente:

- Debe configurar la distribución para almacenar en la caché en función del encabezado `CloudFront-Viewer-Country`. Para obtener más información, consulte Caché en función de encabezados de solicitud seleccionados.
- CloudFront agrega el encabezado `CloudFront-Viewer-Country` después del evento de solicitud del lector. Para utilizar este ejemplo, debe crear un activador para el evento de solicitud al origen.

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
```

Ejemplo: Envío de distintas versiones de un objeto en función del dispositivo

El siguiente ejemplo muestra cómo ofrecer distintas versiones de un objeto en función del tipo de dispositivo que el usuario está utilizando; por ejemplo, un dispositivo móvil o una tablet. Tenga en cuenta lo siguiente:

- Debe configurar la distribución para almacenar en la caché en función de los encabezados `CloudFront-Is-*-Viewer`. Para obtener más información, consulte Caché en función de encabezados de solicitud seleccionados.
- CloudFront agrega los encabezados `CloudFront-Is-*-Viewer` después del evento de solicitud del lector. Para utilizar este ejemplo, debe crear un activador para el evento de solicitud al origen.

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
```

Selección de origen dinámico basada en contenido: ejemplos

En los ejemplos siguientes se muestra cómo puede usar Lambda@Edge para el direccionamiento a diferentes orígenes en función de la información de la solicitud.

Temas

- Ejemplo: Uso de un desencadenador de solicitud de origen para cambiar desde un origen personalizado a un origen de Amazon S3
- Ejemplo: Uso de un desencadenador de solicitud de origen para cambiar la región de origen de Amazon S3
- Ejemplo: Uso de un desencadenador de solicitud de origen para cambiar desde un origen de Amazon S3 a un origen personalizado
- Ejemplo: Uso de un desencadenador de solicitud al origen para transferir gradualmente el tráfico desde un bucket de Amazon S3 a otro
- Ejemplo: Uso de un desencadenador de solicitud de origen para cambiar el nombre del dominio de origen en función del encabezado de país

Ejemplo: Uso de un desencadenador de solicitud de origen para cambiar desde un origen personalizado a un origen de Amazon S3

Esta función demuestra cómo utilizar un desencadenador de solicitud al origen para cambiar desde un origen personalizado a un origen de Amazon S3 desde el que recuperar el contenido, en función de las propiedades de la solicitud.

Node.js

```
'use strict';

 const querystring = require('querystring');

 exports.handler = (event, context, callback) => {
     const request = event.Records[0].cf.request;

     /**
      * Reads query string to check if S3 origin should be used, and
      * if true, sets S3 origin properties.
      */

     const params = querystring.parse(request.querystring);

     if (params['useS3Origin']) {
         if (params['useS3Origin'] === 'true') {
             const s3DomainName = 'amzn-s3-demo-bucket.s3.amazonaws.com';

             /* Set S3 origin fields */
             request.origin = {
                 s3: {
                     domainName: s3DomainName,
                     region: '',
                     authMethod: 'origin-access-identity',
                     path: '',
                     customHeaders: {}
                 }
             };
             request.headers['host'] = [{ key: 'host', value: s3DomainName}];
         }
     }

    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
```

```
    '''
    Reads query string to check if S3 origin should be used, and
    if true, sets S3 origin properties
    '''
    params = {k: v[0] for k, v in parse_qs(request['querystring']).items()}
    if params.get('useS3Origin') == 'true':
        s3DomainName = 'amzn-s3-demo-bucket.s3.amazonaws.com'

        # Set S3 origin fields
        request['origin'] = {
            's3': {
                'domainName': s3DomainName,
                'region': '',
                'authMethod': 'origin-access-identity',
                'path': '',
                'customHeaders': {}
            }
        }
        request['headers']['host'] = [{'key': 'host', 'value': s3DomainName}]
    return request
```

Ejemplo: Uso de un desencadenador de solicitud de origen para cambiar la región de origen de Amazon S3

Esta función demuestra cómo utilizar un desencadenador de solicitud al origen para cambiar el origen de Amazon S3 desde el que se recupera el contenido, en función de las propiedades de la solicitud.

En este ejemplo, utilizamos el valor del encabezado `CloudFront-Viewer-Country` para actualizar el nombre de dominio del bucket de S3 por un bucket de una región que está más cerca del lector. Esto puede resultar útil de varias maneras:

- Reduce las latencias cuando la región especificada está más cerca del país del lector.
- Proporciona soberanía de los datos, al asegurarse de que los datos se distribuyen desde un origen que está en el país del que provino la solicitud.

Para utilizar este ejemplo, debe hacer lo siguiente:

- Configure la distribución para almacenar en la caché en función del encabezado `CloudFront-Viewer-Country`. Para obtener más información, consulte Caché en función de encabezados de solicitud seleccionados.
- Crear un disparador para esta función en el evento de solicitud al origen. CloudFront agrega el encabezado `CloudFront-Viewer-Country` después del evento de solicitud del lector; por lo tanto, para utilizar este ejemplo, debe asegurarse de que la función ejecuta una solicitud de origen.

> **Note**
>
> El siguiente código de ejemplo usa la misma identidad de acceso de origen (OAI) para todos los buckets de S3 que usa para el origen. Para obtener más información, consulte Identidad de acceso de origen.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;

    /**
     * This blueprint demonstrates how an origin-request trigger can be used to
     * change the origin from which the content is fetched, based on request
 properties.
     * In this example, we use the value of the CloudFront-Viewer-Country header
     * to update the S3 bucket domain name to a bucket in a Region that is closer to
     * the viewer.
     *
     * This can be useful in several ways:
     *      1) Reduces latencies when the Region specified is nearer to the viewer's
     *         country.
     *      2) Provides data sovereignty by making sure that data is served from an
     *         origin that's in the same country that the request came from.
     *
     * NOTE: 1. You must configure your distribution to cache based on the
     *          CloudFront-Viewer-Country header. For more information, see
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-
headers
```

```
     *       2. CloudFront adds the CloudFront-Viewer-Country header after the
 viewer
     *          request event. To use this example, you must create a trigger for
 the
     *          origin request event.
     */

    const countryToRegion = {
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
    };

    if (request.headers['cloudfront-viewer-country']) {
        const countryCode = request.headers['cloudfront-viewer-country'][0].value;
        const region = countryToRegion[countryCode];

        /**
         * If the viewer's country is not in the list you specify, the request
         * goes to the default S3 bucket you've configured.
         */
        if (region) {
            /**
             * If you've set up OAI, the bucket policy in the destination bucket
             * should allow the OAI GetObject operation, as configured by default
             * for an S3 origin with OAI. Another requirement with OAI is to provide
             * the Region so it can be used for the SIGV4 signature. Otherwise, the
             * Region is not required.
             */
            request.origin.s3.region = region;
            const domainName = `amzn-s3-demo-bucket-in-${region}.s3.
${region}.amazonaws.com`;
            request.origin.s3.domainName = domainName;
            request.headers['host'] = [{ key: 'host', value: domainName }];
        }
    }

    callback(null, request);
};
```

Python

```
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    '''
    This blueprint demonstrates how an origin-request trigger can be used to
    change the origin from which the content is fetched, based on request
 properties.
    In this example, we use the value of the CloudFront-Viewer-Country header
    to update the S3 bucket domain name to a bucket in a Region that is closer to
    the viewer.

    This can be useful in several ways:
        1) Reduces latencies when the Region specified is nearer to the viewer's
            country.
        2) Provides data sovereignty by making sure that data is served from an
            origin that's in the same country that the request came from.

    NOTE: 1. You must configure your distribution to cache based on the
            CloudFront-Viewer-Country header. For more information, see
            https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-headers
          2. CloudFront adds the CloudFront-Viewer-Country header after the viewer
            request event. To use this example, you must create a trigger for the
            origin request event.
    '''

    countryToRegion = {
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
    }

    viewerCountry = request['headers'].get('cloudfront-viewer-country')
    if viewerCountry:
        countryCode = viewerCountry[0]['value']
        region = countryToRegion.get(countryCode)

        # If the viewer's country in not in the list you specify, the request
        # goes to the default S3 bucket you've configured
        if region:
```

```
            '''
            If you've set up OAI, the bucket policy in the destination bucket
            should allow the OAI GetObject operation, as configured by default
            for an S3 origin with OAI. Another requirement with OAI is to provide
            the Region so it can be used for the SIGV4 signature. Otherwise, the
            Region is not required.
            '''
            request['origin']['s3']['region'] = region
            domainName = 'amzn-s3-demo-bucket-in-{0}.s3.
{0}.amazonaws.com'.format(region)
            request['origin']['s3']['domainName'] = domainName
            request['headers']['host'] = [{'key': 'host', 'value': domainName}]

    return request
```

Ejemplo: Uso de un desencadenador de solicitud de origen para cambiar desde un origen de Amazon S3 a un origen personalizado

Esta función demuestra cómo utilizar un disparador de solicitud al origen para cambiar el origen personalizado desde el que se recupera el contenido, en función de las propiedades de la solicitud.

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
```

Ejemplo: Uso de un desencadenador de solicitud al origen para transferir gradualmente el tráfico desde un bucket de Amazon S3 a otro

Esta función demuestra cómo transferir gradualmente el tráfico desde un bucket de Amazon S3 a otro de forma controlada.

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
```

Ejemplo: Uso de un desencadenador de solicitud de origen para cambiar el nombre del dominio de origen en función del encabezado de país

Esta función demuestra cómo cambiar el nombre del dominio de origen en función del encabezado `CloudFront-Viewer-Country`, de forma que el contenido se distribuya desde un origen más cercano al país del lector.

La implementación de esta funcionalidad para su distribución puede tener ventajas como las siguientes:

- Reducir las latencias cuando la región especificada está más cerca del país del lector
- Proporcionar soberanía de los datos, al asegurarse de que los datos se distribuyen desde un origen que está en el país del que provino la solicitud

Tenga en cuenta que para habilitar esta funcionalidad, debe configurar su distribución para almacenar en la caché en función del encabezado `CloudFront-Viewer-Country`. Para obtener más información, consulte the section called "Caché en función de encabezados de solicitud seleccionados".

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
```

Actualización de estados de error: ejemplos

En los ejemplos siguientes se proporciona orientación acerca de cómo puede usar Lambda@Edge para cambiar el estado de error que se devuelve a los usuarios.

Temas

- Ejemplo: Uso de un desencadenador de respuesta de origen para actualizar el código de estado de error a 200
- Ejemplo: Uso de un desencadenador de respuesta de origen para actualizar el código de estado de error a 302

Ejemplo: Uso de un desencadenador de respuesta de origen para actualizar el código de estado de error a 200

Esta función demuestra cómo actualizar el estado de la respuesta a 200 y generar un cuerpo con contenido estático para devolverlo al espectador en la siguiente situación:

- La función se desencadena en una respuesta del origen.
- El estado de la respuesta del servidor de origen es un código de estado de error (4xx o 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
```

Ejemplo: Uso de un desencadenador de respuesta de origen para actualizar el código de estado de error a 302

Esta función demuestra cómo actualizar el código de estado HTTP a 302 para la redirección a otra ruta (comportamiento de la caché) en la que se ha configurado un origen diferente. Tenga en cuenta lo siguiente:

- La función se desencadena en una respuesta del origen.
- El estado de la respuesta del servidor de origen es un código de estado de error (4xx o 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
```

Acceso al cuerpo de la solicitud: ejemplos

En los ejemplos siguientes se muestra cómo puede usar Lambda@Edge para trabajar con las solicitudes POST.

> **Note**
>
> Para utilizar estos ejemplos, debe habilitar la opción incluir cuerpo en la asociación de funciones Lambda de la distribución. No está habilitada de forma predeterminada.
>
> - Para habilitar esta configuración en la consola de CloudFront, seleccione la casilla de verificación Incluir cuerpo en la Asociación de funciones Lambda.
> - Para habilitar esta configuración en la API de CloudFront o con CloudFormation, establezca el campo `IncludeBody` en `true` en `LambdaFunctionAssociation`.

Temas

- Ejemplo: Uso de un desencadenador de solicitud para leer un formulario HTML
- Ejemplo: Uso de un desencadenador de solicitud para modificar un formulario HTML

Ejemplo: Uso de un desencadenador de solicitud para leer un formulario HTML

Esta función ilustra cómo puede procesar el cuerpo de una solicitud POST generada por un formulario HTML (formulario web), como por ejemplo un formulario tipo "póngase en contacto con nosotros". Por ejemplo, es posible que tenga un formulario HTML como el siguiente:

```
<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>
```

Para la función de ejemplo que se indica a continuación, la función se debe desencadenar en una solicitud al origen o del lector de CloudFront.

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
```

Ejemplo: Uso de un desencadenador de solicitud para modificar un formulario HTML

Esta función ilustra cómo puede modificar el cuerpo de una solicitud POST generada por un formulario HTML (formulario web). La función se activa en una solicitud al origen o del lector de CloudFront.

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)
```

Restricciones en funciones de borde

En los temas siguientes se describen las restricciones que se aplican a CloudFront Functions y Lambda @Edge. Algunas restricciones se aplican a todas las funciones de borde y otras solo se aplican a CloudFront Functions o Lambda @Edge.

En este tema se proporciona información detallada sobre las limitaciones y las restricciones que debe tener en cuenta al desarrollar e implementar funciones periféricas con CloudFront.

Comprender estas restricciones lo ayuda a asegurarse de que las funciones periféricas funcionan según lo previsto y cumplen las características admitidas.

Temas

- Restricciones en todas las funciones de borde
- Restricciones en CloudFront Functions
- Restricciones de Lambda @Edge

Para obtener información acerca de las cuotas (anteriormente denominadas límites), consulte Cuotas en CloudFront Functions y Cuotas de Lambda@Edge.

Restricciones en todas las funciones de borde

Las siguientes restricciones se aplican a todas las funciones periféricas, tanto de CloudFront Functions como de Lambda @Edge.

Temas

- Propiedad de Cuenta de AWS
- Combinación de funciones de CloudFront con Lambda @Edge
- HTTP status codes
- Encabezados HTTP
- Cadenas de consulta
- URI
- Codificación de URI, cadena de consulta y encabezados
- Microsoft Smooth Streaming
- Etiquetado

Propiedad de Cuenta de AWS

Para asociar una función de borde con una distribución de CloudFront, la función y la distribución deben pertenecer al mismo propietarioCuenta de AWS.

Combinación de funciones de CloudFront con Lambda @Edge

Para un determinado comportamiento de caché, se aplican las siguientes restricciones:

- Cada tipo de evento (solicitud de lector, solicitud de origen, respuesta de origen y respuesta de lector) solo puede tener una asociación de función de borde.
- No se puede combinar CloudFront Functions y Lambda@Edge en eventos de lector (solicitud y respuesta).

Todas las demás combinaciones de funciones de borde están permitidas. En la tabla siguiente se explican las combinaciones permitidas.

	CloudFront Functions

		Solicitud del lector	Respuesta del lector
Lambda@Edge	Solicitud del lector	No permitido	No permitido
	Solicitud del origen	Permitido	Permitido
	Respuesta del origen	Permitido	Permitido
	Respuesta del lector	No permitido	No permitido

HTTP status codes

CloudFront no invoca funciones periféricas para eventos de respuesta al lector si el origen devuelve el código de estado HTTP 400 o un número superior.

Las funciones de Lambda @Edge para eventos de respuesta de origen se invocan para All (Todos), incluso si el origen devuelve el código de estado HTTP 400 o un número superior. Para obtener más información, consulte Actualización de respuestas HTTP en desencadenadores de respuesta de origen.

Encabezados HTTP

Determinados encabezados HTTP no están permitidos, lo que significa que no están expuestos a funciones perimetrales y las funciones no pueden agregarlos. Otros encabezados son de solo lectura, lo que significa que las funciones pueden leerlos pero no pueden agregarlos, modificarlos ni eliminarlos.

Temas

- Encabezados no permitidos
- Encabezados de solo lectura

Encabezados no permitidos

Los siguientes encabezados HTTP no están expuestos a funciones perimetrales y las funciones no pueden agregarlos. Si su función agrega uno de estos encabezados, no supera la validación de CloudFront y CloudFront devuelve el código de estado HTTP 502 (Gateway incorrecta) al lector.

- `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`

Encabezados de solo lectura

Los siguientes encabezados son de solo lectura. La función puede leerlos y utilizarlos como entrada para la lógica de la función, pero no puede cambiar los valores. Si su función añade o edita un

encabezado de solo lectura, la solicitud no supera la validación de CloudFront y CloudFront devuelve el código de estado HTTP 502 (Gateway incorrecta) al lector.

Encabezados de solo lectura en eventos de solicitud de lector

Los siguientes encabezados son de solo lectura en los eventos de solicitud de lector.

- `Content-Length`
- `Host`
- `Transfer-Encoding`
- `Via`

Encabezados de solo lectura en eventos de solicitud de origen (solo Lambda @Edge)

Los siguientes encabezados son de solo lectura en eventos de solicitud de origen, que solo existen en Lambda @Edge.

- `Accept-Encoding`
- `Content-Length`
- `If-Modified-Since`
- `If-None-Match`
- `If-Range`
- `If-Unmodified-Since`
- `Transfer-Encoding`
- `Via`

Encabezados de solo lectura en eventos de respuesta de origen (solo Lambda @Edge)

Los siguientes encabezados son de solo lectura en eventos de respuesta de origen, que solo existen en Lambda @Edge.

- `Transfer-Encoding`
- `Via`

Encabezados de solo lectura en eventos de respuesta de lector

Los siguientes encabezados son de solo lectura en eventos de respuesta de lector para CloudFront Functions y Lambda@Edge.

- `Warning`
- `Via`

Los siguientes encabezados son de solo lectura en los eventos de respuesta de lector para Lambda@Edge.

- `Content-Length`
- `Content-Encoding`
- `Transfer-Encoding`

Cadenas de consulta

Las siguientes restricciones se aplican a las funciones que leen, actualizan o crean una cadena de consulta en un URI de solicitud.

- (Solo Lambda @Edge) Para acceder a la cadena de consulta en una solicitud de origen o función de respuesta de origen, la política de caché o la política de solicitud de origen debe establecerse enAll (Todos): paraCadenas de consulta.
- Una función puede crear o actualizar una cadena de consulta para eventos de solicitud de lector y solicitud de origen (los eventos de solicitud de origen solo existen en Lambda @Edge).
- Una función puede leer una cadena de consulta, pero no puede crear o actualizar una, para eventos de respuesta de origen y respuesta de lector (los eventos de respuesta de origen solo existen en Lambda @Edge).
- Las siguientes restricciones se aplica si una función crea o actualiza una cadena de consulta:
  - La cadena de consulta no puede incluir espacios, caracteres de control ni el identificador de fragmento (#).
  - El tamaño total del URI () y la cadena de consulta () debe ser inferior a 8 192 caracteres.
  - Le recomendamos que utilice la codificación de porcentaje para el URI y la cadena de consulta. Para obtener más información, consulte Codificación de URI, cadena de consulta y encabezados.

URI

Si una función cambia la URI de una solicitud, eso no cambia el comportamiento de la caché frente a la solicitud ni el origen al que se reenvía la solicitud.

El tamaño total del URI y la cadena de consulta debe ser inferior a 8192 caracteres.

Codificación de URI, cadena de consulta y encabezados

Los valores de URI, cadena de consulta y encabezados que se pasan a funciones periféricas tienen la codificación UTF-8. La función debe usar la codificación UTF-8 para los valores de URI, cadena de consulta y encabezado que devuelve. La codificación de porcentaje es compatible con la codificación UTF-8.

La siguiente lista explica cómo CloudFront maneja la codificación del URI, la cadena de consulta y los encabezados:

- Cuando los valores de la solicitud tienen la codificación UTF-8, CloudFront reenvía los valores a la función de sin cambiarlos.
- Cuando los valores en la solicitud tienen codificación de caracteres ISO 8859-1, CloudFront convierte los valores a la codificación UTF-8 antes de reenviarlos a su función.
- Si los valores en la solicitud están codificados mediante alguna otra codificación de caracteres, CloudFront supone que tienen la codificación ISO-8859-1 e intenta convertir esa codificación de ISO-8859-1 a UTF-8.

> **Important**
>
> Los caracteres convertidos podrían ser una interpretación inexacta de los valores de la solicitud original. Esto podría hacer que su función o su origen produzcan un resultado no deseado.

Los valores del URI, la cadena de consulta y los encabezados que CloudFront reenvía al origen dependen de si una función cambia los valores:

- Si una función no cambia el URI, la cadena de consulta o el encabezado, CloudFront reenvía los valores que recibió en la solicitud al origen.
- Si la función cambia el URI, la cadena de consulta o el encabezado, CloudFront reenvía los valores con codificación UTF-8.

Microsoft Smooth Streaming

No puede utilizar funciones periféricas con una distribución de CloudFront que esté utilizando para streaming de archivos multimedia que haya transcodificado en formato Microsoft Smooth Streaming.

Etiquetado

No se pueden agregar etiquetas a funciones periféricas. Para obtener más información sobre el etiquetado en CloudFront, consulte Etiquetado de una distribución.

Restricciones en CloudFront Functions

Las siguientes restricciones se aplican solo a CloudFront Functions.

Contenido

- Registros
- Cuerpo de la solicitud
- Uso de credenciales temporales con la API KeyValueStore de CloudFront
- Tiempo de ejecución
- Utilización de cómputo

Para obtener información acerca de las cuotas (anteriormente denominadas límites), consulte Cuotas en CloudFront Functions.

Registros

Los registros de funciones en CloudFront Functions están limitados a 10 KB.

Cuerpo de la solicitud

CloudFront Functions no tiene acceso al cuerpo de la solicitud HTTP.

Uso de credenciales temporales con la API KeyValueStore de CloudFront

Puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales (también conocidas como tokens de sesión). Gracias a los tokens de sesión, podrá asumir temporalmente un rol de AWS Identity and Access Management (IAM) para poder acceder a Servicios de AWS.

Para llamar a la API KeyValueStore de CloudFront, utilice un punto de conexión regional en AWS STS para devolver un token de sesión de la versión 2. Si utiliza el punto de conexión global para AWS STS (`sts.amazonaws.com`), AWS STS generará un token de sesión de la versión 1, que no es compatible con Signature Version 4A (SigV4A). Como resultado, se producirá un error de autenticación.

Para llamar a la API KeyValueStore de CloudFront, puede utilizar las siguientes opciones:

SDK de AWS CLI y AWS

Puede configurar la AWS CLI o un SDK de AWS para utilizar puntos de conexión de AWS STS regionales. Para obtener más información, consulte Puntos de conexión regionalizados de AWS STS en la Guía de referencia de AWS SDK y las herramientas.

Para obtener más información sobre los puntos de conexión de AWS STS disponibles, consulte Regiones y puntos de conexión en la Guía del usuario de IAM.

SAML

Puede configurar SAML para utilizar puntos de conexión de AWS STS regionales. Para obtener más información, consulte la entrada de blog How to use regional SAML endpoints for failover.

API **`SetSecurityTokenServicePreferences`**

En lugar de utilizar un punto de conexión de AWS STS regional, puede configurar el punto de conexión global para que AWS STS devuelva tokens de sesión de la versión 2. Para ello, utilice la operación de la API SetSecurityTokenServicePreferences para configurar la Cuenta de AWS.

Example Ejemplo: Comando de la CLI de IAM

```
aws iam set-security-token-service-preferences --global-endpoint-token-version
 v2Token
```

> **Tip**
>
> Le recomendamos que utilice los puntos de conexión regionales de AWS STS en lugar de esta opción. Los puntos de conexión regionales proporcionan una mayor disponibilidad y escenarios de conmutación por error.

Proveedor de identidades personalizado

Si está utilizando un proveedor de identidades personalizado que realiza la federación y asume el rol, utilice una de las opciones anteriores para el sistema del proveedor de identidades principal que es responsable de generar el token de sesión.

Tiempo de ejecución

El entorno de tiempo de ejecución de CloudFront Functions no admite la evaluación dinámica del código y restringe el acceso a la red, al sistema de archivos, a las variables de entorno y a los temporizadores. Para obtener más información, consulte Características restringidas.

> **Note**
>
> Para usar CloudFront KeyValueStore, la función de CloudFront debe usar el tiempo de ejecución 2.0 de JavaScript.

Utilización de cómputo

CloudFront Functions tiene un límite en el tiempo que pueden tardar en ejecutarse, que se mide como Utilización de cómputo. La utilización de cómputo es un número entre 0 y 100 que indica la cantidad de tiempo que la función tardó en ejecutarse como porcentaje del tiempo máximo permitido. Por ejemplo, una utilización de cómputo de 35 significa que la función se completó en 35 % del tiempo máximo permitido.

Cuando prueba una función, puede ver el valor de utilización de cómputo en la salida del evento de prueba. Para las funciones de producción, puede ver la Métrica de utilización de cómputo en la página de Monitoring (Monitorización) de la consola de CloudFront o en CloudWatch.

Restricciones de Lambda @Edge

Las siguientes restricciones se aplican solo a Lambda @Edge.

Contenido

- Resolución de los DNS
- HTTP status codes

- Versión de función de Lambda
- Región de Lambda
- Permisos de rol de Lambda
- Características de Lambda
- Tiempos de ejecución admitidos
- Encabezados CloudFront
- Restricciones para el cuerpo de la solicitud con la opción Incluir cuerpo
- Tiempo de espera de respuesta y tiempo de espera de keep-alive (solo orígenes personalizados)

Para obtener información sobre cuotas, consulte Cuotas de Lambda@Edge.

Resolución de los DNS

CloudFront realiza una resolución DNS en el nombre de dominio de origen antes de ejecutar la función de Lambda@Edge de solicitud de origen. Si el servicio DNS del dominio tiene problemas y CloudFront no puede resolver el nombre de dominio para obtener la dirección IP, la función de Lambda@Edge no se invocará. CloudFront devolverá un código de estado HTTP 502 (puerta de enlace incorrecta) al cliente. Para obtener más información, consulte Error de DNS (`NonS3OriginDnsError`).

Si la lógica de la función modifica el nombre de dominio de origen, CloudFront realizará otra resolución de DNS en el nombre de dominio actualizado después de que la función haya terminado de ejecutarse.

Para obtener más información sobre la administración de la conmutación por error de DNS, consulte Configuring DNS failover en la Guía para desarrolladores de Amazon Route 53.

HTTP status codes

Las funciones de Lambda@Edge para eventos de respuesta de lector no pueden modificar el código de estado HTTP de la respuesta, independientemente de si la respuesta proviene del origen o de la caché de CloudFront.

Versión de función de Lambda

Debe usar una versión numerada de la función de Lambda, no `$LATEST` o alias.

Región de Lambda

La función de Lambda debe estar en la región EE. UU. Este (Norte de Virginia).

Permisos de rol de Lambda

El rol de la ejecución de IAM asociado a la función de Lambda debe permitir que lo asuman las entidades principales del servicio `lambda.amazonaws.com` y `edgelambda.amazonaws.com`. Para obtener más información, consulte Configuración de permisos y roles de IAM para Lambda@Edge.

Características de Lambda

Lambda @Edge no admite las siguientes características de Lambda:

- Configuraciones de administración del tiempo de ejecución de Lambda distintas de Auto (predeterminada)
- Configuración de la función de Lambda para obtener acceso a recursos en la VPC
- Colas de mensajes fallidos de la función de Lambda
- Variables de entorno de Lambda (excepto las variables de entorno reservadas, que se admiten automáticamente)
- Lambda funciona con Administración de dependencias de AWS Lambda con capas
- Mediante AWS X-Ray
- Simultaneidad aprovisionada de Lambda

> **Note**
>
> Las funciones de Lambda@Edge comparten las mismas capacidades de simultaneidad regional que todas las funciones de Lambda. Para obtener más información, consulte Cuotas de Lambda@Edge.

- Creación de una función de Lambda con una imagen de contenedor
- Funciones de Lambda que utilizan la arquitectura arm64
- Funciones de Lambda con más de 512 MB de almacenamiento efímero
- Uso de una clave administrada por el cliente para cifrar los paquetes de implementación .zip

Tiempos de ejecución admitidos

Lambda@Edge admite las versiones más recientes de los tiempos de ejecución de Node.js y Python. Para obtener una lista de las versiones compatibles y sus futuras fechas de obsolescencia, consulte Tiempos de ejecución compatibles en la Guía para desarrolladores de AWS Lambda.

> **Tip**
>
> - Como práctica recomendada, utilice las últimas versiones de los tiempos de ejecución proporcionados para obtener mejoras en el rendimiento y nuevas características.
> - No puede crear ni actualizar funciones con las versiones obsoletas de Node.js. Solo puede asociar las funciones existentes a estas versiones con las distribuciones de CloudFront. Las funciones con estas versiones que están asociadas a las distribuciones continúan ejecutándose. Sin embargo, le recomendamos que traslade la función a versiones más recientes de Node.js. Para obtener más información, consulte Política de obsolescencia del tiempo de ejecución en la Guía para desarrolladores de AWS Lambda y la programación de versiones de Node.js en GitHub.

Encabezados CloudFront

Las funciones de Lambda@Edge pueden leer, editar, eliminar o agregar cualquiera de los siguientes encabezados de CloudFront enumerados en Añadido de encabezados de solicitudes de CloudFront.

> **Notas**
>
> - Si desea que CloudFront agregue estos encabezados, debe configurar CloudFront para que los agregue mediante una política de caché o una política de solicitud de origen.
> - CloudFront agrega los encabezados después del evento de solicitud de lector, lo que significa que los encabezados no están disponibles para las funciones de Lambda @Edge en una solicitud de lector. Los encabezados solo están disponibles para las funciones de Lambda @Edge en una solicitud de origen y una respuesta de origen.
> - Si la solicitud de lector incluye encabezados que tienen estos nombres y configuró CloudFront para que agregue estos encabezados mediante una Política de caché o una Política de solicitud de origen, CloudFront sobrescribe los valores de los encabezados que estaban en la solicitud de lector. Las funciones orientadas al lector ven el valor del

encabezado de la solicitud de lector, mientras que las funciones orientadas al origen ven el valor de encabezado que CloudFront agregó.

- Si una función de solicitud de lector agrega el encabezado `CloudFront-Viewer-Country`, la solicitud no supera la validación de CloudFront y devuelve el código de estado HTTP 502 (puerta de enlace incorrecta) al lector.

Restricciones para el cuerpo de la solicitud con la opción Incluir cuerpo

Cuando elija la opción Incluir cuerpo para exponer el cuerpo de la solicitud a la función de Lambda@Edge, se aplican la siguiente información y los siguientes límites de tamaño para las partes del cuerpo que se exponen o reemplazan.

- CloudFront siempre codifica con base64 el cuerpo de la solicitud antes de exponerlo a Lambda @Edge.
- Si el cuerpo de la solicitud es grande, CloudFront lo limita antes de exponerlo a Lambda@Edge, del siguiente modo:
  - Para los eventos de solicitudes de lector, el cuerpo está limitado a 40 KB.
  - Para las solicitudes de origen, el cuerpo está limitado a 1 MB.
- Si tiene acceso al cuerpo de la solicitud como de solo lectura, CloudFront devuelve el cuerpo completo de la solicitud original al origen.
- Si la función de Lambda @Edge reemplaza el cuerpo de la solicitud, se aplican los siguientes límites de tamaño al cuerpo que devuelve la función:
  - Si la función Lambda @Edge devuelve el cuerpo como texto sin formato:
    - Para los eventos de solicitudes de lector, el límite del cuerpo es 40 KB.
    - Para los eventos de solicitudes de origen, el límite del cuerpo es 1 MB.
  - Si la función Lambda @Edge devuelve el cuerpo como texto codificado con base64:
    - Para los eventos de solicitudes de lector, el límite del cuerpo es 53,2 KB.
    - Para los eventos de solicitudes de origen, el límite del cuerpo es 1,33 MB.

> **Note**
>
> Si la función de Lambda@Edge devuelve un cuerpo que supera estos límites, la solicitud producirá un error con un código de estado HTTP 502 (Error de validación de Lambda). Le

recomendamos que actualice la función Lambda@Edge para que el cuerpo no supere estos límites.

Tiempo de espera de respuesta y tiempo de espera de keep-alive (solo orígenes personalizados)

Si utiliza las funciones de Lambda@Edge para establecer el tiempo de espera de respuesta o el tiempo de espera de keep-alive para sus orígenes de distribución, compruebe que está especificando un valor que su origen pueda admitir. Para obtener más información, consulte Cuotas de tiempo de espera de respuesta y de keep-alive.

Informes, métricas y registros

CloudFront ofrece varias opciones para generar informes, supervisar y registrar los recursos de CloudFront. Puede completar las tareas siguientes:

- Consulte y descargue informes para ver el uso y la actividad de las distribuciones de CloudFront, como informes de facturación, estadísticas de caché, contenido popular y principales remitentes.
- Supervise y realice un seguimiento de CloudFront, incluidas las funciones informáticas periféricas, directamente en la consola de CloudFront o mediante Amazon CloudWatch. CloudFront envía métricas a CloudWatch para distribuciones y funciones periféricas, Lambda@Edge y CloudFront Functions.
- Consulte los registros de las solicitudes de los espectadores que reciben las distribuciones de CloudFront con registros estándar o registros de acceso en tiempo real. Además de los registros de solicitudes de los espectadores, puede usar CloudWatch Logs para obtener registros de las funciones perimetrales de Lambda@Edge y de CloudFront Functions. También puede utilizar la AWS CloudTrail para obtener registros de la actividad de la API de CloudFront en la Cuenta de AWS.
- Realice un seguimiento de los cambios de configuración en los recursos de CloudFront mediante AWS Config.

Para obtener más información sobre estas opciones, consulte los siguientes temas.

Temas

- Informes de uso y facturación de AWS para CloudFront
- Visualización de informes de CloudFront en la consola
- Supervisión de métricas de CloudFront con Amazon CloudWatch
- Registro de funciones de CloudFront y perimetrales
- Realización de un seguimiento de los cambios en la configuración con AWS Config

Informes de uso y facturación de AWS para CloudFront

AWS proporciona dos informes de uso de CloudFront:

- El informe de facturación de AWS es una vista general de toda la actividad deServicios de AWS que utiliza, incluido CloudFront.

- El informe de uso de AWS es un resumen de la actividad de un servicio específico, agrupado por hora, día o mes. También incluye gráficos de uso que proporcionan una representación gráfica del uso de CloudFront.

> **Note**
>
> Al igual que ocurre con otros Servicios de AWS, CloudFront cobra solo por lo que utiliza. Para obtener más información, consulte los precios de CloudFront.

Temas

- Visualización del informe de facturación de AWS para CloudFront
- Visualización del informe de uso de AWS para CloudFront
- Interpretación de la factura de AWS y de los informes de uso de CloudFront

Visualización del informe de facturación de AWS para CloudFront

Puede ver un resumen del uso de AWS y los cargos, enumerados por servio, en la página Bills de la consola de Administración de facturación y costos de AWS.

Visualización del informe de facturación de AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Administración de facturación y costos de AWS en https://console.aws.amazon.com/costmanagement/.
2. En el panel de navegación, seleccione Facturas.
3. Elija un Período de facturación (por ejemplo, agosto de 2023).
4. En la pestaña Cargos por servicio, elija CloudFront y, a continuación, expanda Global o el nombre de Región de AWS.
5. Para descargar un informe de facturación detallado en formato CSV, seleccione Descargar todo en CSV.

Para obtener más información sobre la factura de AWS, consulte Viewing your bill en la Guía del usuario de AWS Billing.

El informe de facturación incluye los siguientes valores que se aplican a CloudFront:

- ProductCode: `AmazonCloudFront`
- UsageType: uno de los siguientes valores:
  - Un código que identifica el tipo de transferencia de datos.
  - `Invalidations`
  - `Executions-CloudFrontFunctions`
  - `KeyValueStore-APIOperations`
  - `KeyValueStore-EdgeReads`
  - `RealTimeLog-KinesisDataStream`
  - `SSL-Cert-Custom`
- ItemDescription: una descripción de la tarifa de facturación de UsageType.
- UsageStart Date y UsageEndDate: el día al que se aplica el uso, en horario universal coordinado (UTC).
- UsageQuantity: uno de los siguientes valores:
  - El número de solicitudes durante el periodo especificado.
  - La cantidad de datos transferidos en gigabytes.
  - La cantidad de objetos invalidados.
  - La suma de los meses prorrateados en los que tuvo certificados SSL asociados con distribuciones de CloudFront habilitadas. Por ejemplo, si tiene un certificado asociado a una distribución habilitada por un mes entero y otro certificado asociado a una distribución habilitado para la mitad del mes, este valor será 1,5.

Visualización del informe de uso de AWS para CloudFront

AWS proporciona un informe de uso de CloudFront más detallado que el de facturación pero menos que los registros de acceso de CloudFront. El informe de uso proporciona datos de uso por hora, día o mes, y se enumeran las operaciones por región y tipo de uso, como datos transferidos fuera de la región de Australia.

Visualización del informe de uso de AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Administración de facturación y costos de AWS en https://console.aws.amazon.com/costmanagement/.
2. En el panel de navegación, seleccione Explorador de costos.

3. En la página Nuevo informe de costo y uso, en el panel Parámetros del informe, elija un rango de fechas y un grado de detalle para el informe.
4. En Filtros, Servicio, seleccione CloudFront.
5. Seleccione el Tipo de uso.
6. En Desglose de costos y usos, seleccione Descargar como CSV.

Para obtener más información sobre el informe de uso de AWS, consulte Informe de uso de AWS en la Guía del usuario de Exportaciones de datos de AWS.

El informe de uso de CloudFront incluye los siguientes valores:

- Servicio – `AmazonCloudFront`
- Operation: método HTTP. Entre los valores se incluyen `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST` y `PUT`.
- UsageType: uno de los siguientes valores:
  - Un código que identifica el tipo de transferencia de datos.
  - `Invalidations`
  - `Executions-CloudFrontFunctions`
  - `KeyValueStore-APIOperations`
  - `KeyValueStore-EdgeReads`
  - `RealTimeLog-KinesisDataStream`
  - `SSL-Cert-Custom`
- Resource: el ID de la distribución de CloudFront asociada con el uso o el ID de un certificado SSL que haya asociado a una distribución de CloudFront.
- StartTime/EndTime: el día correspondiente al uso en horario universal coordinado (UTC).
- UsageValue: 1) la cantidad de solicitudes durante el periodo especificado o 2) la cantidad de datos transferidos en bytes.

Si utiliza Amazon S3 como origen de CloudFront, considere la posibilidad de ejecutar también el informe de uso de Amazon S3. Sin embargo, si utiliza Amazon S3 para fines que no sean de origen de distribución de CloudFront, es posible que no esté claro qué parte se aplica al uso de CloudFront.

> **Tip**
>
> Para obtener información detallada acerca de cada solicitud que CloudFront recibe de sus objetos, active los registros de acceso de CloudFront de su distribución. Para obtener más información, consulte the section called “Registros de acceso (registros estándar)”.

ePara obtener más información sobre cómo entender los tipos de uso y cargos de CloudFront en sus informes, consulte the section called “Interpretación de la factura de AWS y de los informes de uso de CloudFront”.

Interpretación de la factura de AWS y de los informes de uso de CloudFront

Una vez que tenga el informe de facturación y el informe de uso, puede usar este tema para entender cómo interpretar cada cargo de CloudFront que aparece en su factura y el tipo de uso correspondiente a cada cargo. En este tema se incluyen los códigos y abreviaturas de Región de AWS que pueden aparecer en ambos informes.

La mayoría de códigos de ambas columnas incluyen una abreviatura de dos letras que indica la ubicación de la actividad. En la siguiente tabla, la *región* de un código se sustituirá en su factura de AWS y en el informe de uso por una de las siguientes abreviaturas de dos letras:

- AP: Hong Kong, Filipinas, Corea del Sur, Taiwán, y Singapur (Asia Pacífico)
- AU: Australia
- CA: Canadá
- UE: Europa e Israel
- IN: India
- JP: Japón
- ME: Oriente Medio
- SA: América del Sur
- US: Estados Unidos
- ZA: Sudáfrica

Para obtener más información acerca de los precios por Región de AWS, consulte Precios de Amazon CloudFront.

Notas

- En esta tabla no se incluyen cargos por transferencia de objetos desde un bucket de Amazon S3 a ubicaciones de borde de CloudFront. Estos cargos, de haberlos, aparecen en la sección Transferencia de datos de AWS de la factura de AWS.
- En la primera columna se enumeran los cargos que aparecen en su informe de facturación de AWS y se explican sus significados.
- En la segunda columna de la tabla se enumeran los elementos que aparecen en el informe de uso de AWS y se muestra la correlación entre los cargos de la factura y los elementos del informe de uso.

Cargos de CloudFront en su factura de AWS	Valores de la columna UsageType del informe de uso de AWS
región-DataTransfer-Out-Bytes Total de bytes enviados desde las ubicacion es de borde de CloudFront en *región* en respuesta a las solicitudes `GET` y `HEAD` de usuario.	*región*-Out-Bytes-HTTP-Static: Bytes enviados por HTTP para objetos con un TTL ≥ 3600 segundos. *región*-Out-Bytes-HTTPS-Static: Bytes enviados por HTTPS para objetos con un TTL ≥ 3600 segundos. *región*-Out-Bytes-HTTP-Dynamic: Bytes enviados por HTTP para objetos con un TTL < 3600 segundos. *región*-Out-Bytes-HTTPS-Dynamic: Bytes enviados por HTTPS para objetos con un TTL < 3600 segundos. *región*-Out-Bytes-HTTP-Proxy:

Cargos de CloudFront en su factura de AWS	Valores de la columna UsageType del informe de uso de AWS
	Bytes devueltos desde CloudFront a los espectadores por HTTP en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`. *`región`*-Out-Bytes-HTTPS-Proxy: Bytes devueltos desde CloudFront a los espectadores por HTTPS en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`. Esto incluye los bytes devueltos por CloudFront a los espectadores mediante gRPC.
`región`-DataTransfer-Out-OBytes Total de bytes transferidos desde las ubicacion es periféricas de CloudFront al origen o función perimetral en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`. Los cargos incluyen la transferencia de datos para datos de WebSocket de cliente a servidor.	*`región`*-Out-OBytes-HTTP-Proxy Total de bytes transferidos por HTTP desde las ubicaciones periféricas de CloudFront al origen o función periférica en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`. *`región`*-Out-OBytes-HTTPS-Proxy Total de bytes transferidos por HTTPS desde las ubicaciones periféricas de CloudFront al origen o función periférica en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`. Esto incluye los bytes transferidos por gRPC desde las ubicaciones periféricas de CloudFron t al origen o a CloudFront Functions.

Cargos de CloudFront en su factura de AWS	Valores de la columna UsageType del informe de uso de AWS
región-Requests-Tier1 Número de solicitudes HTTP `GET` y `HEAD`.	*región*-Requests-HTTP-Static Número de solicitudes HTTP `GET` y `HEAD` para las que se han enviado objetos con TTL ≥ 3600 segundos. *región*-Requests-HTTP-Dynamic Número de solicitudes HTTP `GET` y `HEAD` para las que se han enviado objetos con TTL < 3600 segundos.
región-Requests-Tier2-HTTPS Número de solicitudes HTTPS `GET` y `HEAD`.	*región*-Requests-HTTPS-Static Número de solicitudes HTTPS `GET` y `HEAD` para las que se han enviado objetos con TTL ≥ 3600 segundos. *región*-Requests-HTTPS-Dynamic Número de solicitudes HTTPS `GET` y `HEAD` para las que se han enviado objetos con TTL < 3600 segundos.
región-Requests-HTTP-Proxy Número de solicitudes HTTP `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT` que CloudFront reenvía al origen o función periférica. También incluye el número de solicitudes de WebSocket HTTP (solicitudes `GET` con el encabezado `Upgrade: websocket`) que CloudFront reenvía al origen o a la función de periferia.	*región*-Requests-HTTP-Proxy Igual que el elemento correspondiente en la factura de CloudFront.

Cargos de CloudFront en su factura de AWS	Valores de la columna UsageType del informe de uso de AWS
región-Requests-HTTPS-Proxy Número de solicitudes HTTPS `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT` que CloudFront reenvía al origen o función periférica. Incluye también los siguientes tipos de solicitud : • El número de solicitudes de WebSocket HTTPS (solicitudes `GET` con el encabezad o `Upgrade: websocket`) que CloudFront reenvía al origen o a la función de periferia. • La cantidad de solicitudes HTTPS gRPC.	*región*-Requests-HTTPS-Proxy Igual que el elemento correspondiente en la factura de CloudFront.
región-Requests-HTTPS-Proxy-FLE Número de solicitudes HTTPS `DELETE`, `OPTIONS`, `PATCH` y `POST` procesadas con cifrado de nivel de campo que CloudFront reenvía al origen o función periférica.	*región*-Requests-HTTPS-Proxy-FLE Igual que el elemento correspondiente en la factura de CloudFront.
región-Bytes-OriginShield Total de bytes transferidos desde el origen a cualquier caché perimetral regional, incluida la caché perimetral regional que esté habilitada como escudo de origen.	*región*-Bytes-OriginShield Igual que el elemento correspondiente en la factura de CloudFront.

Cargos de CloudFront en su factura de AWS	Valores de la columna UsageType del informe de uso de AWS
región-Bytes-OriginShield Total de bytes transferidos desde el origen a cualquier caché perimetral regional, incluida la caché perimetral regional que esté habilitada como escudo de origen.	*región*-Bytes-OriginShield Igual que el elemento correspondiente en la factura de CloudFront.
región-Requests-OriginShield Número de solicitudes que van al escudo de origen como capa incremental. Para las solicitudes dinámicas (no almacenables en caché) que se envían como proxy al origen, el escudo de origen es siempre una capa incremental. Para las solicitudes que se pueden almacenar en caché, el escudo de origen es a veces una capa incremental. Para obtener más información, consulte the section called “Estimación de los costos de Origin Shield”.	*región*-Requests-OriginShield Igual que el elemento correspondiente en la factura de CloudFront.
Invalidaciones El cargo por invalidación de objetos (eliminar los objetos de las ubicaciones periféricas de CloudFront). Para obtener más información, consulte Cargos por invalidación de archivo.	Invalidaciones Igual que el elemento correspondiente en la factura de CloudFront.

Cargos de CloudFront en su factura de AWS	Valores de la columna UsageType del informe de uso de AWS
SSL-Cert-Custom El cargo por el uso de un certificado SSL con un nombre de dominio alternativo de CloudFron t como example.com en lugar del certifica do SSL predeterminado de CloudFront y el nombre de dominio que CloudFront asignó a la distribución.	SSL-Cert-Custom Igual que el elemento correspondiente en la factura de CloudFront.
RealTimeLog-KinesisDataStream El cargo por el número de líneas generadas para los registros en tiempo real.	RealTimeLog-KinesisDataStream Igual que el elemento correspondiente en la factura de CloudFront.
Executions-CloudFrontFunctions El cargo por el número de invocaciones de CloudFront Functions.	Executions-CloudFrontFunctions Igual que el elemento correspondiente en la factura de CloudFront.
region-Lambda-Edge-Request El cargo por el número de invocaciones de la función Lambda@Edge.	***region***-Lambda-Edge-Request Igual que el elemento correspondiente en la factura de CloudFront.
región -Lambda-Edge-GB-Second El cargo durante el período comprendido entre la invocación de la función Lambda@Edge y el momento en que se devuelve o finaliza.	***region***-Lambda-Edge-GB-Second Igual que el elemento correspondiente en la factura de CloudFront.
KeyValueStore-EdgeReads El cargo por el número de llamadas de lectura a los métodos CloudFront KeyValueStore, `get()`, `exists()` y `meta()`. Para obtener más información, consulte Métodos auxiliares para almacenes de clave-valor.	KeyValueStore-EdgeReads Igual que el elemento correspondiente en la factura de CloudFront.

Cargos de CloudFront en su factura de AWS	Valores de la columna UsageType del informe de uso de AWS
KeyValueStore-APIOperations El cargo por el número de llamadas a la API de CloudFront KeyValueStore.	KeyValueStore-APIOperations Igual que el elemento correspondiente en la factura de CloudFront.

Visualización de informes de CloudFront en la consola

Cada informe proporciona datos detallados y visualizaciones, para que pueda optimizar la entrega de contenidos, identificar los cuellos de botella en el rendimiento y tomar decisiones basadas en datos. Tanto si necesita monitorear la eficiencia de la caché, analizar los patrones de tráfico o comprender mejor a sus lectores, puede utilizar estos informes para monitorear y analizar eficazmente las distribuciones de CloudFront.

Puede ver los siguientes informes de su actividad de CloudFront en la consola:

Temas

- Visualización de informes estadísticos de la caché de CloudFront
- Visualización de informes de objetos populares de CloudFront
- Visualización de informes de remitentes principales de CloudFront
- Visualización de informes de uso de CloudFront
- Visualización de informes de espectadores de CloudFront

La mayoría de estos informes se basa en los datos de los registros de acceso de CloudFront, que contienen información detallada sobre cada solicitud de usuario que CloudFront recibe. No es necesario habilitar los registros de acceso para ver los informes. Para obtener más información, consulte Registros de acceso (registros estándar).

Visualización de informes estadísticos de la caché de CloudFront

El informe de estadísticas de caché de Amazon CloudFront muestra la siguiente información:

- Solicitudes totales: la cantidad total de solicitudes de todos los códigos de estado HTTP (por ejemplo, 200 o 404) y todos los métodos (por ejemplo, GET, HEAD o POST)

- Porcentaje de solicitudes de lector por tipo de resultado: los aciertos, los errores como porcentaje del total de solicitudes de lector para la distribución de CloudFront seleccionada
- Bytes transferidos a los lectores: la cantidad total de bytes y la de bytes de errores
- Códigos de estado HTTP: las solicitudes de lector por código de estado HTTP
- Porcentaje de solicitudes GET que no terminaron de descargar: las solicitudes GET de lector que no terminaron de descargar el objeto solicitado, como un porcentaje del total

Los datos de estas estadísticas proceden de la misma fuente que los registros de acceso de CloudFront. Sin embargo, no es necesario habilitar el registro de accesos para ver las estadísticas de caché.

Puede visualizar gráficos durante un intervalo de tiempo especificado dentro de los últimos 60 días, con puntos de datos cada hora o cada día. Generalmente puede ver datos sobre las solicitudes que CloudFront ha recibido tan recientemente como durante la hora anterior, pero en ocasiones es posible que los datos se retrasen hasta 24 horas.

Temas

- Visualización de informes estadísticos de la caché de CloudFront en la consola
- Descarga de datos en formato CSV
- Cómo los gráficos estadísticos de caché están relacionados con los datos contenidos en los registros estándar (registros de acceso) de CloudFront

Visualización de informes estadísticos de la caché de CloudFront en la consola

Puede ver el informe estadístico de la caché de CloudFront en la consola.

Visualización del informe estadístico de la caché de CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, haga clic en Estadísticas de caché.
3. En el panel CloudFront Cache Statistics Reports (Informes de estadísticas de caché de CloudFront), en Start Date (Fecha de inicio) y End Date (Fecha de finalización), seleccione el intervalo de fechas cuyos gráficos de estadísticas desea ver. Los intervalos disponibles dependen del valor seleccionado en Granularity (Grado de detalle):

- Daily (Por día): para ver gráficos con un punto de datos por día, seleccione un intervalo de fechas dentro de los últimos 60 días.
- Hourly (Por hora): para ver gráficos con un punto de datos por cada hora, seleccione un intervalo de fechas igual o inferior a 14 días en los últimos 60 días.

Las fechas y horas se muestran según la hora universal coordinada (UTC).

4. En Granularity (Grado de detalle), especifique si mostrar un punto de datos por día o por hora en los gráficos. Si especifica un intervalo de fechas de más de 14 días, la opción de especificar un punto de datos por hora no estará disponible.
5. En Viewer Location (Ubicación del espectador), elija el continente desde el que se originaron las solicitudes de los espectadores o elija All Locations (Todas las ubicaciones). Los gráficos de estadísticas de caché incluyen los datos de las solicitudes que CloudFront haya recibido desde la ubicación especificada.
6. En la lista Distribution (Distribución), seleccione las distribuciones cuyos datos desea visualizar en los gráficos de uso:
   - Una distribución individual: los gráficos muestran los datos de la distribución web de CloudFront seleccionada. La lista Distribution (Distribución) muestra el ID de distribución y los nombres de dominio alternativos (CNAME), de haberlos. Si una distribución no tiene otros nombres de dominio, la lista incluye los nombres de dominio de origen para la distribución.
   - Todas las distribuciones: los gráficos muestran el total de datos de todas las distribuciones web asociadas a la Cuenta de AWS actual, excepto las distribuciones que ha eliminado.
7. Elija Actualizar.

> **Tip**
>
> - Para ver la información contenida en los puntos de datos por día o por hora de un gráfico, pase por encima del punto de datos correspondiente.
> - Para gráficos que muestran los datos transferidos, puede cambiar el escalado vertical a gigabytes, megabytes o kilobytes.

Descarga de datos en formato CSV

Puede descargar el informe cache statistics (estadísticas de caché) en formato CSV. En esta sección se explica cómo hacerlo y describe los valores del informe.

Para descargar el informe cache statistics (estadísticas de caché) en formato CSV

1. Mientras consulta el informe de estadísticas de caché, seleccione CSV.
2. En el cuadro de diálogo Opening file name (Abriendo nombre de archivo), decida si desea abrir o guardar el archivo.

Información acerca del informe

Las primeras filas del informe incluyen la siguiente información:

Versión

La versión del formato del archivo CSV

Informe

El nombre del informe.

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

StartDateUTC

El principio del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

EndDateUTC

El fin del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

GeneratedTimeUTC

La fecha y hora en ha solicitado el informe, en tiempo universal coordinado (UTC).

Grado de detalle

Define si cada fila del informe representa una hora o un día.

ViewerLocation

El continente desde el que se originan las solicitudes de los espectadores, o `ALL` si ha decidido descargar un informe de todas las ubicaciones.

Datos del informe de estadísticas de caché

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

ViewerLocation

El continente desde el que se originan las solicitudes de los espectadores, o `ALL` si ha decidido descargar un informe de todas las ubicaciones.

TimeBucket

La hora o la fecha a la que son aplicables los datos, en tiempo universal coordinado (UTC).

RequestCount

La cantidad total de solicitudes de todos los códigos de estado HTTP (por ejemplo, 200 o 404) y todos los métodos (por ejemplo, GET, HEAD o POST).

HitCount

La cantidad de solicitudes de lectores para las que se ofrece el objeto desde una caché de borde de CloudFront.

MissCount

La cantidad de solicitudes de lectores para las cuales el objeto no se encuentra actualmente en una caché de borde, por lo que CloudFront debe obtener el objeto desde su origen.

ErrorCount

La cantidad de solicitudes de lectores que generaron un error, por lo que CloudFront no pudo servir el objeto.

IncompleteDownloadCount

La cantidad de solicitudes de espectadores comenzadas por ellos mismos, pero en las que no terminó de descargarse el objeto.

HTTP2xx

La cantidad de solicitudes de espectadores cuyo valor de código de estado HTTP fue 2xx (realizado correctamente).

HTTP3xx

La cantidad de solicitudes de espectadores cuyo valor de código de estado HTTP fue 3xx (acción adicional requerida).

HTTP4xx

La cantidad de solicitudes de espectadores cuyo valor de código de estado HTTP fue 4xx (error del cliente).

HTTP5xx

La cantidad de solicitudes de espectadores cuyo valor de código de estado HTTP fue 5xx (error del servidor).

TotalBytes

La cantidad total de bytes enviados por CloudFront a los lectores en respuesta a todas las solicitudes para todos los métodos de HTTP.

BytesFromMisses

La cantidad de bytes enviados a espectadores para objetos que no estaban en la caché perimetral en el momento de la solicitud. Este valor es una buena estimación de los bytes transferidos desde el origen hasta las cachés de borde de CloudFront. Sin embargo, excluye las solicitudes de objetos que ya están en la caché perimetral, pero que han caducado.

Cómo los gráficos estadísticos de caché están relacionados con los datos contenidos en los registros estándar (registros de acceso) de CloudFront

La siguiente tabla muestra cómo gráficos de estadísticas de caché en la consola de CloudFront se corresponden con los valores contenidos en los registros de acceso de CloudFront. Para obtener más información sobre los registros de acceso de CloudFront, consulte Registros de acceso (registros estándar).

Número total de solicitudes

Este gráfico muestra la cantidad total de solicitudes de todos los códigos de estado HTTP (por ejemplo, 200 o 404) y todos los métodos (por ejemplo, `GET`, `HEAD`, or `POST`). El total de solicitudes que se muestran en esta tabla es igual a la cantidad total de solicitudes en los archivos de registro del mismo periodo.

Porcentaje de solicitudes de lector por tipo de resultado

Este gráfico muestra los aciertos, fallos y errores como porcentaje del total de solicitudes de los lectores a la distribución de CloudFront seleccionada:

- Hit (Acierto): una solicitud del lector cuyo objeto se envió desde una caché de borde de CloudFront. En los registros de acceso, estas son solicitudes cuyo valor de `x-edge-response-result-type` es `Hit`.
- Miss (Fallo): una solicitud del lector para la cual el objeto no se encuentra en ese momento en una caché de borde, por lo que CloudFront debe obtener el objeto desde su origen. En los registros de acceso, estas son solicitudes cuyo valor de `x-edge-response-result-type` es `Miss`.
- Error: una solicitud del lector en la que ocurrió un error, por lo que CloudFront no pudo ofrecer el objeto. En los registros de acceso, estas son solicitudes cuyo valor de `x-edge-response-result-type` es `Error`, `LimitExceeded` o `CapacityExceeded`.

El gráfico no incluye visitas de actualización (solicitudes de objetos que están en la caché de borde, pero que han caducado). En los registros de acceso, las visitas de actualización son solicitudes cuyo valor de `x-edge-response-result-type` es `RefreshHit`.

Bytes transferidos a lectores

Este gráfico muestra dos valores:

- Total bytes (Bytes en total): la cantidad total de bytes enviados por CloudFront a los lectores en respuesta a todas las solicitudes para todos los métodos HTTP. En los registros de acceso de

CloudFront, Total Bytes (Bytes en total) es la suma de los valores de la columna `sc-bytes` de todas las solicitudes realizadas durante el mismo periodo.

- Bytes from misses (Bytes de fallos): la cantidad de bytes enviados a los lectores para objetos que no estaban en la caché de borde en el momento de la solicitud. En los registros de acceso de CloudFront, bytes from misses (bytes de fallos) es la suma de los valores de la columna `sc-bytes` de las solicitudes cuyo valor de `x-edge-result-type` es `Miss`. Este valor es una buena estimación de los bytes transferidos desde el origen hasta las cachés de borde de CloudFront. Sin embargo, excluye las solicitudes de objetos que ya están en la caché perimetral, pero que han caducado.

HTTP status codes

Este gráfico muestra las solicitudes de los espectadores por código de estado HTTP. En los registros de acceso de CloudFront, los códigos de estado aparecen en la columna `sc-status`:

- 2xx: la solicitud se ha realizado correctamente.
- 3xx: se requiere una acción adicional. Por ejemplo, 301 (Movido permanentemente) significa que el objeto solicitado se ha movido a otra ubicación.
- 4xx: aparentemente, el cliente ha cometido un error. Por ejemplo, 404 (No encontrado) significa que el cliente solicitó un objeto que no se pudo encontrar.
- 5xx: el servidor de origen no pudo satisfacer la solicitud. Por ejemplo, 503 (Servicio no disponible) significa que el servidor de origen no está disponible en ese momento.

Porcentaje de solicitudes GET que no terminaron la descarga

Este gráfico muestra el porcentaje del total de solicitudes que corresponde a las solicitudes de espectadores `GET` que no terminaron de descargar el objeto solicitado. Normalmente, la descarga de un objeto no finaliza correctamente porque el espectador cancela la descarga, por ejemplo, al hacer clic en un enlace diferente o cerrar el navegador. En los registros de acceso de CloudFront, estas solicitudes tienen un valor de `200` en la columna `sc-status` y un valor de `Error` en la columna `x-edge-result-type`.

Visualización de informes de objetos populares de CloudFront

Consulte el informe de objetos populares de Amazon CloudFront para ver los 50 objetos más populares de una distribución durante un intervalo de tiempo especificado dentro de los últimos 60 días. También puede ver las estadísticas de esos objetos, incluidas las siguientes:

- Número de solicitudes del objeto

- Número de aciertos y errores
- Porcentaje de aciertos
- Número de bytes servidos para los errores
- Total de bytes servidos
- Número de descargas incompletas
- Número de solicitudes por código de estado HTTP (2xx, 3xx, 4xx y 5xx)

Los datos de estas estadísticas proceden de la misma fuente que los registros de acceso de CloudFront. Sin embargo, no es necesario habilitar el registro de accesos para ver objetos populares.

Temas

- Visualización de informes de objetos populares de CloudFront en la consola
- Cómo calcula CloudFront las estadísticas de objetos populares
- Descarga de datos en formato CSV
- Cómo los datos del informe de objetos populares están relacionados con los datos de los registros estándar (registros de acceso) de CloudFront

Visualización de informes de objetos populares de CloudFront en la consola

Puede ver el informe de objetos populares de CloudFront en la consola.

Visualización de objetos populares de una distribución de CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Haga clic en Objetos populares en el panel de navegación.
3. En el panel CloudFront Popular Objects Report (Informe de objetos populares de CloudFront), en Start Date (Fecha de inicio) y End Date (Fecha de finalización), seleccione el intervalo de fechas para el que desea mostrar una lista de objetos populares. Puede elegir cualquier intervalo de fechas de los últimos 60 días.

   Las fechas y horas se muestran según la hora universal coordinada (UTC).
4. En la lista Distribution (Distribución), seleccione la distribución cuya lista de objetos populares desea ver.

5. Elija Actualizar.

Cómo calcula CloudFront las estadísticas de objetos populares

Para obtener un recuento preciso de los 50 objetos más populares en su distribución, CloudFront cuenta las solicitudes de todos los objetos en intervalos de 10 minutos a partir de la medianoche y mantiene un recuento actual de los 150 objetos más populares durante las próximas 24 horas. (CloudFront también retiene los totales diarios de los 150 objetos más populares durante 60 días).

Cerca de la parte inferior de la lista, los objetos suben y bajan puestos constantemente o salen de la lista, así que los totales de dichos objetos son aproximados. Los 50 objetos de la parte superior de la lista de 150 objetos podrían subir o bajar, pero no suelen salir de la lista, así que el total de los objetos de esa parte es más fiable.

Cuando un objeto sale de la lista de los 150 objetos más populares y vuelve a entrar pasado un día, CloudFront agrega un número estimado de solicitudes para el período durante el cual el objeto no estuvo en la lista. La estimación se basa en el número de solicitudes recibidas por cualquier objeto de la parte inferior de la lista durante dicho periodo.

Si el objeto sube a la parte de los primeros 50 objetos más tarde el mismo día, las estimaciones de la cantidad de solicitudes que CloudFront recibió mientras el objeto estaba fuera de la parte de los primeros 150 objetos suele provocar que la cantidad de solicitudes de ese objeto reflejada en el informe de objetos populares sea mayor que la que aparece en los registros de acceso.

Descarga de datos en formato CSV

Puede descargar el informe popular objects (objetos populares) en formato CSV. En esta sección se explica cómo hacerlo y describe los valores del informe.

Para descargar el informe popular objects (objetos populares) en formato CSV

1. Mientras consulta el informe de objetos populares, haga clic en CSV.
2. En el cuadro de diálogo Opening file name (Abriendo nombre de archivo), decida si desea abrir o guardar el archivo.

Información acerca del informe

Las primeras filas del informe incluyen la siguiente información:

Versión

La versión del formato del archivo CSV

Informe

El nombre del informe.

DistributionID

El ID de la distribución para la que ha solicitado el informe.

StartDateUTC

El principio del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

EndDateUTC

El fin del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

GeneratedTimeUTC

La fecha y hora en ha solicitado el informe, en tiempo universal coordinado (UTC).

Datos del informe de objetos populares

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución para la que ha solicitado el informe.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

Objeto

Lo últimos 500 caracteres de la URL del objeto.

RequestCount

La cantidad total de solicitudes de este objeto.

HitCount

La cantidad de solicitudes de lectores para las que se ofrece el objeto desde una caché de borde de CloudFront.

MissCount

La cantidad de solicitudes de lectores para las cuales el objeto no se encuentra actualmente en una caché de borde, por lo que CloudFront debe obtener el objeto desde su origen.

HitCountPct

El valor de `HitCount` como porcentaje del valor de `RequestCount`.

BytesFromMisses

La cantidad de bytes enviados a espectadores para este objeto mientras no estaba en la caché perimetral en el momento de la solicitud.

TotalBytes

La cantidad total de bytes enviados por CloudFront a los lectores para este objeto en respuesta a todas las solicitudes para todos los métodos de HTTP.

IncompleteDownloadCount

La cantidad de solicitudes de ese objeto comenzadas por los espectadores, pero en las que no terminó de descargarse dicho objeto.

HTTP2xx

La cantidad de solicitudes de espectadores cuyo valor de código de estado HTTP fue 2xx (realizado correctamente).

HTTP3xx

La cantidad de solicitudes de espectadores cuyo valor de código de estado HTTP fue 3xx (acción adicional requerida).

HTTP4xx

La cantidad de solicitudes de espectadores cuyo valor de código de estado HTTP fue 4xx (error del cliente).

HTTP5xx

La cantidad de solicitudes de espectadores cuyo valor de código de estado HTTP fue 5xx (error del servidor).

Cómo los datos del informe de objetos populares están relacionados con los datos de los registros estándar (registros de acceso) de CloudFront

La siguiente lista muestra cómo los valores del informe de objetos populares de la consola de CloudFront se corresponden con los valores contenidos en los registros de acceso de CloudFront. Para obtener más información sobre los registros de acceso de CloudFront, consulte Registros de acceso (registros estándar).

URL

Los últimos 500 caracteres de la URL que los espectadores utilizan para obtener acceso al objeto.

Solicitudes

La cantidad total de solicitudes del objeto. Este valor suele corresponderse estrechamente con la cantidad de solicitudes `GET` del objeto en los registros de acceso de CloudFront.

Hits

La cantidad de solicitudes de lectores para las que se envió el objeto desde una caché de borde de CloudFront. En los registros de acceso, estas son solicitudes cuyo valor de `x-edge-response-result-type` es `Hit`.

Misses

La cantidad de solicitudes de lectores para las cuales el objeto no se encontraba en una caché de borde, por lo que CloudFront debe obtener el objeto desde su origen. En los registros de acceso, estas son solicitudes cuyo valor de `x-edge-response-result-type` es `Miss`.

Porcentaje de aciertos

El valor de la columna Hits (Aciertos) como porcentaje del valor de la columna Requests (Solicitudes).

Bytes de fallos

La cantidad de bytes enviados a espectadores para objetos que no estaban en la caché perimetral en el momento de la solicitud. En los registros de acceso de CloudFront, bytes from misses (bytes de fallos) es la suma de los valores de la columna `sc-bytes` de las solicitudes cuyo valor de `x-edge-result-type` es `Miss`.

Bytes en total

La cantidad total de bytes que CloudFront ha enviado a los lectores en respuesta a todas las solicitudes del objeto por todos los métodos HTTP. En los registros de acceso de CloudFront, total bytes (bytes en total) es la suma de los valores de la columna `sc-bytes` de todas las solicitudes realizadas durante el mismo periodo.

Descargas incompletas

La cantidad de solicitudes de espectadores que no terminaron de descargar el objeto solicitado. Normalmente, el motivo de que una descarga no finalice correctamente es que el espectador la haya cancelado, por ejemplo, al hacer clic en un enlace diferente o cerrar el navegador. En los registros de acceso de CloudFront, estas solicitudes tienen un valor de `200` en la columna `sc-status` y un valor de `Error` en la columna `x-edge-result-type`.

2xx

La cantidad de solicitudes cuyo código de estado HTTP es `2xx`, `Successful`. En los registros de acceso de CloudFront, los códigos de estado aparecen en la columna `sc-status`.

3xx

La cantidad de solicitudes cuyo valor de código de estado HTTP es `3xx`, `Redirection`. Los códigos de estado `3xx` indican que se requiere una acción adicional. Por ejemplo, 301 (Movido permanentemente) significa que el objeto solicitado se ha movido a otra ubicación.

4xx

La cantidad de solicitudes cuyo valor de código de estado HTTP es `4xx`, `Client Error`. Los códigos de estado `4xx` indican que el cliente pudo haber cometido un error. Por ejemplo, 404 (No encontrado) significa que el cliente solicitó un objeto que no se pudo encontrar.

5xx

La cantidad de solicitudes cuyo valor de código de estado HTTP es `5xx`, `Server Error`. Los códigos de estado `5xx` indican que el servidor de origen no pudo satisfacer la solicitud. Por ejemplo, 503 (Servicio no disponible) significa que el servidor de origen no está disponible en ese momento.

Visualización de informes de remitentes principales de CloudFront

El informe de los remitentes principales de CloudFront incluye lo siguiente para cualquier intervalo de fechas de los últimos 60 días:

- Los 25 remitentes principales (dominios de los sitios web en los que se originaron la mayoría de solicitudes HTTP y HTTPS de los objetos que CloudFront está enviando para su distribución)
- Número de solicitudes de un remitente
- Cantidad de solicitudes enviadas por el remitente como porcentaje de las solicitudes realizadas en un periodo específico

Los datos del informe de los remitentes principales proceden de la misma fuente que los registros de acceso de CloudFront. Sin embargo, no es necesario habilitar el registro de accesos para ver los principales remitentes.

Los remitentes principales pueden ser motores de búsqueda, otros sitios web que están directamente vinculados con sus objetos o su propio sitio web. Por ejemplo, si `https://example.com/index.html` se vincula a 10 gráficos, `example.com` es el remitente de todos esos gráficos.

> **Note**
>
> Si un usuario escribe una URL directamente en el navegador, no hay remitente para el objeto solicitado.

Temas

- Visualización de informes de remitentes principales de CloudFront en la consola
- Cómo calcula CloudFront las estadísticas de los remitentes principales
- Descarga de datos en formato CSV
- Cómo los datos del informe de remitentes principales están relacionados con los datos de los registros estándar (registros de acceso) de CloudFront

Visualización de informes de remitentes principales de CloudFront en la consola

Puede visualizar los informes de remitentes principales de CloudFront en la consola.

Visualización de los remitentes principales de una distribución de CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, haga clic en Remitentes principales.

3. En el panel CloudFront Top Referrers Report (Informe de remitentes principales de Cloudfront), en Start Date (Fecha de inicio) y End Date (Fecha de finalización), seleccione el intervalo de fechas cuya lista de remitentes principales desee mostrar.

   Las fechas y horas se muestran según la hora universal coordinada (UTC).
4. En la lista Distribution (Distribución), seleccione la distribución cuya lista de remitentes principales desea ver.
5. Elija Actualizar.

Cómo calcula CloudFront las estadísticas de los remitentes principales

Para obtener un conteo preciso de los 25 remitentes principales, CloudFront cuenta las solicitudes de todos los objetos en intervalos de 10 minutos y mantiene un recuento actual de los 75 remitentes principales. Cerca de la parte inferior de la lista, los remitentes suben y bajan puestos constantemente o salen de la lista, así que los totales de dichos remitentes son aproximados.

Los 25 remitentes de la parte superior de la lista de 75 remitentes podrían subir o bajar, pero no suelen salir de la lista, así que el total de los remitentes de esa parte suele ser más fiable.

Descarga de datos en formato CSV

Puede descargar el informe de remitentes principales en formato CSV. En esta sección se explica cómo hacerlo y describe los valores del informe.

Para descargar el informe de remitentes principales en formato CSV

1. Mientras consulta el informe Remitentes principales, haga clic en CSV.
2. En el cuadro de diálogo Opening file name (Abriendo nombre de archivo), decida si desea abrir o guardar el archivo.

Información acerca del informe

Las primeras filas del informe incluyen la siguiente información:

Versión

La versión del formato del archivo CSV

Informe

El nombre del informe.

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

StartDateUTC

El principio del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

EndDateUTC

El fin del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

GeneratedTimeUTC

La fecha y hora en ha solicitado el informe, en tiempo universal coordinado (UTC).

Los datos del informe de remitentes principales

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

Referrer

El nombre del dominio del remitente.

RequestCount

La cantidad total de solicitudes desde el nombre de dominio de la columna `Referrer`.

RequestsPct

La cantidad de solicitudes enviadas por el remitente como porcentaje de las solicitudes realizadas en un periodo específico.

Cómo los datos del informe de remitentes principales están relacionados con los datos de los registros estándar (registros de acceso) de CloudFront

La siguiente lista muestra cómo los valores del informe de remitentes principales de la consola de CloudFront se corresponden con los valores contenidos en los registros de acceso de CloudFront. Para obtener más información sobre los registros de acceso de CloudFront, consulte Registros de acceso (registros estándar).

Referrer

El nombre del dominio del remitente. En los registros de acceso, los remitentes se enumeran en la columna `cs(Referer)`.

Número de solicitudes

La cantidad total de solicitudes desde el nombre de dominio de la columna Referrer (Remitente). Este valor suele corresponderse estrechamente con la cantidad de solicitudes `GET` del remitente en los registros de acceso de CloudFront.

Solicitud %

La cantidad de solicitudes enviadas por el remitente como porcentaje de las solicitudes realizadas en un periodo específico. Si tiene más de 25 remitentes, no podrá calcular el valor Request % (% de solicitudes) en función de los datos de esta tabla, ya que la columna request count (número de solicitudes) no incluye todas las solicitudes del período especificado.

Visualización de informes de uso de CloudFront

Los informes de uso de CloudFront incluyen la siguiente información:

- Number of requests (Cantidad de solicitudes): muestra la cantidad total de solicitudes a las que responde CloudFront desde ubicaciones de borde en la región seleccionada durante cada intervalo de tiempo para la distribución de CloudFront especificada.
- Data transferred by protocol (Datos transferidos por protocolo) y data transferred by destination (datos transferidos por destino): muestra la cantidad total de datos transferidos desde ubicaciones

de borde de CloudFront en la región seleccionada durante cada intervalo de tiempo para la distribución de CloudFront especificada. Separan los datos de manera diferente, como se indica a continuación:

- By protocol (Por protocolo): separa los datos por protocolo: HTTP o HTTPS.
- By destination: separa los datos por destino: a sus usuarios o a su origen.

El informe de uso de CloudFront se basa en el informe de uso de AWS para CloudFront. Este informe no requiere ninguna configuración adicional. Para obtener más información, consulte Visualización del informe de uso de AWS para CloudFront.

Puede visualizar informes para un intervalo de tiempo especificado dentro de los últimos 60 días, con puntos de datos cada hora o cada día. Generalmente puede ver datos de las solicitudes que CloudFront ha recibido tan recientemente como durante las cuatro horas anteriores, pero en ocasiones es posible que los datos se retrasen hasta 24 horas.

Para obtener más información, consulte Cómo los gráficos de uso están relacionados con los datos contenidos en el informe de uso de CloudFront.

Temas

- Visualización de informes de uso de CloudFront en la consola
- Descarga de datos en formato CSV
- Cómo los gráficos de uso están relacionados con los datos contenidos en el informe de uso de CloudFront

Visualización de informes de uso de CloudFront en la consola

Puede ver el informe de uso de CloudFront en la consola.

Visualización de informes de uso de CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Usage Reports (Informes de uso).
3. En el panel CloudFront Usage Reports (Informes de uso de CloudFront), en Start Date (Fecha de inicio) y End Date (Fecha de finalización), seleccione el intervalo de fechas cuyos gráficos de uso desea mostrar. Los intervalos disponibles dependen del valor seleccionado en Granularity (Grado de detalle):

- Daily (Por día): para ver gráficos con un punto de datos por día, seleccione un intervalo de fechas dentro de los últimos 60 días.
- Hourly (Por hora): para ver gráficos con un punto de datos por cada hora, seleccione un intervalo de fechas igual o inferior a 14 días en los últimos 60 días.

Las fechas y horas se muestran según la hora universal coordinada (UTC).

4. En Granularity (Grado de detalle), especifique si mostrar un punto de datos por día o por hora en los gráficos. Si especifica un intervalo de fechas de más de 14 días, la opción de especificar un punto de datos por hora no estará disponible.
5. En Billing Region (Región de facturación), elija la región de facturación de CloudFront que contiene los datos que desea ver o elegir All Regions (Todas las regiones). Los gráficos de uso incluyen los datos de las solicitudes que CloudFront procesa en las ubicaciones de borde en la región especificada. La región en la que CloudFront procesa solicitudes que pueden o no corresponder con la ubicación de los usuarios.

   Seleccione solo regiones que estén incluidas en la clase de precio de su distribución. De lo contrario, los gráficos de uso probablemente no contendrán ningún dato. Por ejemplo, si selecciona la clase de precio 200 para su distribución, las regiones de facturación de América del Sur y Australia no se incluyen por lo que, por lo general, CloudFront no procesará las solicitudes de esas regiones. Para obtener más información acerca de las clases de precios, consulte Precios de CloudFront.
6. En la lista Distribution (Distribución), seleccione las distribuciones cuyos datos desea visualizar en los gráficos de uso:

   - Una distribución individual: los gráficos muestran los datos de la distribución web de CloudFront seleccionada. La lista Distribution (Distribución) muestra el ID de distribución y los nombres de dominio alternativos (CNAME), de haberlos. Si una distribución no tiene otros nombres de dominio, la lista incluye los nombres de dominio de origen para la distribución.
   - Todas las distribuciones (excepto las eliminadas): los gráficos muestran el total de datos de todas las distribuciones web asociadas a la cuenta actual de AWS, excepto las distribuciones web que ha eliminado.
   - Todas las distribuciones eliminadas: los gráficos muestran el total de datos de todas las distribuciones asociadas a la cuenta actual de AWS y que se eliminaron durante los últimos 60 días.
7. Elija Actualizar gráfico.

> **Tip**
>
> - Para ver la información contenida en los puntos de datos por día o por hora de un gráfico, pase por encima del punto de datos correspondiente.
> - Para gráficos que muestran los datos transferidos, tenga en cuenta que puede cambiar el escalado vertical a gigabytes, megabytes o kilobytes.

Descarga de datos en formato CSV

Puede descargar el informe de uso en formato CSV. En esta sección se explica cómo hacerlo y describe los valores del informe.

Para descargar el informe de uso en formato CSV

1. Mientras consulta el informe de uso, seleccione CSV.
2. En el cuadro de diálogo Opening file name (Abriendo nombre de archivo), decida si desea abrir o guardar el archivo.

Información acerca del informe

Las primeras filas del informe incluyen la siguiente información:

Versión

La versión del formato del archivo CSV

Informe

El nombre del informe.

DistributionID

El ID de la distribución del informe solicitado, `ALL` si se ha solicitado el informe de todas las distribuciones o `ALL_DELETED` si se ha solicitado el informe de todas las distribuciones eliminadas.

StartDateUTC

El principio del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

EndDateUTC

El fin del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

GeneratedTimeUTC

La fecha y hora en ha solicitado el informe, en tiempo universal coordinado (UTC).

Grado de detalle

Define si cada fila del informe representa una hora o un día.

BillingRegion

El continente desde el que se han originado las solicitudes de los espectadores; o `ALL` si ha decidido descargar un informe de todas las regiones de facturación.

Datos del informe de uso

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, `ALL` si se ha solicitado el informe de todas las distribuciones o `ALL_DELETED` si se ha solicitado el informe de todas las distribuciones eliminadas.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

BillingRegion

La región de facturación de CloudFront cuyo informe ha solicitado o `ALL`.

TimeBucket

La hora o la fecha a la que son aplicables los datos, en tiempo universal coordinado (UTC).

HTTP

La cantidad de solicitudes HTTP a las que CloudFront ha respondido desde ubicaciones de borde en la región seleccionada durante cada intervalo de tiempo, en la distribución de CloudFront especificada. Entre los valores se encuentran:

- La cantidad de solicitudes `GET` y `HEAD` que activan la transferencia de datos de CloudFront a sus lectores
- La cantidad de solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT` que activan la transferencia de datos de CloudFront a su origen

HTTPS

La cantidad de solicitudes HTTPS a las que CloudFront ha respondido desde ubicaciones de borde en la región seleccionada durante cada intervalo de tiempo, en la distribución de CloudFront especificada. Entre los valores se encuentran:

- La cantidad de solicitudes `GET` y `HEAD` que activan la transferencia de datos de CloudFront a sus lectores
- La cantidad de solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT` que activan la transferencia de datos de CloudFront a su origen

HTTPBytes

La cantidad total de datos transferidos a través de HTTP desde las ubicaciones de borde de CloudFront en la región de facturación seleccionada durante el periodo de tiempo especificado para la distribución de CloudFront. Entre los valores se encuentran:

- Los datos que se han transferido desde CloudFront hasta sus lectores en respuesta a las solicitudes `GET` y `HEAD`
- Los datos que se han transferido desde CloudFront para solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.
- Los datos que se han transferido desde CloudFront hasta sus lectores en respuesta a las solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`

HTTPSBytes

La cantidad total de datos transferidos a través de HTTPS desde las ubicaciones de borde de CloudFront en la región de facturación seleccionada durante el periodo de tiempo especificado para la distribución de CloudFront. Entre los valores se encuentran:

- Los datos que se han transferido desde CloudFront hasta sus lectores en respuesta a las solicitudes `GET` y `HEAD`
- Los datos que se han transferido desde CloudFront para solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.
- Los datos que se han transferido desde CloudFront hasta sus lectores en respuesta a las solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`

BytesIn

La cantidad total de datos transferidos desde CloudFront hasta el origen en respuesta a las solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT` en la región seleccionada durante cada intervalo de tiempo especificado para la distribución de CloudFront.

BytesOut

La cantidad total de datos transferidos a través de HTTP y HTTPS desde CloudFront hasta sus lectores en la región seleccionada durante cada intervalo de tiempo especificado para la distribución de CloudFront. Entre los valores se encuentran:

- Los datos que se han transferido desde CloudFront hasta sus lectores en respuesta a las solicitudes `GET` y `HEAD`
- Los datos que se han transferido desde CloudFront hasta sus lectores en respuesta a las solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`

Cómo los gráficos de uso están relacionados con los datos contenidos en el informe de uso de CloudFront

La siguiente lista muestra cómo el uso de gráficos en la consola de CloudFront se corresponde con los valores de la columna Usage Type (Tipo de uso) del informe de uso de CloudFront.

Temas

- Cantidad de solicitudes
- Datos transferidos por protocolo
- Datos transferidos por destino

Cantidad de solicitudes

Este gráfico muestra la cantidad total de solicitudes a las que responde CloudFront desde ubicaciones de borde en la región seleccionada durante cada intervalo de tiempo para la distribución de CloudFront especificada, separadas por protocolo (HTTP o HTTPS) y tipo (estático, dinámico o proxy).

Cantidad de solicitudes HTTP

- *`región`*-Requests-HTTP-Static: número de solicitudes HTTP `GET` y `HEAD` enviadas para objetos con TTL ≥ 3600 segundos

- *región*-Requests-HTTP-Dynamic: cantidad de solicitudes HTTP `GET` y `HEAD` enviadas de objetos con TTL < 3 600 segundos
- *región*-Requests-HTTP-Proxy: número de solicitudes HTTP `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT` que CloudFront reenvía a su origen

Cantidad de solicitudes HTTPS

- *región*-Requests-HTTPS-Static: número de solicitudes HTTPS `GET` y `HEAD` enviadas para objetos con TTL ≥ 3600 segundos
- *región*-Requests-HTTPS-Dynamic: cantidad de solicitudes HTTPS `GET` y `HEAD` enviadas de objetos con TTL < 3 600 segundos
- *región*-Requests-HTTPS-Proxy: número de solicitudes HTTPS `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT` que CloudFront reenvía a su origen

Datos transferidos por protocolo

Este gráfico muestra la cantidad total de datos transferidos desde ubicaciones de periferia de CloudFront en la región seleccionada durante cada intervalo de tiempo para la distribución de CloudFront especificada, separados por protocolo (HTTP o HTTPS), tipo (estático, dinámico o proxy) y destino (lectores u origen).

Datos transferidos a través de HTTP

- *región*-Out-Bytes-HTTP-Static: bytes enviados por HTTP de objetos con un TTL ≥ 3600 segundos.
- *región*-Out-Bytes-HTTP-Dynamic: bytes enviados por HTTP de objetos con un TTL < 3 600 segundos.
- *región*-Out-Bytes-HTTP-Proxy: bytes devueltos de CloudFront a los lectores por HTTP en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.
- *región*-Out-OBytes-HTTP-Proxy: total de bytes transferidos por HTTP desde las ubicaciones de borde de CloudFront al origen en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.

Datos transferidos a través de HTTPS

- *región*-Out-Bytes-HTTP-Static: bytes enviados por HTTPS de objetos con un TTL ≥ 3600 segundos.
- *región*-Out-Bytes-HTTPS-Dynamic: bytes enviados por HTTPS de objetos con un TTL < 3 600 segundos.

- *región*-Out-Bytes-HTTPS-Proxy: bytes devueltos de CloudFront a los lectores por HTTPS en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.
- *región*-Out-OBytes-HTTPS-Proxy: total de bytes transferidos por HTTPS desde las ubicaciones de borde de CloudFront al origen en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.

Datos transferidos por destino

Este gráfico muestra la cantidad total de datos transferidos desde ubicaciones de periferia de CloudFront en la región seleccionada durante cada intervalo de tiempo para la distribución de CloudFront especificada, separados por destino (lectores u origen), protocolo (HTTP o HTTPS) y tipo (estático, dinámico o proxy).

Datos transferidos de CloudFront a sus lectores

- *región*-Out-Bytes-HTTP-Static: bytes enviados por HTTP de objetos con un TTL ≥ 3600 segundos.
- *región*-Out-Bytes-HTTP-Static: bytes enviados por HTTPS de objetos con un TTL ≥ 3600 segundos.
- *región*-Out-Bytes-HTTP-Dynamic: bytes enviados por HTTP de objetos con un TTL < 3 600 segundos.
- *región*-Out-Bytes-HTTPS-Dynamic: bytes enviados por HTTPS de objetos con un TTL < 3 600 segundos.
- *región*-Out-Bytes-HTTP-Proxy: bytes devueltos de CloudFront a los lectores por HTTP en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.
- *región*-Out-Bytes-HTTPS-Proxy: bytes devueltos de CloudFront a los lectores por HTTPS en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.

Datos transferidos de CloudFront a su origen

- *región*-Out-OBytes-HTTP-Proxy: total de bytes transferidos por HTTP desde las ubicaciones de borde de CloudFront al origen en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.
- *región*-Out-OBytes-HTTPS-Proxy: total de bytes transferidos por HTTPS desde las ubicaciones de borde de CloudFront al origen en respuesta a solicitudes `DELETE`, `OPTIONS`, `PATCH`, `POST` y `PUT`.

Visualización de informes de espectadores de CloudFront

Los informes de espectadores de CloudFront incluyen la siguiente información para cualquier intervalo de fechas de los últimos 60 días:

- Dispositivos: los tipos de dispositivos que se utilizan con más frecuencia para acceder a su contenido (como de escritorio o móviles)
- Navegadores: los 10 navegadores más utilizados para acceder a su contenido (como Chrome o Firefox)
- Sistemas operativos: los 10 sistemas operativos más utilizados para acceder al contenido (como Linux, macOS o Windows)
- Ubicaciones: las 50 ubicaciones (por país o estado o territorio de EE. UU.) de los espectadores que obtienen acceso a su contenido con mayor frecuencia.
  - También puede ver ubicaciones con puntos de datos horarios para cualquier intervalo de fechas de hasta 14 días en los últimos 60 días

> **Note**
>
> No es necesario habilitar el registro de accesos para ver gráficos e informes de lectores.

Temas

- Visualización de gráficos e informes de espectadores en la consola
- Descarga de datos en formato CSV
- Datos incluidos en los informes de espectadores
- Cómo los datos del informe de ubicaciones están relacionados con los datos de los registros estándar (registros de acceso) de CloudFront

Visualización de gráficos e informes de espectadores en la consola

Puede visualizar gráficos e informes de espectadores de CloudFront en la consola.

Visualización de gráficos e informes de espectadores de CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.

2. En el panel de navegación, elija Espectadores.
3. En el panel CloudFront Viewers (Lectores de CloudFront), en Start Date (Fecha de inicio) y End Date (Fecha de finalización), seleccione el intervalo de fechas cuyos gráficos e informes desea mostrar.

   En el gráfico Locations (Ubicaciones), los intervalos disponibles dependen del valor seleccionado en Granularity (Grado de detalle):

   - Daily (Por día): para ver gráficos con un punto de datos por día, seleccione un intervalo de fechas dentro de los últimos 60 días.
   - Hourly (Por hora): para ver gráficos con un punto de datos por cada hora, seleccione un intervalo de fechas igual o inferior a 14 días en los últimos 60 días.

   Las fechas y horas se muestran según la hora universal coordinada (UTC).
4. Solo gráficos de navegadores y de sistemas operativos: en Grouping (Agrupación), especifique si desea agrupar los navegadores y sistemas operativos por nombre (Chrome, Firefox) o bien por nombre y versión (Chrome 40,0, Firefox 35,0).
5. Solo gráfico de ubicaciones: en Granularity (Grado de detalle), especifique si desea mostrar en los gráficos un punto de datos por día o por hora. Si especifica un intervalo de fechas de más de 14 días, la opción de especificar un punto de datos por hora no estará disponible.
6. Solo gráfico de ubicaciones: en Details (Detalles), especifique si desea mostrar las ubicaciones más populares por país o por estados de Estados Unidos.
7. En la lista Distribution (Distribución), seleccione la distribución cuyos datos desea ver en los gráficos de uso:

   - Una distribución individual: los gráficos muestran los datos de la distribución web de CloudFront seleccionada. La lista Distribution (Distribución) muestra el ID de distribución y un nombre de dominio alternativo (CNAME), de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.
   - Todas las distribuciones (excepto las eliminadas): los gráficos muestran el total de datos de todas las distribuciones web asociadas a la cuenta actual de AWS, excepto las distribuciones web que ha eliminado.
8. Elija Actualizar.

Para ver la información contenida en los puntos de datos por día o por hora de un gráfico, pase por encima del punto de datos correspondiente.

Descarga de datos en formato CSV

Puede descargar todos los informes de lectores en formato CSV. En esta sección se explica cómo descargar dichos informes y describe sus valores.

Para descargar informes de lectores en formato CSV

1. Al visualizar el informe de espectadores, haga clic en CSV.
2. Elija los datos que desea descargar, por ejemplo, Devices (Dispositivos) o Devices Trends (Tendencias de dispositivos).
3. En el cuadro de diálogo Opening file name (Abriendo nombre de archivo), decida si desea abrir o guardar el archivo.

Datos incluidos en los informes de espectadores

Las primeras filas de cada informe incluyen la siguiente información:

Versión

La versión del formato del archivo CSV

Informe

El nombre del informe.

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

StartDateUTC

El principio del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

EndDateUTC

El fin del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

GeneratedTimeUTC

La fecha y hora en ha solicitado el informe, en tiempo universal coordinado (UTC).

Grouping (solo en informes de navegadores y de sistemas operativos)

Forma de agrupación de los datos: por el nombre del navegador o sistema operativo, o por su nombre y versión.

Grado de detalle

Define si cada fila del informe representa una hora o un día.

Detalles (solo informe de ubicaciones)

Forma de listar las solicitudes: por país o por estado de los Estados Unidos.

En los siguientes temas, se describe la información de los diferentes informes de espectadores.

Temas

- Informe de dispositivos
- Informe de tendencias de dispositivos
- Informe de navegadores
- Informe de tendencias de navegación
- Informe de sistemas operativos
- Informe de tendencias de sistemas operativos
- Informe de ubicaciones
- Informe de tendencias de ubicación

Informe de dispositivos

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

Solicitudes

La cantidad de solicitudes que CloudFront ha recibido de cada tipo de dispositivo.

RequestsPct

La cantidad de solicitudes que CloudFront ha recibido desde cada tipo de dispositivo como porcentaje del total de solicitudes que CloudFront ha recibido de todos los dispositivos.

Personalizada

Solicitudes cuyo valor del encabezado HTTP `User-Agent` no se asoció con uno de los tipos de dispositivo estándar, por ejemplo, `Desktop` o `Mobile`.

Informe de tendencias de dispositivos

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

TimeBucket

La hora o la fecha a la que son aplicables los datos, en tiempo universal coordinado (UTC).

Escritorio

La cantidad de solicitudes que CloudFront ha recibido desde equipos de escritorio durante el periodo establecido.

Móvil

La cantidad de solicitudes que CloudFront ha recibido desde dispositivos móviles durante el periodo establecido. Entre los dispositivos móviles se pueden incluir tablets y teléfonos móviles. Si CloudFront no puede determinar si una solicitud se ha originado desde un dispositivo móvil o una tableta, se refleja en la columna `Mobile`.

Smart-TV

La cantidad de solicitudes que CloudFront ha recibido desde televisores inteligentes durante el periodo establecido.

Tablet

La cantidad de solicitudes que CloudFront ha recibido desde tabletas durante el periodo establecido. Si CloudFront no puede determinar si una solicitud se ha originado desde un dispositivo móvil o una tableta, se refleja en la columna `Mobile`.

Desconocido

Solicitudes cuyo valor del encabezado HTTP `User-Agent` no se asoció con uno de los tipos de dispositivo estándar, por ejemplo, `Desktop` o `Mobile`.

Vacío

La cantidad de solicitudes que CloudFront ha recibido y que no incluyeron un valor en el encabezado HTTP `User-Agent` durante el periodo establecido.

Informe de navegadores

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

Grupo

El navegador o el navegador y la versión desde los que CloudFront ha recibido solicitudes en función del valor de `Grouping`. Además de los nombres de los navegadores, otros valores son:

- Bot/Crawler (Bot/Rastreador): sobre todo solicitudes de motores de búsqueda que están indexando su contenido.
- Empty (Vacío): solicitudes cuyo valor del encabezado HTTP `User-Agent` estaba vacío.
- Other (Otros): navegadores que CloudFront ha identificado pero que no se encuentran entre los más populares. Si `Bot/Crawler`, `Empty` o `Unknown` no aparecen entre los nueve primeros valores, también se incluyen en `Other`.
- Unknown (Desconocidos): solicitudes cuyo valor del encabezado HTTP `User-Agent` no se asoció con uno de los navegadores estándar. La mayoría de las solicitudes de esta categoría proceden de aplicaciones personalizadas o secuencias de comandos.

Solicitudes

La cantidad de solicitudes que CloudFront ha recibido de cada tipo de navegador.

RequestsPct

La cantidad de solicitudes que CloudFront ha recibido desde cada tipo de navegador como porcentaje del total de solicitudes que CloudFront ha recibido durante el período determinado.

Informe de tendencias de navegación

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

TimeBucket

La hora o la fecha a la que son aplicables los datos, en tiempo universal coordinado (UTC).

(Browsers)

Las demás columnas del informe reflejan los navegadores o navegadores y sus versiones, en función del valor de `Grouping`. Además de los nombres de los navegadores, otros valores son:

- Bot/Crawler (Bot/Rastreador): sobre todo solicitudes de motores de búsqueda que están indexando su contenido.
- Empty (Vacío): solicitudes cuyo valor del encabezado HTTP `User-Agent` estaba vacío.
- Other (Otros): navegadores que CloudFront ha identificado pero que no se encuentran entre los más populares. Si `Bot/Crawler`, `Empty` o `Unknown` no aparecen entre los nueve primeros valores, también se incluyen en `Other`.
- Unknown (Desconocidos): solicitudes cuyo valor del encabezado HTTP `User-Agent` no se asoció con uno de los navegadores estándar. La mayoría de las solicitudes de esta categoría proceden de aplicaciones personalizadas o secuencias de comandos.

Informe de sistemas operativos

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

Grupo

El sistema operativo o el sistema operativo y la versión desde los que CloudFront ha recibido solicitudes en función del valor de `Grouping`. Además de los nombres de los sistemas operativos, otros valores son:

- Bot/Crawler (Bot/Rastreador): sobre todo solicitudes de motores de búsqueda que están indexando su contenido.
- Empty (Vacío): solicitudes cuyo valor del encabezado HTTP `User-Agent` estaba vacío.

- Other (Otros): sistemas operativos que CloudFront ha identificado pero que no se encuentran entre los más populares. Si `Bot/Crawler`, `Empty` o `Unknown` no aparecen entre los nueve primeros valores, también se incluyen en `Other`.
- Unknown (Desconocidos): solicitudes cuyo valor del encabezado HTTP `User-Agent` no se asoció con uno de los navegadores estándar. La mayoría de las solicitudes de esta categoría proceden de aplicaciones personalizadas o secuencias de comandos.

Solicitudes

La cantidad de solicitudes que CloudFront ha recibido de cada tipo de sistema operativo.

RequestsPct

La cantidad de solicitudes que CloudFront ha recibido desde cada tipo de sistema operativo como porcentaje del total de solicitudes que CloudFront ha recibido durante el período determinado.

Informe de tendencias de sistemas operativos

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

TimeBucket

La hora o la fecha a la que son aplicables los datos, en tiempo universal coordinado (UTC).

(Operating systems)

Las demás columnas del informe reflejan los sistemas operativos o sistemas operativos y sus versiones en función del valor de `Grouping`. Además de los nombres de los sistemas operativos, otros valores son:

- Bot/Crawler (Bot/Rastreador): sobre todo solicitudes de motores de búsqueda que están indexando su contenido.

- Empty (Vacío): solicitudes cuyo valor del encabezado HTTP `User-Agent` estaba vacío.
- Other (Otros): sistemas operativos que CloudFront ha identificado pero que no se encuentran entre los más populares. Si `Bot/Crawler`, `Empty` o `Unknown` no aparecen entre los nueve primeros valores, también se incluyen en `Other`.
- Unknown (Desconocido): solicitudes cuyo sistema operativo no se especifica en el encabezado HTTP `User-Agent`.

Informe de ubicaciones

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

LocationCode

La abreviatura de la ubicación desde la que CloudFront recibe solicitudes. Para obtener más información acerca de los valores posibles, consulte la descripción de Location en Cómo los datos del informe de ubicaciones están relacionados con los datos de los registros estándar (registros de acceso) de CloudFront.

LocationName

El nombre de la ubicación desde la que CloudFront ha recibido solicitudes.

Solicitudes

La cantidad de solicitudes que CloudFront ha recibido desde cada ubicación.

RequestsPct

La cantidad de solicitudes que CloudFront ha recibido desde cada ubicación como porcentaje del total de solicitudes que CloudFront ha recibido de todas las ubicaciones durante el período determinado.

TotalBytes

La cantidad total de bytes que CloudFront ha enviado a los lectores en el estado o país, en la distribución y el periodo especificados.

Informe de tendencias de ubicación

El informe incluye los siguientes valores:

DistributionID

El ID de la distribución del informe solicitado, o `ALL`, si se ha solicitado el informe de todas las distribuciones.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

TimeBucket

La hora o la fecha a la que son aplicables los datos, en tiempo universal coordinado (UTC).

(Locations)

Las demás columnas del informe reflejan las ubicaciones desde las que CloudFront ha recibido solicitudes. Para obtener más información acerca de los valores posibles, consulte la descripción de Location en Cómo los datos del informe de ubicaciones están relacionados con los datos de los registros estándar (registros de acceso) de CloudFront.

Cómo los datos del informe de ubicaciones están relacionados con los datos de los registros estándar (registros de acceso) de CloudFront

La siguiente lista muestra cómo los datos del informe Locations de la consola de CloudFront se corresponden con los valores contenidos en los registros de acceso de CloudFront. Para obtener más información sobre los registros de acceso de CloudFront, consulte Registros de acceso (registros estándar).

Ubicación

El país o estado de EE. UU. en el que se encuentra el espectador. En los registros de acceso, la columna `c-ip` contiene la dirección IP del dispositivo en el que se está ejecutando el espectador. Utilizamos los datos de geolocalización para identificar la ubicación geográfica del dispositivo en función de la dirección IP.

Si consulta el informe Ubicaciones por país, la lista se basa en los códigos de la norma ISO 3166-2 de representación de nombres de países y sus subdivisiones (parte 2: código de subdivisión de país). La lista de países incluye los siguientes valores adicionales:

- Anonymous Proxy (Proxy anónimo): la solicitud se ha originado en un proxy anónimo.
- Satellite Provider (Proveedor satelital); la solicitud se ha originado desde un proveedor satelital que ofrece servicios de Internet a varios países. Los lectores pueden estar en países con un alto riesgo de fraude.
- Europe (Unknown) (Europa) (Desconocido): la solicitud se ha originado desde una IP en un bloque utilizado por varios países europeos. No se puede determinar el país en el que se ha originado la solicitud. CloudFront utiliza Europe (Unknown) (Europa (desconocido)) como valor predeterminado.
- Asia/Pacific (Unknown) (Asia/Pacífico (Desconocido)): la solicitud se ha originado desde una IP en un bloque utilizado por varios países de la región Asia/Pacífico. No se puede determinar el país en el que se ha originado la solicitud. CloudFront utiliza Asia/Pacific (Unknown) (Asia(Pacífico (desconocido)) como valor predeterminado.

Si consulta el informe Locations (Ubicaciones) por estado de Estados Unidos, tenga en cuenta que puede incluir regiones de territorios y zonas militares estadounidenses.

> **Note**
>
> Si CloudFront no puede determinar la ubicación de un usuario, la ubicación aparecerá como desconocida en los informes de lector.

Request Count

La cantidad total de solicitudes del país o estado de Estados Unidos en el que se encuentra el espectador, en la distribución y el periodo especificados. Este valor suele corresponderse estrechamente con la cantidad de solicitudes `GET` desde direcciones IP en ese país o estado en los registros de acceso de CloudFront.

Solicitud %

Una de las siguientes, en función del valor que haya seleccionado para Details (Detalles):

- Countries (Países): las solicitudes de este país como porcentaje del total de solicitudes.
- Estados de Estados Unidos: las solicitudes de este estado como un porcentaje del total de solicitudes de Estados Unidos.

Si las solicitudes han venido de más de 50 países, no podrá calcular el valor Request % (% de solicitudes) en función de los datos de esta tabla, ya que la columna Request Count (Número de solicitudes) no incluye todas las solicitudes del período especificado.

Bytes

La cantidad total de bytes que CloudFront ha enviado a los lectores en el estado o país, en la distribución y el periodo especificados. Para cambiar la visualización de datos en esta columna a KB, MB o GB, elija el enlace del encabezado.

Supervisión de métricas de CloudFront con Amazon CloudWatch

Amazon CloudFront está integrado con Amazon CloudWatch y publica automáticamente las métricas operativas para las distribuciones y funciones periféricas (Lambda@Edge y CloudFront Functions). Puede usar estas métricas para solucionar problemas, realizar un seguimiento y depurar. Muchas de estas métricas se muestran en un conjunto de gráficos en la consola de CloudFront y también se puede acceder a ellos con la API o la CLI de CloudFront. Todas estas métricas están disponibles en la Consola de CloudWatch o mediante la API o la CLI de CloudWatch. Las métricas de CloudFront no se contabilizan en las cuotas de CloudWatch (antes llamadas límites) ni generan ningún coste adicional.

Además de las métricas predeterminadas para distribuciones de CloudFront, puede activar métricas adicionales por un coste adicional. Las métricas adicionales se aplican a distribuciones de CloudFront y deben activarse para cada distribución de forma individual. Para obtener más información sobre el costo, consulte the section called “Estimación del costo de las métricas adicionales de CloudFront”.

También puede establecer alarmas basadas en estas métricas en la consola de CloudFront o en la consola de CloudWatch, la API o la CLI. Por ejemplo, puede configurar una alarma en función de

la métrica de `5xxErrorRate`, que representa el porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta está en el rango de `500` a `599`, inclusive. Cuando la tasa de error alcanza un valor determinado durante una determinada cantidad de tiempo, por ejemplo, el 5 % de las solicitudes durante 5 minutos seguidos, se activa la alarma. Especifique el valor de la alarma y su unidad de tiempo al crear la alarma.

> **Notas**
>
> - Cuando crea una alarma CloudWatch en la consola CloudFront, se crea una para usted en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`). Si crea una alarma desde la consola de CloudWatch, debe usar la misma región. Debido a que CloudFront es un servicio global, las métricas del servicio se envían a Este de EE. UU. (Norte de Virginia).
> - Al crear alarmas, se aplican los precios de CloudWatch estándar.

Temas

- Visualización de métricas de funciones periféricas y de CloudFront
- Creación de alarmas de para métricas de
- Descarga de datos de métricas en formato CSV
- Tipos de métricas para CloudFront

Visualización de métricas de funciones periféricas y de CloudFront

Puede consultar métricas operativas sobre las distribuciones de CloudFront y funciones perimetrales en la consola de CloudFront.

Visualización de métricas de funciones periféricas y de CloudFront en CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, seleccione Supervisión.
3. Para ver gráficos sobre la actividad de una distribución de CloudFront o una función perimetral específica, elija una y, a continuación, elija View distribution metrics (Ver las métricas de distribución) o View metrics (Ver métricas).
4. Puede personalizar los gráficos por medio de uno de los siguientes procedimientos:

a. Para cambiar el intervalo de tiempo de la información que se muestra en los gráficos, seleccione 1h (1 hora), 3h (3 horas), u otro rango o especifique un rango personalizado.

b. Para cambiar la frecuencia con la que CloudFront actualiza la información en el gráfico, elija la flecha hacia abajo junto al icono de actualización y, a continuación, seleccione una frecuencia de actualización. El valor predeterminado de actualización es de 1 minuto, pero puede elegir otras opciones.

5. Para ver los gráficos de CloudFront en la consola de CloudWatch, elija Add to dashboard (Agregar al panel). Debe utilizar la región Este de EE. UU. (Norte de Virginia) para ver los gráficos en la consola de CloudWatch.

Temas

- Métricas de distribución predeterminadas de CloudFront
- Activación de métricas de distribución adicionales de CloudFront
- Métricas de la función de Lambda@Edge predeterminada
- Métricas de CloudFront Functions predeterminadas

Métricas de distribución predeterminadas de CloudFront

Las siguientes métricas predeterminadas se incluyen en todas las distribuciones de CloudFront sin costo adicional:

Solicitudes

La cantidad total de solicitudes de lector recibidas por CloudFront, para todos los métodos HTTP y para las solicitudes HTTP y HTTPS.

Bytes descargados

La cantidad total de bytes descargados por los lectores para las solicitudes `GET` y `HEAD`.

Bytes cargados

La cantidad total de bytes que los lectores cargaron en CloudFront mediante las solicitudes `OPTIONS`, `POST` y `PUT`.

Tasa de errores 4xx

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `4xx`.

Tasa de errores 5xx

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `5xx`.

Tasa de errores total

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `4xx` o `5xx`.

Estas métricas se muestran en gráficos para cada distribución de CloudFront en la página Supervisión de la consola de CloudFront. En cada gráfico, los totales se muestran con una granularidad de un minuto. Además de ver los gráficos, también puede descargar informes de métricas como archivos CSV.

Activación de métricas de distribución adicionales de CloudFront

Además de las métricas predeterminadas, puede activar métricas adicionales por un coste adicional. Para obtener más información sobre el costo, consulte the section called “Estimación del costo de las métricas adicionales de CloudFront”.

Estas métricas adicionales se deben activar para cada distribución de forma individual:

Tasa de aciertos de caché

El porcentaje de todas las solicitudes almacenables en caché para las que CloudFront distribuyó el contenido desde su caché. Las solicitudes HTTP `POST` y `PUT`, así como los errores, no se consideran solicitudes almacenables en caché.

Latencia de origen

El tiempo total transcurrido desde que CloudFront recibe una solicitud hasta que comienza a proporcionar una respuesta a la red (no al lector) en las solicitudes que se distribuyen desde el origen, no desde la caché de CloudFront. Esto también se conoce como latencia de primer byte o time-to-first-byte.

Tasa de error por código de estado

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es un código particular en el rango de `4xx` o `5xx`. Esta métrica está disponible para todos estos códigos de error: `401`, `403`, `404`, `502`, `503` y `504`.

Puede activar métricas adicionales en la consola de CloudFront, con CloudFormation, AWS Command Line Interface (AWS CLI) o la API de CloudFront.

Console

Activación de métricas adicionales

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, seleccione Supervisión.
3. Elija la distribución para la que desea activar métricas adicionales y, a continuación, elija View distribution metrics (Ver métricas de distribución).
4. Elija Manage additional metrics (Administrar métricas adicionales).
5. En la ventana Manage additional metrics (Administrar métricas adicionales), active Enabled (Activado). Después de activar las métricas adicionales, puede cerrar la ventana Manage additional metrics (Administrar métricas adicionales).

   Cuando active las métricas adicionales, se mostrarán en gráficos. En cada gráfico, los totales se muestran con una granularidad de un minuto. Además de ver los gráficos, también puede descargar informes de métricas como archivos CSV.

CloudFormation

Para activar métricas adicionales con CloudFormation, use el tipo de recurso `AWS::CloudFront::MonitoringSubscription`. En el siguiente ejemplo se muestra la sintaxis de plantilla de CloudFormation, en formato YAML, para habilitar métricas adicionales.

```
Type: AWS::CloudFront::MonitoringSubscription
Properties:
  DistributionId: EDFDVBD6EXAMPLE
  MonitoringSubscription:
    RealtimeMetricsSubscriptionConfig:
      RealtimeMetricsSubscriptionStatus: Enabled
```

CLI

Para administrar métricas adicionales con la AWS Command Line Interface (AWS CLI), utilice uno de los siguientes comandos:

Para activar métricas adicionales para una distribución

- Utilice el comando create-monitoring-subscription como se muestra en el ejemplo siguiente. Reemplace *EDFDVBD6EXAMPLE* por el ID de la distribución para la que está habilitando métricas adicionales.

```
aws cloudfront create-monitoring-subscription --
distribution-id EDFDVBD6EXAMPLE --monitoring-subscription
 RealtimeMetricsSubscriptionConfig={RealtimeMetricsSubscriptionStatus=Enabled}
```

Para ver si las métricas adicionales están activadas para una distribución

- Utilice el comando get-monitoring-subscription como se muestra en el ejemplo siguiente. Reemplace *EDFDVBD6EXAMPLE* por el ID de la distribución que está comprobando.

```
aws cloudfront get-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

Para desactivar métricas adicionales para una distribución

- Utilice el comando delete-monitoring-subscription como se muestra en el ejemplo siguiente. Reemplace *EDFDVBD6EXAMPLE* por el ID de la distribución para la que está desactivando métricas adicionales.

```
aws cloudfront delete-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

API

Para administrar métricas adicionales con la API de CloudFront, utilice una de las siguientes operaciones de la API.

- Para activar métricas adicionales para una distribución, utilice CreateMonitoringSubscription.
- Para consultar si las métricas adicionales están activadas para una distribución, utilice GetMonitoringSubscription.

- Para desactivar métricas adicionales para una distribución, utilice DeleteMonitoringSubscription.

Para obtener más información sobre estas operaciones de la API, consulte la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Estimación del costo de las métricas adicionales de CloudFront

Cuando activa métricas adicionales para una distribución, CloudFront envía hasta 8 métricas a CloudWatch en la región Este de EE. UU. (Norte de Virginia). CloudWatch cobra una tarifa fija baja por cada métrica. Esta tarifa se cobra solo una vez al mes por métrica (hasta 8 métricas por distribución). Se trata de una tarifa fija, por lo que el costo sigue siendo el mismo independientemente del número de solicitudes o respuestas que reciba o envíe la distribución de CloudFront. Para conocer la tarifa por métrica, consulte la página de precios de Amazon CloudWatch y la calculadora de precios de CloudWatch. Se aplican cargos adicionales de la API al recuperar las métricas con la API de CloudWatch.

Métricas de la función de Lambda@Edge predeterminada

Puede usar métricas de CloudWatch para monitorear, en tiempo real, los problemas con sus funciones de Lambda@Edge. No hay cargo adicional para estas métricas.

Al adjuntar una función de Lambda@Edge a un comportamiento de la caché en una distribución de CloudFront, Lambda comienza a enviar métricas a CloudWatch automáticamente. Las métricas están disponibles para todas las regiones de Lambda, pero para ver las métricas en la consola de CloudWatch u obtener los datos de métricas de la API de CloudWatch, debe utilizar la región Este de EE. UU. (Norte de Virginia) (`us-east-1`). El nombre del grupo de métricas tiene el formato de: `AWS/CloudFront/`*`distribution-ID`*, donde *`ID-distribución`* es el ID de la distribución de CloudFront a la que está asociada la función de Lambda@Edge. Para obtener más información sobre las métricas de CloudWatch, consulte la Guía del usuario de Amazon CloudWatch.

Las siguientes métricas predeterminadas se muestran en gráficos para cada función de Lambda@Edge en la página Supervisión de la consola de CloudFront:

- `5xx`Intervalo de errores de para Lambda@Edge
- Errores de ejecución de Lambda
- Respuestas no válidas de Lambda
- Limitaciones de Lambda

Los gráficos incluyen la cantidad de invocaciones, errores, limitaciones, etc. En cada gráfico, los totales se muestran con una granularidad de un minuto, agrupados por región de AWS.

Si ve un pico de errores que desea investigar, por ejemplo, puede elegir una función y, a continuación, ver los archivos de registro por región de AWS hasta que determine qué función está causando los problemas y en qué región de AWS. Para obtener más información sobre la resolución de errores Lambda@Edge, consulte:

- the section called “Cómo determinar el tipo de error”
- Cuatro pasos para depurar su entrega de contenido en AWS

Métricas de CloudFront Functions predeterminadas

CloudFront Functions envía métricas operativas a Amazon CloudWatch para que pueda supervisar sus funciones. Ver estas métricas puede ayudarle a solucionar problemas, a realizar un seguimiento y a depurar. CloudFront Functions publica en CloudWatch las siguientes métricas:

- Invocaciones (`FunctionInvocations`): el número de veces que se inició (invocó) la función en un periodo de tiempo determinado.
- Errores de validación (`FunctionValidationErrors`): el número de errores de validación que la función produjo en un periodo de tiempo determinado. Los errores de validación se producen cuando la función se ejecuta correctamente, pero devuelve datos no válidos (un objeto de evento no válido).
- Errores de ejecución (`FunctionExecutionErrors`): el número de errores de ejecución que se produjeron en un periodo de tiempo determinado. Los errores de ejecución se producen cuando la función no se completa correctamente.
- Utilización de cómputo (`FunctionComputeUtilization`): la cantidad de tiempo que la función tardó en ejecutarse como un porcentaje del tiempo máximo permitido. Por ejemplo, un valor de 35 significa que la función se completó en el 35 % del tiempo máximo permitido. Esta métrica es un número entre 0 y 100.

  Si este valor alcanza 100 o está cerca de esa cifra, la función ha utilizado o está cerca de utilizar el tiempo de ejecución permitido y es posible que las solicitudes posteriores se vean limitadas. Si la función se ejecuta al 80 % o más de su utilización, le recomendamos que la revise para reducir el tiempo de ejecución y mejorar la utilización. Por ejemplo, puede que solo desee registrar los errores, simplificar cualquier expresión regular compleja o eliminar el análisis sintáctico de objetos JSON complejos.

- Limitaciones (`FunctionThrottles`): el número de veces que se limitó la función en un periodo de tiempo determinado. Las funciones se pueden limitar por las siguientes razones:
  - La función supera continuamente el tiempo máximo permitido para la ejecución
  - La función produce errores de compilación
  - Hay un número inusualmente elevado de solicitudes por segundo

CloudFront KeyValueStore también envía las siguientes métricas operativas a Amazon CloudWatch:

- Solicitudes de lectura (`KvsReadRequests`): el número de veces que la función leyó correctamente del almacén de clave-valor en un periodo de tiempo determinado.
- Errores de lectura (`KvsReadErrors`): el número de veces que la función no leyó del almacén de clave-valor en un periodo de tiempo determinado.

Todas estas métricas se publican en CloudWatch en la región EE. UU. Este (Norte de Virginia) (`us-east-1`), en el espacio de nombres de CloudFront. También puede verlas en la consola de CloudWatch. En la consola de CloudWatch, puede ver las métricas por función o por función por distribución.

También puede utilizar CloudWatch para establecer alarmas en función de estas métricas. Por ejemplo, puede establecer una alarma en función de la métrica de tiempo de ejecución (`FunctionComputeUtilization`), que representa el porcentaje de tiempo disponible que la función tardó en ejecutarse. Cuando el tiempo de ejecución alcanza un determinado valor durante un tiempo determinado. Por ejemplo, si elige más del 70 % del tiempo disponible durante 15 minutos continuos, la alarma se desencadena. Especifique el valor de las alarmas y su unidad de tiempo al crear la alarma.

> **Note**
>
> CloudFront Functions envía métricas a CloudWatch solo para las funciones de la etapa `LIVE` que se ejecutan en respuesta a solicitudes y respuestas de producción. Al probar una función, CloudFront no envía ninguna métrica a CloudWatch. La salida de prueba contiene información sobre errores, uso de cómputo y registros de funciones (instrucciones `console.log()`), pero esta información no se envía a CloudWatch.

Para obtener información sobre cómo obtener estas métricas con la API de CloudWatch, consulte the section called “Métricas de CloudFront”.

Creación de alarmas de para métricas de

En la consola de CloudFront, puede configurar alarmas para que le envíen notificaciones a través de Amazon Simple Notification Service (Amazon SNS) en función de métricas específicas de CloudFront.

Creación de alarmas para métricas

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, elija Alarmas.
3. Elija Crear alarma.
4. Para Detalles, especifique lo siguiente:
   a. Nombre de alarma: un nombre para la alarma.
   b. Distribución: la distribución de CloudFront para la que está creando la alarma.
5. Para Condición, especifique lo siguiente:
   a. Métrica: la métrica para la que está creando la alarma.
   b. "IF" <condition>: el umbral cuando CloudWatch debe desencadenar una alarma y enviar una notificación al tema de Amazon SNS. Por ejemplo, para recibir una notificación cuando el intervalo de error de `5xx` supera el 1 %, especifique lo siguiente:

      Tasa de errores 5xx > 1
   c. Periodos consecutivos "FOR": el periodo de tiempo durante el que se debe cumplir la condición antes de desencadenar una alarma. Cuando elija un valor, apunte a un equilibrio adecuado entre un valor que no active la alarma por problemas temporales, pero sí por problemas constantes o reales.
   d. (Opcional) Notificar: el tema de Amazon SNS al que se envía la notificación si esta métrica desencadena una alarma.
6. Elija Crear alarma.

Notas

- Al ingresar los valores de la condición, utilice números enteros sin signos de puntuación. Por ejemplo, para especificar mil, escriba **`1000`**.
- Para `4xx`, `5xx` y el total de tasas de errores, el valor a especificar es un porcentaje.
- Para las solicitudes, los bytes descargados y los bytes cargados, el valor a especificar son unidades. Por ejemplo, 1073742000 bytes.

Para obtener más información acerca de la creación de temas de Amazon SNS, consulte Creación de un tema de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Descarga de datos de métricas en formato CSV

Puede descargar los datos de métricas de CloudWatch para una distribución de CloudFront en formato CSV.

Descarga de datos de métricas en formato CSV

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. En el panel de navegación, seleccione Supervisión.
3. Elija la distribución y, a continuación, elija Ver métricas de distribución.
4. Elija Descargar CSV y, a continuación, elija el periodo de tiempo, por ejemplo, Durante el último día (periodo de 1 hora).
5. Una vez descargado el archivo, ábralo para ver la siguiente información.

Temas

- Información acerca del informe
- Datos del informe de las métricas

Información acerca del informe

Las primeras filas del informe incluyen la siguiente información:

Versión

La versión de informes de CloudFront.

Informe

El nombre del informe.

DistributionID

ID de la distribución para la que ejecutó el informe.

StartDateUTC

El principio del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

EndDateUTC

El fin del intervalo de fechas para el que ha solicitado el informe, en tiempo universal coordinado (UTC).

GeneratedTimeUTC

La fecha y hora en ha solicitado el informe, en tiempo universal coordinado (UTC).

Grado de detalle

El periodo de tiempo para cada fila del informe, por ejemplo, `ONE_MINUTE`.

Datos del informe de las métricas

El informe incluye los siguientes valores:

DistributionID

ID de la distribución para la que ejecutó el informe.

FriendlyName

Un nombre de dominio alternativos (CNAME) para la distribución, de haberlo. Si una distribución no tiene otros nombres de dominio, la lista incluye un nombre de dominio de origen para la distribución.

TimeBucket

La hora o la fecha a la que son aplicables los datos, en tiempo universal coordinado (UTC).

Solicitudes

La cantidad total de solicitudes de todos los códigos de estado HTTP (por ejemplo, `200`, `404`, etc.) y todos los métodos (por ejemplo, `GET`, `HEAD`, `POST`, etc.) durante ese periodo de tiempo.

BytesDownloaded

La cantidad de bytes que los espectadores han descargado mediante la distribución especificada durante el periodo de tiempo definido.

BytesUploaded

La cantidad de bytes que los espectadores han cargado mediante la distribución especificada durante el periodo de tiempo definido.

TotalErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `4xx` o `5xx` para la distribución especificada durante el periodo de tiempo definido.

4xxErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `4xx` para la distribución especificada durante el periodo de tiempo definido.

5xxErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `5xx` para la distribución especificada durante el periodo de tiempo definido.

Si ha activado métricas adicionales para su distribución, el informe también incluye los siguientes valores adicionales:

401ErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `401` para la distribución especificada durante el periodo de tiempo definido.

403ErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `403` para la distribución especificada durante el periodo de tiempo definido.

404ErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `404` para la distribución especificada durante el periodo de tiempo definido.

502ErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `502` para la distribución especificada durante el periodo de tiempo definido.

503ErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `503` para la distribución especificada durante el periodo de tiempo definido.

504ErrorRatePct

El porcentaje de solicitudes cuyo código de estado HTTP fue un error de `504` para la distribución especificada durante el periodo de tiempo definido.

OriginLatency

El tiempo total empleado en milisegundos desde que CloudFront recibió una solicitud hasta que comenzó a proporcionar una respuesta a la red (no al lector) en las solicitudes que se distribuyeron desde el origen, no desde la caché de CloudFront. Esto también se conoce como latencia de primer byte o time-to-first-byte.

CacheHitRate

El porcentaje de todas las solicitudes almacenables en caché para las que CloudFront distribuyó el contenido desde su caché. Las solicitudes HTTP `POST` y `PUT`, así como los errores, no se consideran solicitudes almacenables en caché.

Tipos de métricas para CloudFront

Puede usar la API de CloudWatch o AWS Command Line Interface (AWS CLI) para obtener las métricas de CloudFront en programas o aplicaciones que cree. Puede usar los datos sin procesar para crear sus propios paneles personalizados, sus propias herramientas de alarma, etc.

Para obtener más información, consulte get-metric-data en la Referencia de comandos de AWS CLI o la operación de la API GetMetricData en la Referencia de la API de Amazon CloudWatch.

Temas

- Valores para todas las métricas de CloudFront
- Valores para las métricas de distribución de CloudFront
- Valores para las métricas de funciones de CloudFront

> **Note**
>
> Para obtener las métricas de CloudFront con la API de CloudWatch, debe utilizar la región EE. UU. Este (Norte de Virginia) (`us-east-1`). También necesita conocer ciertos valores y tipos para cada métrica.

Valores para todas las métricas de CloudFront

Los siguientes valores se aplican a todas las métricas de CloudFront:

`Namespace`

El valor para `Namespace` siempre es `AWS/CloudFront`.

Dimensiones

Cada métrica de CloudFront tiene las siguientes dimensiones:

`DistributionId`

El ID de la distribución de CloudFront para la que desea obtener métricas.

`FunctionName`

El nombre de la función (en CloudFront Functions) para la que desea obtener métricas.

Esta dimensión solo se aplica a las funciones.

`Region`

El valor de `Region` siempre es `Global`, porque CloudFront es un servicio global.

Valores para las métricas de distribución de CloudFront

Utilice la información de la siguiente lista para obtener detalles sobre métricas de distribución específicas de CloudFront con la API de CloudWatch. Algunas de estas métricas solo están disponibles si se han activado métricas adicionales para la distribución.

> **Note**
>
> Solo se aplica una estadística, `Average` o `Sum`, para cada métrica. La siguiente lista especifica qué estadística se aplica a esa métrica.

Tasa de errores 4xx

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `4xx`.

- Nombre de métrica: `4xxErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Tasa de errores 401

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `401`. Para obtener esta métrica, primero debe activar métricas adicionales.

- Nombre de métrica: `401ErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Tasa de errores 403

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `403`. Para obtener esta métrica, primero debe activar métricas adicionales.

- Nombre de métrica: `403ErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Tasa de errores 404

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `404`. Para obtener esta métrica, primero debe activar métricas adicionales.

- Nombre de métrica: `404ErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Tasa de errores 5xx

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `5xx`.

- Nombre de métrica: `5xxErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Tasa de errores 502

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `502`. Para obtener esta métrica, primero debe activar métricas adicionales.

- Nombre de métrica: `502ErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Tasa de errores 503

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `503`. Para obtener esta métrica, primero debe activar métricas adicionales.

- Nombre de métrica: `503ErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Tasa de errores 504

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `504`. Para obtener esta métrica, primero debe activar métricas adicionales.

- Nombre de métrica: `504ErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Bytes descargados

La cantidad total de bytes descargados por los lectores para las solicitudes `GET` y `HEAD`.

- Nombre de métrica: `BytesDownloaded`
- Estadística válida: `Sum`

- Unidad: `None`

Bytes cargados

La cantidad total de bytes que los lectores cargaron en CloudFront mediante las solicitudes `OPTIONS`, `POST` y `PUT`.

- Nombre de métrica: `BytesUploaded`
- Estadística válida: `Sum`
- Unidad: `None`

Tasa de aciertos de caché

El porcentaje de todas las solicitudes almacenables en caché para las que CloudFront distribuyó el contenido desde su caché. Las solicitudes HTTP `POST` y `PUT`, así como los errores, no se consideran solicitudes almacenables en caché. Para obtener esta métrica, primero debe activar métricas adicionales.

- Nombre de métrica: `CacheHitRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Latencia de origen

El tiempo total empleado en milisegundos desde que CloudFront recibe una solicitud hasta que comienza a proporcionar una respuesta a la red (no al lector) en las solicitudes que se distribuyeron desde el origen, no desde la caché de CloudFront. Esto también se conoce como latencia de primer byte o time-to-first-byte. Para obtener esta métrica, primero debe activar métricas adicionales.

- Nombre de métrica: `OriginLatency`
- Estadística válida: `Percentile`
- Unidad: `Milliseconds`

> **Note**
>
> Para obtener la estadística de `Percentile` desde la API de CloudWatch, use el parámetro `ExtendedStatistics`, no `Statistics`. Para obtener más información, consulte GetMetricStatistics en la Referencia de la API de Amazon CloudWatch o la documentación de referencia de los SDK de AWS

Solicitudes

La cantidad total de solicitudes de lector recibidas por CloudFront, para todos los métodos HTTP y para las solicitudes HTTP y HTTPS.

- Nombre de métrica: `Requests`
- Estadística válida: `Sum`
- Unidad: `None`

Tasa de errores total

El porcentaje de todas las solicitudes de espectador para las cuales el código de estado HTTP de la respuesta es `4xx` o `5xx`.

- Nombre de métrica: `TotalErrorRate`
- Estadística válida: `Average`
- Unidad: `Percent`

Valores para las métricas de funciones de CloudFront

Utilice la información de la siguiente lista para obtener detalles sobre métricas específicas de CloudFront con la API de CloudWatch.

> **Note**
>
> Solo se aplica una estadística, `Average` o `Sum`, para cada métrica. La siguiente lista especifica qué estadística se aplica a esa métrica.

Invocaciones

El número de veces que se inició (invocó) la función en un periodo de tiempo determinado.

- Nombre de métrica: `FunctionInvocations`
- Estadística válida: `Sum`
- Unidad: `None`

Errores de validación

El número de errores de validación que produjo la función en un periodo de tiempo determinado. Los errores de validación se producen cuando la función se ejecuta correctamente, pero devuelve datos no válidos (un objeto de evento no válido).

- Nombre de métrica: `FunctionValidationErrors`
- Estadística válida: `Sum`
- Unidad: `None`

Errores de ejecución

El número de errores de ejecución que se produjeron en un periodo de tiempo determinado. Los errores de ejecución se producen cuando la función no se completa correctamente.

- Nombre de métrica: `FunctionExecutionErrors`
- Estadística válida: `Sum`
- Unidad: `None`

Utilización de cómputo

La cantidad de tiempo (0-100) que la función tardó en ejecutarse como porcentaje del tiempo máximo permitido. Por ejemplo, un valor de 35 significa que la función se completó en el 35 % del tiempo máximo permitido.

- Nombre de métrica: `FunctionComputeUtilization`
- Estadística válida: `Average`
- Unidad: `Percent`

Limitaciones

El número de veces que se limitó la función en un periodo de tiempo determinado.

- Nombre de métrica: `FunctionThrottles`
- Estadística válida: `Sum`
- Unidad: `None`

Registro de funciones de CloudFront y perimetrales

Amazon CloudFront proporciona diferentes tipos de registro. Puede registrar las solicitudes de espectador que llegan a las distribuciones de CloudFront o puede registrar la actividad del servicio de CloudFront (actividad de la API) en la cuenta de AWS. También puede obtener registros de CloudFront Functions y funciones de Lambda@Edge.

Solicitudes de registro

CloudFront proporciona las siguientes formas de registrar las solicitudes que llegan a las distribuciones.

Registros de acceso (registros estándar)

Los registros de acceso de CloudFront proporcionan registros detallados sobre cada solicitud que se realiza en una distribución. Puede usar los registros para situaciones como las auditorías de seguridad y acceso.

Los registros de acceso de CloudFront se entregan al destino de entrega especificado.

Utilice los registros de acceso cuando necesite:

- Análisis e informes históricos
- Requisitos de conformidad y auditorías de seguridad
- Retención de registros rentable a largo plazo

Para obtener más información, consulte Registros de acceso (registros estándar).

Registros de acceso en tiempo real

Los registros de acceso en tiempo real de CloudFront se entregan en cuestión de segundos después de recibir las solicitudes y proporcionar información sobre las solicitudes realizadas a una distribución en tiempo real. Puede elegir la frecuencia de muestreo de los registros de acceso en tiempo real, es decir, el porcentaje de solicitudes de las que desea recibir entradas de registros de acceso en tiempo real. También puede elegir los campos específicos de los que desea recibir registros de log. Los registros de acceso en tiempo real son ideales para supervisar en directo el rendimiento de la entrega de contenido.

Los registros de acceso en tiempo real de CloudFront se envían al flujo de datos de su elección en Amazon Kinesis Data Streams. CloudFront aplica cargos por los registros de acceso en tiempo real, que se suman a los cargos que se aplican por el uso de Kinesis Data Streams.

Utilice los registros de acceso en tiempo real cuando necesite:

- Supervisión y alertas en tiempo real
- Paneles en directo e información operativa

Para obtener más información, consulte Uso de registros de acceso en tiempo real.

Registros de conexiones

Los registros de conexión proporcionan información detallada sobre la conexión entre el servidor y el cliente en el caso de las distribuciones compatibles con mTLS. Los registros de conexión proporcionan visibilidad de la información de los certificados del cliente, los motivos de los errores de autenticación de mTLS y si se ha permitido o rechazado una conexión.

Al igual que los registros de acceso (registros estándar), los registros de conexión se entregan al destino de entrega especificado.

> **Note**
>
> Para habilitar los registros de conexión, primero debe habilitar mTLS para la distribución.

Utilice los registros de conexión cuando necesite:

- Motivos de las conexiones exitosas o erróneas durante el establecimiento de comunicación de TLS
- Visibilidad de la información de certificados de cliente

Para obtener más información, consulte Observabilidad mediante registros de conexión.

Registro de las funciones perimetrales

Puede utilizar registros de Amazon CloudWatch para obtener registros de las funciones perimetrales de Lambda@Edge y de CloudFront Functions. Puede acceder a los registros mediante la consola de CloudWatch o la API de CloudWatch Logs. Para obtener más información, consulte the section called “Registros de funciones perimetrales”.

Registro de la actividad del servicio

Puede utilizar AWS CloudTrail para registrar la actividad de servicio de CloudFront (actividad de la API) en la cuenta de AWS. CloudTrail proporciona un registro de las medidas de la API adoptadas por un usuario, un rol o servicio de AWS en CloudFront. Mediante la información recopilada por CloudTrail, puede determinar la solicitud de la API que se realizó a CloudFront, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información, consulte Registro de llamadas a la API de Amazon CloudFront con AWS CloudTrail.

Para obtener más información acerca del registro, consulte los siguientes temas:

Temas

- Registros de acceso (registros estándar)
- Uso de registros de acceso en tiempo real
- Registros de funciones perimetrales
- Registro de llamadas a la API de Amazon CloudFront con AWS CloudTrail

Registros de acceso (registros estándar)

Puede configurar CloudFront para crear archivos de registro que contengan información detallada sobre cada solicitud de usuario (espectador) que CloudFront recibe. Estos se denominan registros de acceso, también conocidos como registros estándar.

Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, el tiempo de procesamiento, las rutas de solicitud y las respuestas del servidor. Puede utilizar estos registros de acceso para analizar los tiempos de respuesta y solucionar problemas.

En el siguiente diagrama se muestra cómo CloudFront registra información sobre solicitudes para los objetos. En este ejemplo, las distribuciones están configuradas para enviar registros de acceso a un bucket de Amazon S3.

1. En este ejemplo se muestran dos sitios web, A y B, y sus distribuciones de CloudFront correspondientes. Los usuarios solicitan sus objetos a través de URL asociadas a las distribuciones.
2. CloudFront dirige cada solicitud a la ubicación de borde adecuada.
3. CloudFront escribe los datos de cada solicitud en un archivo de registro específico en esa distribución. En este ejemplo, la información acerca de las solicitudes relacionadas con la Distribución A se escriben en un archivo de registro para la Distribución A. La información acerca de las solicitudes relacionadas con la Distribución B se escriben en un archivo de registro para la Distribución B.
4. CloudFront periódicamente guarda el archivo de registro de la distribución en el bucket de Amazon S3 especificado al habilitar el registro. A continuación, CloudFront comienza a guardar información acerca de las solicitudes posteriores en un nuevo archivo de registro para la distribución.

   Si los espectadores no obtienen acceso a su contenido durante una hora determinada, no se reciben archivos de registro de esa hora.

> **Note**
>
> Recomendamos utilizar los registros de acceso para comprender la naturaleza de las solicitudes hechas a su contenido y no como una relación exhaustiva de todas las solicitudes. CloudFront envía registros de acceso en la medida en que sea posible. La entrada de registro de una solicitud determinada puede entregarse mucho después de la solicitud se haya procesado realmente y, en casos contados, es probable que una entrada de registro no se entregue en absoluto. Cuando se omite una entrada de registro de los registros de acceso, la cantidad de entradas de los registros de acceso no coincide con el uso que aparece en los informes de facturación y de uso de AWS.

CloudFront admite dos versiones del registro estándar. El registro estándar (heredado) permite enviar los registros de acceso únicamente a Amazon S3. El registro estándar (v2) admite destinos de entrega adicionales. Puede configurar ambas opciones de registro o cualquiera de ellas en su distribución. Para obtener más información, consulte los temas siguientes:

Temas

- Configuración del registro estándar (v2)
- Configuración del registro estándar (heredado)
- Referencia de registro estándar

> **Tip**
>
> CloudFront también ofrece registros de acceso en tiempo real, que proporcionan información sobre las solicitudes realizadas a una distribución en tiempo real (los registros se envían en cuestión de segundos después de recibir las solicitudes). Puede usar los registros de acceso en tiempo real para supervisar, analizar y tomar medidas en función del rendimiento de entrega de contenido. Para obtener más información, consulte Uso de registros de acceso en tiempo real.

Configuración del registro estándar (v2)

Puede habilitar los registros de acceso (registros estándar) al crear o actualizar una distribución. El registro estándar (v2) incluye las siguientes características:

- Enviar registros de acceso a Registros de Amazon CloudWatch, Amazon Data Firehose y Amazon Simple Storage Service (Amazon S3).
- Seleccionar los campos de registro que desee. También puede seleccionar un subconjunto de campos de registro de acceso en tiempo real.
- Seleccionar formatos de archivo de registro de salida adicionales.

Si utiliza Amazon S3, dispone de las siguientes características opcionales:

- Enviar registros en Regiones de AWS de inscripción
- Organizar sus registros con particiones
- Activar los nombres de archivo compatibles con Hive

Para obtener más información, consulte Envío de registros a Amazon S3.

Para comenzar a utilizar el registro estándar, complete los siguientes pasos:

1. Configure los permisos necesarios para el Servicio de AWS especificado que recibirá sus registros.
2. Configure el registro estándar desde la consola de CloudFront o la API de CloudWatch.
3. Consulte sus registros de acceso.

> **Note**
>
> - Si activa el registro estándar (v2), esto no afectará ni cambiará el registro estándar (heredado). Puede seguir utilizando el registro estándar (heredado) para su distribución, además del registro estándar (v2). Para obtener más información, consulte Configuración del registro estándar (heredado).
> - Si ya ha activado el registro estándar (heredado) y quiere activar el registro estándar (v2) en Amazon S3, le recomendamos que especifique un bucket de Amazon S3 diferente o utilice una ruta distinta en el mismo bucket (por ejemplo, utilice un prefijo de registro o una partición). Esto le ayuda a realizar un seguimiento de los archivos de registro que están asociados a cada distribución y evita que los archivos de registro se sobrescriban entre sí.

Permisos

CloudFront utiliza los registros distribuidos de CloudWatch para entregar los registros de acceso. Para ello, necesita los permisos al Servicio de AWS especificado para poder activar la entrega de registros.

Para ver los permisos necesarios para cada destino de registro, elija uno de los siguientes temas en la Guía del usuario de Registros de Amazon CloudWatch.

- Registros de CloudWatch
- Firehose
- Amazon S3

Una vez que haya configurado los permisos para su destino de registro, puede activar el registro estándar para su distribución.

> **Note**
>
> CloudFront admite el envío de registros de acceso a diferentes Cuentas de AWS (entre cuentas). Para activar la entrega entre cuentas, ambas cuentas (la suya y la cuenta receptora) deben tener los permisos necesarios. Para obtener más información, consulte la sección Activación del registro estándar para la entrega entre cuentas o el ejemplo de entrega entre cuentas de la Guía del usuario de Registros de Amazon CloudWatch.

Activación del registro estándar

Para activar el registro estándar, puede utilizar la consola de CloudFront o la API de CloudWatch.

Contenido

- Activación del registro estándar (consola de CloudFront)
- Activación del registro estándar (API de CloudWatch)

Activación del registro estándar (consola de CloudFront)

Para activar el registro estándar en una distribución de CloudFront (consola)

1. Utilice la consola de CloudFront para actualizar una distribución existente.

2. Elija la pestaña Logging (Registro).
3. Elija Agregar y, a continuación, seleccione el servicio para recibir los registros:
   - Registros de CloudWatch
   - Firehose
   - Amazon S3
4. En Destino, seleccione el recurso para su servicio. Si aún no ha creado el recurso, puede elegir Crear o consultar la siguiente documentación.
   - Para Registros de CloudWatch, introduzca el nombre del grupo de registro.
   - Para Firehose, introduzca el flujo de entrega de Firehose.
   - Para Amazon S3, introduzca el nombre del bucket.

   > **Tip**
   >
   > Para especificar un prefijo, introdúzcalo después del nombre del bucket, por ejemplo, `amzn-s3-demo-bucket.s3.amazonaws.com/MyLogPrefix`. Si no especifica ningún prefijo, CloudFront le agregará uno automáticamente. Para obtener más información, consulte Envío de registros a Amazon S3.

5. En configuración adicional: opcional, puede especificar las siguientes opciones:
   a. En Selección de campos, seleccione los nombres de los campos de registro que desea entregar en su destino. Puede seleccionar campos de registro de acceso y un subconjunto de campos de registro de acceso en tiempo real.
   b. (Solo Amazon S3) En Partición, especifique la ruta para particionar los datos del archivo de registro.
   c. (Solo Amazon S3) En Formato de archivo compatible con Hive, puede seleccionar la casilla de verificación para utilizar rutas de S3 compatibles con Hive. Esto ayuda a simplificar la carga de nuevos datos en las herramientas compatibles con Hive.
   d. En Formato de salida, especifique el formato que prefiera.

> **Note**
>
> Si elige Parquet, esta opción conlleva cargos de CloudWatch por convertir sus registros de acceso a Apache Parquet. Para obtener más información, consulte la sección Registros distribuidos de Precios de CloudWatch.

e. En Delimitador de campo, especifique cómo separar los campos de registro.

6. Complete los pasos para actualizar o crear su distribución.
7. Para agregar otro destino, repita los pasos 3-6.
8. En la página Registros, compruebe que el estado de los registros estándar sea Activado junto a la distribución.
9. (Opcional) Para habilitar el registro de cookies, elija Administrar, Configuración y active Registro de cookies; a continuación, elija Guardar cambios.

> **Tip**
>
> Registro de cookies es una configuración global que se aplica a todos los registros estándar de su distribución. No puede anular esta configuración para distintos destinos de entrega.

Para obtener más información sobre la entrega de registros estándar y los campos de registro, consulte Referencia de registro estándar.

Activación del registro estándar (API de CloudWatch)

También puede utilizar la API de CloudWatch para habilitar el registro estándar en sus distribuciones.

> **Notas**
>
> - Al llamar a la API de CloudWatch para activar el registro estándar, debe especificar la región Este de EE. UU. (Norte de Virginia) (`us-east-1`), aunque desee activar la entrega entre regiones a otro destino. Por ejemplo, si quiere enviar sus registros de acceso a un bucket de S3 en la región de Europa (Irlanda) (`eu-west-1`), utilice la API de CloudWatch en la región `us-east-1`.

- Existe una opción adicional para incluir cookies en el registro estándar. En la API de CloudFront, este es el parámetro `IncludeCookies`. Si configura el registro de acceso mediante la API de CloudWatch y especifica que desea incluir cookies, debe usar la consola de CloudFront o la API de CloudFront para actualizar la distribución de forma que incluya cookies. De lo contrario, CloudFront no podrá enviar cookies a su destino de registro. Para obtener más información, consulte Registro de cookies.

Para activar el registro estándar en una distribución (API de CloudWatch)

1. Después de crear una distribución, obtenga el nombre de recurso de Amazon (ARN).

   Puede encontrar el ARN en la página de Distribución de la consola de CloudFront o puede utilizar la operación de la API GetDistribution. El ARN de las distribuciones usa el siguiente formato: `arn:aws:cloudfront::123456789012:distribution/d111111abcdef8`

2. A continuación, utilice la operación de la API de CloudWatch PutDeliverySource para crear un origen de entrega para la distribución.

   a. Introduzca un nombre para el origen de entrega.

   b. Transmita el `resourceArn` de la distribución.

   c. En `logType`, especifique `ACCESS_LOGS` como el tipo de registros que se recopilan.

   d. Example Ejemplo de comando put-delivery-source de la AWS CLI

      A continuación, se muestra un ejemplo de cómo configurar un origen de entrega en una distribución.

```
aws logs put-delivery-source --name S3-delivery --resource-arn
 arn:aws:cloudfront::123456789012:distribution/d111111abcdef8 --log-type
 ACCESS_LOGS
```

      Output

```
{
 "deliverySource": {
 "name": "S3-delivery",
 "arn": "arn:aws:logs:us-east-1:123456789012:delivery-source:S3-delivery",
 "resourceArns": [
 "arn:aws:cloudfront::123456789012:distribution/d111111abcdef8"
```

```
 ],
 "service": "cloudfront",
 "logType": "ACCESS_LOGS"
 }
}
```

3. Utilice la operación de la API PutDeliveryDestination para configurar dónde almacenar los registros.

   a. En `destinationResourceArn`, especifique el ARN del destino. Puede ser un grupo de registros de CloudWatch, una secuencia de entrega de Firehose o un bucket de Amazon S3.

   b. En `outputFormat`, especifique el formato de salida de sus registros.

   c. Example Ejemplo de comando put-delivery-destination de la AWS CLI

      A continuación, se muestra un ejemplo de cómo configurar un destino de entrega en un bucket de Amazon S3.

```
aws logs put-delivery-destination --name S3-destination --delivery-destination-
configuration destinationResourceArn=arn:aws:s3:::amzn-s3-demo-bucket
```

      Output

```
{
    "name": "S3-destination",
    "arn": "arn:aws:logs:us-east-1:123456789012:delivery-destination:S3-
destination",
    "deliveryDestinationType": "S3",
    "deliveryDestinationConfiguration": {
        "destinationResourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
}
```

> **Note**
>
> Si entrega registros entre cuentas, debe usar la operación de la API PutDeliveryDestinationPolicy para asignar una política de AWS Identity and Access

Management (IAM) a la cuenta de destino. La política de IAM permite la entrega de una cuenta a otra.

4. Use la operación de la API CreateDelivery para vincular el origen de entrega con el destino creado en los pasos anteriores. Esta operación de la API asocia el origen de la entrega con el destino final.

   a. En `deliverySourceName`, especifique un nombre del origen.

   b. En `deliveryDestinationArn`, especifique el ARN del destino de entrega.

   c. En `fieldDelimiter`, especifique la cadena para separar cada campo de registro.

   d. En `recordFields`, especifique los campos de registro que desee.

   e. Si usa S3, especifique si desea usar `enableHiveCompatiblePath` y`suffixPath`.

   Example Ejemplo de comando create-delivery de la AWS CLI

   A continuación, se muestra un ejemplo de creación de una entrega.

```
aws logs create-delivery --delivery-source-name cf-delivery --delivery-destination-
arn arn:aws:logs:us-east-1:123456789012:delivery-destination:S3-destination
```

   Output

```
{
    "id": "abcNegnBoTR123",
    "arn": "arn:aws:logs:us-east-1:123456789012:delivery:abcNegnBoTR123",
    "deliverySourceName": "cf-delivery",
    "deliveryDestinationArn": "arn:aws:logs:us-east-1:123456789012:delivery-
destination:S3-destination",
    "deliveryDestinationType": "S3",
    "recordFields": [
        "date",
        "time",
        "x-edge-location",
        "sc-bytes",
        "c-ip",
        "cs-method",
        "cs(Host)",
        "cs-uri-stem",
        "sc-status",
```

```
        "cs(Referer)",
        "cs(User-Agent)",
        "cs-uri-query",
        "cs(Cookie)",
        "x-edge-result-type",
        "x-edge-request-id",
        "x-host-header",
        "cs-protocol",
        "cs-bytes",
        "time-taken",
        "x-forwarded-for",
        "ssl-protocol",
        "ssl-cipher",
        "x-edge-response-result-type",
        "cs-protocol-version",
        "fle-status",
        "fle-encrypted-fields",
        "c-port",
        "time-to-first-byte",
        "x-edge-detailed-result-type",
        "sc-content-type",
        "sc-content-len",
        "sc-range-start",
        "sc-range-end",
        "c-country",
        "cache-behavior-path-pattern"
    ],
     "fieldDelimiter": ""
}
```

5. Desde la consola de CloudFront, en la página Registros, compruebe que el estado de los registros estándar sea Activado junto a la distribución.

   Para obtener más información sobre la entrega de registros estándar y los campos de registro, consulte Referencia de registro estándar.

> **Note**
>
> Para habilitar el registro estándar (v2) para CloudFront con AWS CloudFormation, puede usar las siguientes propiedades de Registros de CloudWatch:
>
> - Delivery

- DeliveryDestination
- DeliverySource

`ResourceArn` es la distribución de CloudFront y `LogType` debe ser `ACCESS_LOGS` como el tipo de registro admitido.

Activación del registro estándar para la entrega entre cuentas

Si activa el registro estándar en la Cuenta de AWS y desea enviar los registros de acceso a otra cuenta, asegúrese de configurar correctamente la cuenta de origen y la cuenta de destino. La cuenta de origen con la distribución de CloudFront envía sus registros de acceso a la cuenta de destino.

En este procedimiento de ejemplo, la cuenta de origen (*111111111111*) envía sus registros de acceso a un bucket de Amazon S3 de la cuenta de destino (*222222222222*). Para enviar registros de acceso a un bucket de Amazon S3 en la cuenta de destino, utilice la AWS CLI.

Configuración de la cuenta de destino

Para la cuenta de destino, realice el procedimiento siguiente.

Para configurar la cuenta de destino

1. Para crear el destino de entrega del registro, puede introducir el comando siguiente de la AWS CLI. En este ejemplo, se utiliza la cadena *MyLogPrefix* para crear un prefijo para los registros de acceso.

```
aws logs put-delivery-destination --name cloudfront-delivery-destination --
delivery-destination-configuration "destinationResourceArn=arn:aws:s3:::amzn-s3-
demo-bucket-cloudfront-logs/MyLogPrefix"
```

Output

```
{
    "deliveryDestination": {
        "name": "cloudfront-delivery-destination",
        "arn": "arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination",
        "deliveryDestinationType": "S3",
```

```
        "deliveryDestinationConfiguration": {"destinationResourceArn":
 "arn:aws:s3:::amzn-s3-demo-bucket-cloudfront-logs/MyLogPrefix"}
    }
}
```

> **Note**
>
> Si especifica un bucket de S3 sin prefijo, CloudFront anexará automáticamente el `AWSLogs/<account-ID>/CloudFront` como prefijo que aparece en la `suffixPath` del destino de entrega de S3. Para obtener más información, consulte S3DeliveryConfiguration.

2. Agregue la política de recursos del destino de entrega del registro para permitir que la cuenta de origen cree una entrega del registro.

   En la siguiente política, sustituya *111111111111* por el ID de cuenta de origen y especifique el ARN de destino de la entrega a partir de la salida del paso 1.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateDelivery",
            "Effect": "Allow",
            "Principal": {"AWS": "111111111111"},
            "Action": ["logs:CreateDelivery"],
            "Resource": "arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination"
        }
    ]
}
```

3. Guarde el archivo como, por ejemplo, `deliverypolicy.json`.
4. Para asociar la política anterior al destino de la entrega, introduzca el siguiente comando de la AWS CLI.

```
aws logs put-delivery-destination-policy --delivery-destination-name cloudfront-
delivery-destination --delivery-destination-policy file://deliverypolicy.json
```

5. Agregue la siguiente instrucción a la política de bucket de Amazon S3 de destino y sustituya el ARN del recurso y el ID de la cuenta de origen. Esta política permite que la entidad principal de servicio de `delivery.logs.amazonaws.com` realice la acción `s3:PutObject`.

```
{
    "Sid": "AWSLogsDeliveryWrite",
    "Effect": "Allow",
    "Principal": {"Service": "delivery.logs.amazonaws.com"},
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-cloudfront-logs/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceAccount": "111111111111"
        },
        "ArnLike": {"aws:SourceArn": "arn:aws:logs:us-east-1:111111111111:delivery-
source:*"}
    }
}
```

6. Si utiliza AWS KMS para su bucket, agregue la siguiente instrucción a la política de claves de KMS para conceder permisos a la entidad principal del servicio de `delivery.logs.amazonaws.com`.

```
{
    "Sid": "Allow Logs Delivery to use the key",
    "Effect": "Allow",
    "Principal": {"Service": "delivery.logs.amazonaws.com"},
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {"aws:SourceAccount": "111111111111"},
```

```
        "ArnLike": {"aws:SourceArn": "arn:aws:logs:us-east-1:111111111111:delivery-
source:*"}
    }
}
```

Configuración de la cuenta de origen

Tras configurar la cuenta de destino, siga este procedimiento para crear el origen de la entrega y activar el registro de la distribución en la cuenta de origen.

Para configurar la cuenta de origen

1. Cree un origen de entrega para el registro estándar de CloudFront de modo que pueda enviar archivos de registro a Registros de CloudWatch.

   Puede introducir el siguiente comando de la AWS CLI sustituyendo el nombre y el ARN de la distribución.

   ```
   aws logs put-delivery-source --name s3-cf-delivery --resource-arn
    arn:aws:cloudfront::111111111111:distribution/E1TR1RHV123ABC --log-type
    ACCESS_LOGS
   ```

   Output

   ```
   {
       "deliverySource": {
           "name": "s3-cf-delivery",
           "arn": "arn:aws:logs:us-east-1:111111111111:delivery-source:s3-cf-
   delivery",
           "resourceArns":
    ["arn:aws:cloudfront::111111111111:distribution/E1TR1RHV123ABC"],
           "service": "cloudfront",
           "logType": "ACCESS_LOGS"
       }
   }
   ```

2. Cree una entrega para mapear el origen de entrega del registro de la cuenta de origen y el destino de entrega del registro de la cuenta de destino.

   En el siguiente comando de la AWS CLI, especifique el ARN de destino de la entrega a partir de la salida del Paso 1: Configuración de la cuenta de destino.

```
aws logs create-delivery --delivery-source-name s3-cf-delivery --
delivery-destination-arn arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination
```

Output

```
{
    "delivery": {
        "id": "OPmOpLahVzhx1234",
        "arn": "arn:aws:logs:us-east-1:111111111111:delivery:OPmOpLahVzhx1234",
        "deliverySourceName": "s3-cf-delivery",
        "deliveryDestinationArn": "arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination",
        "deliveryDestinationType": "S3",
        "recordFields": [
            "date",
            "time",
            "x-edge-location",
            "sc-bytes",
            "c-ip",
            "cs-method",
            "cs(Host)",
            "cs-uri-stem",
            "sc-status",
            "cs(Referer)",
            "cs(User-Agent)",
            "cs-uri-query",
            "cs(Cookie)",
            "x-edge-result-type",
            "x-edge-request-id",
            "x-host-header",
            "cs-protocol",
            "cs-bytes",
            "time-taken",
            "x-forwarded-for",
            "ssl-protocol",
            "ssl-cipher",
            "x-edge-response-result-type",
            "cs-protocol-version",
            "fle-status",
            "fle-encrypted-fields",
            "c-port",
```

```
            "time-to-first-byte",
            "x-edge-detailed-result-type",
            "sc-content-type",
            "sc-content-len",
            "sc-range-start",
            "sc-range-end",
            "c-country",
            "cache-behavior-path-pattern"
        ],
        "fieldDelimiter": "\t"
    }
}
```

3. Compruebe que la entrega entre cuentas se ha realizado correctamente.

   a. Desde la cuenta de *origen*, inicie sesión en la consola de CloudFront y elija su distribución. En la pestaña Registro, en Tipo, verá una entrada creada para la entrega de registros entre cuentas de S3.

   b. Desde la cuenta de *destino*, inicie sesión en la consola de Amazon S3 y elija su bucket de Amazon S3. Verá el prefijo *MyLogPrefix* en el nombre del bucket y todos los registros de acceso que se entreguen en esa carpeta.

Formato de archivo de salida

Según el destino de entrega que elija, puede especificar uno de los siguientes formatos para los archivos de registro:

- JSON
- Sin formato
- w3c
- Raw
- Parquet (solo Amazon S3)

> **Note**
>
> Solo puede establecer el formato de salida cuando crea por primera vez el destino de entrega. Esto no se puede actualizar más tarde. Para cambiar el formato de salida, elimine la entrega y cree otra.

Para obtener más información, consulte PutDeliveryDestination en la Referencia de la API de Registros de Amazon CloudWatch.

Edición de configuración de registro estándar

Puede activar o desactivar el registro y actualizar otra configuración de registro mediante la consola de CloudFront o la API de CloudWatch. Los cambios de configuración de registro surten efecto en un plazo de 12 horas.

Para obtener más información, consulte los temas siguientes:

- Para actualizar una distribución mediante la consola de CloudFront, consulte Actualizar una distribución.
- Para actualizar una distribución mediante la API de CloudFront, consulte UpdateDistribution en la Referencia de la API de Amazon CloudFront.
- Para obtener más información sobre las operaciones de la API de Registros de CloudWatch, consulte la Referencia de la API de Registros de Amazon CloudWatch.

Campos de registro de acceso

Puede seleccionar los mismos campos de registro que admite el registro estándar (heredado). Para obtener más información, consulte Campos de archivos de registro.

Además, puede seleccionar los siguientes campos de registro de acceso en tiempo real.

1. **`timestamp(ms)`**: marca de tiempo en milisegundos.
2. **`origin-fbl`**: cantidad de segundos de latencia del primer byte entre CloudFront y el origen.
3. **`origin-lbl`**: cantidad de segundos de latencia del último byte entre CloudFront y el origen.
4. **`asn`**: número de sistema autónomo (ASN) del espectador.
5. **`c-country`**: código de país que representa la ubicación geográfica del espectador, según lo determinado por la dirección IP del espectador. Para obtener una lista de códigos de países, consulte ISO 3166-1 alpha-2.
6. **`cache-behavior-path-pattern`**: patrón de ruta que identifica el comportamiento de caché que coincidió con la solicitud del espectador.

Envíe los registros a CloudWatch Logs

Para enviar registros a Registros de CloudWatch, debe crear un grupo de registro de Registros de CloudWatch o usar uno existente. Para obtener más información sobre cómo configurar un grupo de registro de Registros de CloudWatch, consulte Working with Log Groups and Log Streams.

Después de crear el grupo de registro, debe contar con los permisos necesarios para permitir el registro estándar. Para obtener más información sobre los permisos necesarios, consulte Logs sent to CloudWatch Logs en la Guía del usuario de Registros de Amazon CloudWatch.

> **Notas**
>
> - Cuando especifique el nombre del grupo de registro de Registros de CloudWatch, utilice únicamente el patrón de expresiones regulares `[\w-]`. Para obtener más información, consulte la operación de la API PutDeliveryDestination en la Referencia de la API de Registros de Amazon CloudWatch.
> - Compruebe que la política de recursos del grupo de registro no supere el límite de tamaño. Consulte la sección Log group resource policy size limit considerations del tema Registros de CloudWatch.

Ejemplo de registro de acceso enviado a Registros de CloudWatch

```
{
"date": "2024-11-14",
"time": "21:34:06",
"x-edge-location": "SOF50-P2",
"asn": "16509",
"timestamp(ms)": "1731620046814",
"origin-fbl": "0.251",
"origin-lbl": "0.251",
"x-host-header": "d111111abcdef8.cloudfront.net",
"cs(Cookie)": "examplecookie=value"
}
```

Envío de registros a Firehose

Para enviar registros a Firehose, cree o use un flujo de entrega de Firehose existente. A continuación, especifique una secuencia de entrega de Firehose como el destino de entrega de

registro. Debe especificar una secuencia de entrega de Firehose en la región Este de EE. UU. (Norte de Virginia) us-east-1.

Para obtener más información sobre cómo crear su flujo de entrega, consulte Creating an Amazon Data Firehose delivery stream.

Después de crear el flujo de entrega, debe contar con los permisos necesarios para permitir el registro estándar. Para obtener más información, consulte Logs sent to Firehose en la Guía del usuario de Registros de Amazon CloudWatch.

> **Note**
>
> Cuando especifique el nombre del flujo de Firehose, use únicamente el patrón de expresiones regulares `[\w-]`. Para obtener más información, consulte la operación de la API PutDeliveryDestination en la Referencia de la API de Registros de Amazon CloudWatch.

Ejemplo de registro de acceso enviado a Firehose

```
{"date":"2024-11-15","time":"19:45:51","x-edge-location":"SOF50-
P2","asn":"16509","timestamp(ms)":"1731699951183","origin-fbl":"0.254","origin-
lbl":"0.254","x-host-
header":"d111111abcdef8.cloudfront.net","cs(Cookie)":"examplecookie=value"}
{"date":"2024-11-15","time":"19:45:52","x-edge-location":"SOF50-
P2","asn":"16509","timestamp(ms)":"1731699952950","origin-fbl":"0.125","origin-
lbl":"0.125","x-host-
header":"d111111abcdef8.cloudfront.net","cs(Cookie)":"examplecookie=value"}
```

Envío de registros a Amazon S3

Para enviar sus registros de acceso a Amazon S3, cree o utilice un bucket de S3 existente. Cuando active el registro en CloudFront, especifique el nombre del bucket. Para obtener más información sobre la creación de un bucket, consulte Create a bucket en la Guía del usuario de Amazon Simple Storage Service.

Después de crear el bucket, debe contar con los permisos necesarios para permitir el registro estándar. Para obtener más información, consulte Registros enviados a Amazon S3 en la Guía del usuario de Registros de Amazon CloudWatch.

- Una vez que active el registro, AWS agregará automáticamente las políticas de bucket necesarias.

- También puede usar buckets de S3 en las Regiones de AWS de inscripción.

> **Note**
>
> Si ya ha activado el registro estándar (heredado) y quiere activar el registro estándar (v2) en Amazon S3, le recomendamos que especifique un bucket de Amazon S3 diferente o utilice una ruta distinta en el mismo bucket (por ejemplo, utilice un prefijo de registro o una partición). Esto le ayuda a realizar un seguimiento de los archivos de registro que están asociados a cada distribución y evita que los archivos de registro se sobrescriban entre sí.

Temas

- Especificación de un bucket de S3
- Particiones
- Formato de nombre de archivo compatible con Hive
- Ejemplos de rutas a los registros de acceso
- Ejemplo de registro de acceso enviado a Amazon S3

Especificación de un bucket de S3

Cuando especifique un bucket de S3 como destino de entrega, tenga en cuenta lo siguiente.

El nombre del bucket de S3 solo puede usar el patrón de expresiones regulares `[\w-]`. Para obtener más información, consulte la operación de la API PutDeliveryDestination en la Referencia de la API de Registros de Amazon CloudWatch.

Si especificó un prefijo para su bucket de S3, sus registros aparecen en esa ruta. Si no especifica ningún prefijo, CloudFront anexará automáticamente el prefijo `AWSLogs/{account-id}/CloudFront`.

Para obtener más información, consulte Ejemplos de rutas a los registros de acceso.

Particiones

Puede utilizar la partición para organizar los registros de acceso cuando CloudFront los envía a su bucket de S3. Esto le ayuda a organizar y localizar sus registros de acceso en función de la ruta que desee.

Puede utilizar las siguientes variables para crear una ruta de carpeta.

- `{DistributionId}` o `{distributionid}`
- `{yyyy}`
- `{MM}`
- `{dd}`
- `{HH}`
- `{accountid}`

Puede utilizar cualquier número de variables y especificar los nombres de las carpetas en la ruta. A continuación, CloudFront utiliza esta ruta para crear una estructura de carpetas en el bucket de S3.

Ejemplos

- *my_distribution_log_data*/{DistributionId}/*logs*
- /*cloudfront*/{DistributionId}/*my_distribution_log_data*/{yyyy}/{MM}/{dd}/{HH}/*logs*

> **Note**
>
> Puede usar cualquiera de las variables como ID de distribución en la ruta del sufijo. Sin embargo, si va a enviar los registros de acceso a AWS Glue, debe usar la variable `{distributionid}`, ya que AWS Glue espera que los nombres de las particiones estén en minúsculas. Actualice la configuración de registro existente en CloudFront para reemplazar `{DistributionId}` por `{distributionid}`.

Formato de nombre de archivo compatible con Hive

Puede utilizar esta opción para que los objetos de S3 que contienen los registros de acceso entregados utilicen una estructura de prefijos que permita la integración con Apache Hive. Para obtener más información, consulte la operación de la API CreateDelivery.

Example Ejemplo

```
/cloudfront/DistributionId={DistributionId}/my_distribution_log_data/year={yyyy}/
month={MM}/day={dd}/hour={HH}/logs
```

Para obtener más información sobre las particiones y las opciones compatibles con Hive, consulte el elemento S3DeliveryConfiguration en la Referencia de la API de Registros de Amazon CloudWatch.

Ejemplos de rutas a los registros de acceso

Al especificar un bucket de S3 como destino, puede usar las siguientes opciones para crear la ruta a sus registros de acceso:

- Un bucket de Amazon S3, con o sin prefijo
- Partición, mediante una variable proporcionada por CloudFront o introduciendo la suya propia
- Activación de la opción Compatible con Hive

En las siguientes tablas, se muestra cómo aparecen los registros de acceso en el bucket, según las opciones que elija.

Bucket de Amazon S3 con prefijo

Nombre de bucket de Amazon S3	Partición que especifique en la ruta del sufijo	Ruta del sufijo actualizada	¿Se ha activado Compatible con Hive?	Los registros de acceso se envían a
`amzn-s3-demo-bucket/MyLogPrefix`	Ninguno	Ninguno	No	`amzn-s3-demo-bucket/MyLogPrefix/`
`amzn-s3-demo-bucket/MyLogPrefix`	`myFolderA/`	`myFolderA/`	No	`amzn-s3-demo-bucket/MyLogPrefix/myFolderA/`
`amzn-s3-demo-bucket/MyLogPrefix`	`myFolderA/{yyyy}`	`myFolderA/{yyyy}`	Sí	`amzn-s3-demo-bucket/MyLogPrefix/myFolderA/year=2025`

Bucket de Amazon S3 sin prefijo

Nombre de bucket de Amazon S3	Partición que especifique en la ruta del sufijo	Ruta del sufijo actualizada	¿Se ha activado Compatible con Hive?	Los registros de acceso se envían a
amzn-s3-demo-bucket	Ninguno	AWSLogs/{account-id}/CloudFront/	No	amzn-s3-demo-bucket/AWSLogs/ <your-account-ID> /CloudFront/
amzn-s3-demo-bucket	myFolderA/	AWSLogs/{account-id}/CloudFront/myFolderA/	No	amzn-s3-demo-bucket/AWSLogs/ <your-account-ID> /CloudFront/myFolderA/
amzn-s3-demo-bucket	myFolderA/	AWSLogs/{account-id}/CloudFront/myFolderA/	Sí	amzn-s3-demo-bucket/AWSLogs/aws-account-id=<your-account-ID> /CloudFront/myFolderA/
amzn-s3-demo-bucket	myFolderA/{yyyy}	AWSLogs/{account-id}/CloudFront/myFolderA/{yyyy}	Sí	amzn-s3-demo-bucket/AWSLogs/aws-account-id=<your-acc

Nombre de bucket de Amazon S3	Partición que especifique en la ruta del sufijo	Ruta del sufijo actualizada	¿Se ha activado Compatible con Hive?	Los registros de acceso se envían a
				`ount-ID>` / `CloudFront/myFolderA/year=2025`

ID de Cuenta de AWS como partición

Nombre de bucket de Amazon S3	Partición que especifique en la ruta del sufijo	Ruta del sufijo actualizada	¿Se ha activado Compatible con Hive?	Los registros de acceso se envían a
`amzn-s3-demo-bucket`	Ninguno	`AWSLogs/{account-id}/CloudFront/`	Sí	`amzn-s3-demo-bucket/AWSLogs/aws-account-id=<your-account-ID>/CloudFront/`
`amzn-s3-demo-bucket`	`myFolderA/{accountid}`	`AWSLogs/{account-id}/CloudFront/myFolderA/{accountid}`	Sí	`amzn-s3-demo-bucket/AWSLogs/aws-account-id=<your-account-ID>/CloudFront/myFolderA/accountid= <your-account-ID>`

> **Notas**
>
> - La variable `{account-id}` está reservada para CloudFront. CloudFront agrega automáticamente esta variable a la ruta del sufijo si especifica un bucket de Amazon S3 sin prefijo. Si sus registros son compatibles con Hive, esta variable aparece como `aws-account-id`.
> - Puede usar la variable `{accountid}` para que CloudFront agregue su ID de cuenta a la ruta del sufijo. Si sus registros son compatibles con Hive, esta variable aparece como `accountid`.
> - Para obtener más información sobre la ruta del sufijo, consulte S3DeliveryConfiguration.

Ejemplo de registro de acceso enviado a Amazon S3

```
#Fields: date time x-edge-location asn timestamp(ms) x-host-header cs(Cookie)
2024-11-14    22:30:25    SOF50-P2    16509    1731623425421
d111111abcdef8.cloudfront.net    examplecookie=value2
```

Desactivación del registro estándar

Puede desactivar el registro estándar de su distribución si ya no lo necesita.

Para desactivar el registro estándar

1. Inicie sesión en la consola de CloudFront.
2. Elija Distribución y, a continuación, su ID de distribución.
3. Elija Registro y, a continuación, en Destinos de registro estándar, seleccione el destino.
4. Elija Administrar y, a continuación, Eliminar.
5. Repita el paso anterior si tiene más de un registro estándar.

> **Note**
>
> Al eliminar el registro estándar de la consola de CloudFront, esta acción solo elimina la entrega y el destino de entrega. No elimina el origen de entrega de su Cuenta de AWS. Para eliminar un origen de entrega, especifique el nombre de origen de entrega en el comando `aws logs delete-delivery-source --name DeliverySourceName`. Para obtener

más información, consulte DeleteDeliverySource en la Referencia de la API de Registros de Amazon CloudWatch.

Solución de problemas

Utilice la siguiente información para solucionar problemas comunes cuando trabaje con el registro estándar de CloudFront (v2).

El origen de entrega ya existe

Al activar el registro estándar en una distribución, se crea un origen de entrega. A continuación, utiliza ese origen de entrega para crear las entregas al tipo de destino que desee: Registros de CloudWatch, Firehose o Amazon S3. En la actualidad, solo puede haber un origen de entrega por distribución. Si intenta crear otro origen de entrega para la misma distribución, aparecerá el siguiente mensaje de error.

```
This ResourceId has already been used in another Delivery Source in this account
```

Para crear otro origen de entrega, elimine primero el existente. Para obtener más información, consulte DeleteDeliverySource en la Referencia de la API de Registros de Amazon CloudWatch.

He cambiado la ruta del sufijo y el bucket de Amazon S3 no puede recibir mis registros

Si habilitó el registro estándar (v2) y especificó un ARN de bucket sin prefijo, CloudFront agregará el siguiente valor predeterminado a la ruta del sufijo: `AWSLogs/{account-id}/CloudFront`. Si utiliza la consola de CloudFront o la operación de la API UpdateDeliveryConfiguration para especificar una ruta de sufijo diferente, debe actualizar la política del bucket de Amazon S3 para usar la misma ruta.

Example Ejemplo: Actualización de la ruta del sufijo

1. La ruta del sufijo predeterminada es `AWSLogs/{account-id}/CloudFront` y la reemplaza por `myFolderA`.
2. Como la nueva ruta del sufijo es diferente a la ruta especificada en la política del bucket de Amazon S3, no se entregarán los registros de acceso.
3. Puede realizar uno de los siguientes pasos:
   - Actualice el permiso del bucket de Amazon S3 de `amzn-s3-demo-bucket/AWSLogs/<your-account-ID>/CloudFront/*` a `amzn-s3-demo-bucket/myFolderA/*`.

- Actualice su configuración de registro para volver a utilizar el sufijo predeterminado: `AWSLogs/{account-id}/CloudFront`

Para obtener más información, consulte Permisos.

Eliminación de archivos de registro

CloudFront no elimina automáticamente los archivos de registro de su destino. Para obtener información sobre la eliminación de archivos de registro, consulte los siguientes temas:

Amazon S3

- Deleting objects en la Guía del usuario de la consola de Amazon Simple Storage Service

Registros de CloudWatch

- Working with log groups and log streams en la Guía del usuario de Registros de Amazon CloudWatch
- DeleteLogGroup en la Referencia de la API de Registros de Amazon CloudWatch

Firehose

- DeleteDeliveryStream en la Referencia de la API de Amazon Data Firehose

Precios

CloudFront no cobra por activar los registros estándar. Sin embargo, puede incurrir en cargos por la entrega, la ingesta, el almacenamiento o el acceso, según el destino de entrega de los registros que seleccione. Para obtener más información, consulte Precios de Registros de Amazon CloudWatch. En Nivel de pago, seleccione la pestaña Registros y, a continuación, en Registros distribuidos, consulte la información de cada destino de entrega.

Para obtener más información sobre los precios de cada Servicio de AWS, consulte los siguientes temas:

- Precios de Registros de Amazon CloudWatch
- Precios de Amazon Data Firehose
- Precios de Amazon S

> **Note**
>
> No hay cargos adicionales por la entrega de registros a Amazon S3, aunque puede incurrir en cargos de Amazon S3 por almacenar y acceder a los archivos de registro. Si activa la opción Parquet para convertir sus registros de acceso a Apache Parquet, esta opción incurrirá en gastos de CloudWatch. Para obtener más información, consulte la sección Registros distribuidos de Precios de CloudWatch.

Configuración del registro estándar (heredado)

> **Notas**
>
> - Este tema es para la versión anterior del registro estándar. Para obtener la última versión, consulte Configuración del registro estándar (v2).
> - Si ya ha activado el registro estándar (heredado) y quiere activar el registro estándar (v2) en Amazon S3, le recomendamos que especifique un bucket de Amazon S3 diferente o utilice una ruta distinta en el mismo bucket (por ejemplo, utilice un prefijo de registro o una partición). Esto le ayuda a realizar un seguimiento de los archivos de registro que están asociados a cada distribución y evita que los archivos de registro se sobrescriban entre sí.

Para comenzar con el registro estándar (heredado), siga estos pasos:

1. Elija un bucket de Amazon S3 que reciba sus registros y agregue los permisos necesarios.
2. Configure el registro estándar (heredado) desde la consola de CloudFront o la API de CloudFront. Solo puede elegir un bucket de Amazon S3 para recibir los registros.
3. Consulte sus registros de acceso.

Elección de un bucket de Amazon S3 para registros estándar

Al habilitar el registro para una distribución, se especifica el bucket de Amazon S3 en el que desea que CloudFront almacene los archivos de registro. Si utiliza Amazon S3 como origen, le recomendamos que utilice un bucket independiente para los archivos de registro.

Especifique el bucket de Amazon S3 donde desea que CloudFront almacene los registros de acceso, por ejemplo, `amzn-s3-demo-bucket.s3.amazonaws.com`.

Puede almacenar los archivos de registro de varias distribuciones en el mismo bucket. Al habilitar el registro, puede especificar un prefijo para los nombres de archivo, para así realizar un seguimiento de que los archivos de registro que se asocian con las distribuciones.

Elección de un bucket de S3

- El bucket debe tener una lista de control de acceso (ACL) habilitada. Si elige un bucket sin ACL habilitada desde la consola de CloudFront, aparecerá un mensaje de error. Consulte Permisos.
- No elija un bucket de Amazon S3 con Propiedad de objetos de S3 configurado como propietario del bucket forzado. Esta configuración desactiva las ACL para el bucket y los objetos que contiene, lo que evita que CloudFront entregue archivos de registro al bucket.
- No elija un bucket de Amazon S3 en las siguientes Regiones de AWS. CloudFront no entrega registros estándar a buckets en estas regiones:
  - Africa (Cape Town)
  - Asia-Pacífico (Hong Kong)
  - Asia-Pacífico (Hyderabad)
  - Asia-Pacífico (Yakarta)
  - Asia-Pacífico (Melbourne)
  - Oeste de Canadá (Calgary)
  - Europa (Milán)
  - Europa (España)
  - Europa (Zúrich)
  - Israel (Tel Aviv)
  - Medio Oriente (Baréin)
  - Medio Oriente (EAU)

Permisos

> **Important**
>
> A partir de abril de 2023, debe habilitar ACL de S3 para los nuevos buckets de S3 que se utilicen para los registros estándar de CloudFront. Puede habilitar las ACL cuando cree un bucket o habilitar ACL para un bucket existente.
> Para obtener más información sobre los cambios, consulte Configuración predeterminada para preguntas frecuentes de buckets de S3 nuevos en la Guía del usuario de Amazon Simple Storage Service y Aviso: Los cambios en la seguridad de Amazon S3 llegarán en abril de 2023 en el Blog de novedades de AWS.

La Cuenta de AWS debe tener los siguientes permisos para el bucket que especifique para los archivos de registro:

- La ACL del bucket debe concederle `FULL_CONTROL`. Si es el propietario del bucket, su cuenta tiene este permiso de forma predeterminada. Si no está, el propietario del bucket debe actualizar la ACL del bucket.
- `s3:GetBucketAcl`
- `s3:PutBucketAcl`

ACL para el bucket

Al crear o actualizar una distribución y habilitar el registro, CloudFront utiliza estos permisos para actualizar ACL para que el bucket le conceda a la cuenta `awslogsdelivery` permiso `FULL_CONTROL`. La cuenta `awslogsdelivery` escribe archivos de registro en el bucket. Si su cuenta no tiene los permisos necesarios para actualizar la ACL, se producirá un error al crear o actualizar la distribución.

En determinadas circunstancias, si envía una solicitud de forma programada para crear un bucket con un nombre específico, pero ya existe uno con ese nombre, S3 restablece los permisos del bucket a sus valores predeterminados. Si configura CloudFront para guardar los registros de acceso en un bucket de S3 y los registros dejan de guardarse en ese bucket, compruebe los permisos del bucket para asegurarse de que CloudFront dispone de los permisos necesarios.

Restauración de la ACL para el bucket

Si elimina permisos para la cuenta `awslogsdelivery`, CloudFront no podrá guardar registros en el bucket de S3. Para permitir que CloudFront comience a guardar los registros de la distribución de nuevo, restaure el permiso de ACL realizando una de las siguientes acciones:

- Desactive el registro de la distribución en CloudFront y, a continuación, habilítelo de nuevo. Para obtener más información, consulte Registro estándar.
- Agregue el permiso de ACL para `awslogsdelivery` manualmente mediante el acceso al bucket de S3 en la consola de Amazon S3 y agregando permiso. Para añadir la ACL para `awslogsdelivery`, debe proporcionar el ID canónico de la cuenta, que es el siguiente:

  ```
  c4c1ede66af53448b93c283ce9448c4ba468c9432aa01d700d3878632f77d2d0
  ```

  Para obtener más información acerca de cómo agregar ACL a buckets de S3, consulte Configuración de ACL en la Guía del usuario de Amazon Simple Storage Service.

ACL para cada archivo de registro

Además de la ACL del bucket, hay una ACL en cada archivo de registro. El propietario del bucket tiene permisos `FULL_CONTROL` en cada archivo de registro, el propietario de la distribución (si no es el mismo que el del bucket) no tiene permiso, y la cuenta `awslogsdelivery` tiene permisos de lectura y escritura.

Deshabilitar los registros

Si desactiva el registro, CloudFront no elimina las ACL del bucket ni de los archivos de registro. Puede eliminar las ACL si es necesario.

Política de claves necesarias para buckets de SSE-KMS

Si el bucket de S3 de los registros estándar utiliza cifrado del servidor con AWS KMS keys (SSE-KMS) mediante una clave administrada por el cliente, se debe agregar la siguiente instrucción a la política de claves para la clave administrada por el cliente. Esto permite a CloudFront escribir archivos de registro en el bucket. No puede utilizar SSE-KMS con la Clave administrada de AWS, porque CloudFront no podrá escribir los archivos de registro en el bucket.

```
{
    "Sid": "Allow CloudFront to use the key to deliver logs",
    "Effect": "Allow",
```

```
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Si el bucket de S3 para los registros estándar utiliza SSE-KMS con una clave de bucket de S3, también debe agregar el permiso `kms:Decrypt` a la instrucción de la política. En ese caso, la instrucción total de la política se ve del siguiente modo.

```
{
    "Sid": "Allow CloudFront to use the key to deliver logs",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

> **Note**
>
> Cuando habilite SSE-KMS para el bucket de S3, especifique el ARN completo de la clave administrada por el cliente. Para obtener más información, consulte Uso del cifrado del servidor con AWS KMS keys (SSE-KMS) en la Guía del usuario de Amazon Simple Storage Service.

Activación del registro estándar (heredado)

Para activar los registros estándar, use la consola de CloudFront o la API de CloudFront.

Contenido

- Activación del registro estándar (heredado) (consola de CloudFront)
- Activación del registro estándar (heredado) (API de CloudFront)

Activación del registro estándar (heredado) (consola de CloudFront)

Para activar los registros estándar en una distribución de CloudFront (consola)

1. Utilice la consola de CloudFront para crear una nueva distribución o actualizar una existente.
2. En la sección Registro estándar, en Entrega de registros, seleccione Activado.
3. (Opcional) En Registro de cookies, seleccione Activado si desea incluir cookies en sus registros. Para obtener más información, consulte Registro de cookies.

   > **Tip**
   >
   > El registro de cookies es una configuración global que se aplica a todos los registros estándar de su distribución. No puede anular esta configuración para distintos destinos de entrega.

4. En la sección Entregar a, especifique Amazon S3 (heredado).
5. Especifique el bucket de Amazon S3. Si aún no tiene uno, puede elegir Crear o consultar la documentación para crear un bucket.
6. (Opcional) En Prefijo del registro, especifique la cadena, de haberla, a la que CloudFront debe agregar un prefijo para los nombres de archivo de los registros de acceso de esta distribución; por ejemplo, `exampleprefix/`. La barra inclinada (/) al final es opcional pero recomendable para simplificar la navegación de los archivos de registro. Para obtener más información, consulte Prefijo de registros.
7. Complete los pasos para actualizar o crear su distribución.
8. En la página Registros, compruebe que el estado de los registros estándar sea Activado junto a la distribución.

   Para obtener más información sobre la entrega de registros estándar y los campos de registro, consulte Referencia de registro estándar.

Activación del registro estándar (heredado) (API de CloudFront)

También puede utilizar la API de CloudFront para activar los registros estándar en sus distribuciones.

Para activar los registros estándar en una distribución (API de CloudFront)

- Utilice la operación de la API CreateDistribution o UpdateDistribution, y configure el objeto LoggingConfig.

Edición de configuración de registro estándar

Puede habilitar o desactivar el registro, cambiar el bucket de Amazon S3 en el que se almacenan los registros y cambiar el prefijo de los archivos de registro a través de la consola de CloudFront o la API de CloudFront. Los cambios de configuración de registro surten efecto en un plazo de 12 horas.

Para obtener más información, consulte los siguientes temas:

- Para actualizar una distribución mediante la consola de CloudFront, consulte Actualizar una distribución.
- Para actualizar una distribución mediante la API de CloudFront, consulte UpdateDistribution en la Referencia de la API de Amazon CloudFront.

Envío de registros a Amazon S3

Cuando envía los registros a Amazon S3, los registros aparecen en el siguiente formato.

Formato del nombre de archivo

El nombre de cada archivo de registro que CloudFront guarda en el bucket de Amazon S3 utiliza el formato de nombre de archivo siguiente:

```
<optional prefix>/<distribution ID>.YYYY-MM-DD-HH.unique-ID.gz
```

La fecha y la hora se muestran según la hora universal coordinada (UTC).

Por ejemplo, si utiliza `example-prefix` como prefijo y el ID de distribución es `EMLARXS9EXAMPLE`, los nombres de archivo tendrán el siguiente aspecto:

```
example-prefix/EMLARXS9EXAMPLE.2019-11-14-20.RT4KCN4SGK9.gz
```

Al habilitar el registro para una distribución, puede especificar un prefijo para los nombres de archivo, para así realizar un seguimiento de que los archivos de registro que se asocian a las distribuciones. Si incluye un valor para el prefijo del archivo de registro y el prefijo no termina con una barra inclinada (`/`), CloudFront agrega una automáticamente. Si el prefijo termina con una barra inclinada, CloudFront no agrega otra.

`.gz` al final del nombre del archivo indica que CloudFront ha comprimido el archivo de registro con gzip.

Formato de archivo de registro estándar

Cada entrada del archivo de registro ofrece información acerca de una única solicitud de espectador. Los archivos log tienen las siguientes características:

- Utilice el formato de archivo de registro ampliado W3C.
- Contienen valores separados por pestañas.
- Contienen registros que no están necesariamente en orden cronológico.
- Contiene dos líneas de encabezado: una con la versión de formato de archivo y otra que muestra la cantidad de campos de W3C incluidos en cada registro.
- Contiene equivalentes codificados en URL para espacios y otros caracteres determinados en valores de campo.

  Los equivalentes codificados en URL se utilizan para los siguientes caracteres:

  - Códigos de caracteres ASCII de 0 a 32, ambos incluidos
  - Códigos de caracteres ASCII 127 y superiores
  - Todos los caracteres de la tabla siguiente

  El estándar de codificación de URL se define en RFC 1738.

Valor de URL codificada	Carácter
%3C	<
%3E	>
%22	"
%23	#
%25	%
%7B	{
%7D	}
%7C	|

Valor de URL codificada	Carácter
%5C	\
%5E	^
%7E	~
%5B	[
%5D	]
%60	`
%27	'
%20	espacio

Eliminación de archivos de registro

CloudFront no elimina automáticamente los archivos de registro del bucket de Amazon S3. Para obtener más información sobre la eliminación de archivos de registro de un bucket de Amazon S3, consulte Eliminación de objetos en la Guía del usuario de la consola de Amazon Simple Storage Service.

Precios

El registro estándar es una característica opcional de CloudFront. CloudFront no cobra por activar los registros estándar. Sin embargo, se acumulan cargos de Amazon S3 usuales en concepto de almacenamiento y acceso a los archivos en Amazon S3. Puede eliminarlos en cualquier momento.

Para obtener más información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

Para obtener más información acerca de los precios de CloudFront, consulte Precios de CloudFront.

Referencia de registro estándar

Las siguientes secciones se aplican tanto al registro estándar (v2) como al registro estándar (heredado).

Temas

- Intervalo de entrega de archivos de registro
- Cómo se registran las solicitudes cuando la URL o los encabezados de la solicitud sobrepasan el tamaño máximo
- Campos de un archivo de registro
- Análisis de registros

Intervalo de entrega de archivos de registro

CloudFront entrega registros para su distribución varias veces cada hora. En general, un archivo de registro contiene información acerca de las solicitudes que CloudFront ha recibido durante un periodo determinado. Normalmente, CloudFront entrega el archivo de registro de ese periodo al destino una hora después de que se produzcan los eventos reflejados en el registro. Tenga en cuenta, sin embargo, que algunas o todas las entradas de los archivos de registro de un periodo a veces pueden retrasarse hasta 24 horas. Cuando se retrasan entradas de registro, CloudFront las guarda en un archivo de registro cuyo nombre de archivo incluye la fecha y la hora del periodo en el que se realizaron las solicitudes en lugar de incluir la fecha y la hora de entrega del archivo.

Al crear un archivo de registro, CloudFront consolida información para la distribución desde todas las ubicaciones de borde que recibieron solicitudes de los objetos durante el periodo que abarca dicho archivo de registro.

CloudFront puede guardar más de un archivo por periodo en función de la cantidad de solicitudes de objetos asociados con una distribución que recibe CloudFront.

CloudFront comienza a enviar de forma fiable los registros de acceso unas cuatro horas después de habilitar los registros. Es posible obtener algunos registros de acceso antes del momento de envío.

> **Note**
>
> Si ningún usuario solicita sus objetos durante un periodo, no recibirá archivos de registro para ese periodo.

Cómo se registran las solicitudes cuando la URL o los encabezados de la solicitud sobrepasan el tamaño máximo

Si el tamaño total de todos los encabezados de solicitud, incluidas las cookies, supera los 20 KB o si la URL supera los 8192 bytes, CloudFront no puede analizar la solicitud por completo y no puede

registrar la solicitud. Dado que la solicitud no se registra, el código de estado que se devuelve no se verá en los archivos de registro de error de HTTP.

Si el cuerpo de la solicitud supera el tamaño máximo, se registra la solicitud, incluido el código de estado de error de HTTP.

Campos de un archivo de registro

El archivo de registro de una distribución contiene 33 campos. La lista siguiente contiene el nombre de cada campo, en orden, junto con una descripción de la información de ese campo.

1. **`date`**

   La fecha en que se produjo el evento en el formato `YYYY-MM-DD`. Por ejemplo, `2019-06-30`. La fecha y la hora se muestran según la hora universal coordinada (UTC). Para conexiones de WebSockets, indica la fecha de cierre de la conexión.
2. **`time`**

   La hora a la que el servidor de CloudFront terminó de responder a la solicitud (en UTC), por ejemplo, `01:42:39`. Para conexiones de WebSockets, indica la hora de cierre de la conexión.
3. **`x-edge-location`**

   La ubicación de borde que atendió la solicitud. Cada ubicación periférica se identifica mediante un código de tres letras y un número asignado arbitrariamente (por ejemplo, DFW3). El código de tres letras normalmente se corresponde con el código del aeropuerto de la Asociación de Transporte Aéreo Internacional (IATA) más cercano a la ubicación geográfica de la ubicación periférica. Estas abreviaturas pueden cambiar en el futuro.
4. **`sc-bytes`**

   El número total de bytes que el servidor ha enviado al lector en respuesta a la solicitud, incluidos los encabezados. Para conexiones WebSocket y gRPC, se trata del número total de bytes enviados desde el servidor al cliente a través de la conexión.
5. **`c-ip`**

   La dirección IP del espectador que ha realizado la solicitud, por ejemplo, `192.0.2.183` o `2001:0db8:85a3::8a2e:0370:7334`. Si el lector ha utilizado un proxy HTTP o un equilibrador de carga para enviar la solicitud, el valor de este campo es la dirección IP del proxy o del balanceador de carga. Consulte también el campo `x-forwarded-for`.
6. **`cs-method`**

El método de solicitud HTTP recibido del lector.

7. **`cs(Host)`**

   El nombre de dominio de la distribución de CloudFront (por ejemplo, d111111abcdef8.cloudfront.net).

8. **`cs-uri-stem`**

   La parte de la URL de solicitud que identifica la ruta y el objeto (por ejemplo, `/images/cat.jpg`). Los signos de interrogación (?) de las URL y las cadenas de consulta no están incluidas en el registro.

9. **`sc-status`**

   Contiene uno de los siguientes valores:

   - El código de estado HTTP de la respuesta del servidor (por ejemplo, `200`).
   - `000`, que indica que el lector ha cerrado la conexión antes de que el servidor pudiese responder a la solicitud. Si el lector cierra la conexión después de que el servidor comience a enviar la respuesta, este campo contiene el código de estado HTTP de la respuesta que el servidor había comenzado a enviar.

10. **`cs(Referer)`**

    El valor del encabezado `Referer` de la solicitud. Este es el nombre del dominio que ha originado la solicitud. Entre los remitentes principales se incluyen motores de búsqueda, otros sitios web que enlazan directamente con sus objetos y su propio sitio web.

11. **`cs(User-Agent)`**

    El valor del encabezado `User-Agent` de la solicitud. El encabezado `User-Agent` identifica el origen de la solicitud, como el tipo de dispositivo y el navegador que enviaron la solicitud o, si la solicitud provino de un motor de búsqueda, de cuál.

12. **`cs-uri-query`**

    La parte de la cadena de consulta de la URL, de haberla.

    Cuando una URL no contiene una cadena de consulta, el valor de este campo es un guion (-). Para obtener más información, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta.

13. **`cs(Cookie)`**

El encabezado `Cookie` de la solicitud, incluidos los pares nombre-valor y los atributos asociados.

Si habilita el registro de cookies, CloudFront registra las cookies de todas las solicitudes independientemente de qué cookies elija reenviar al origen. Cuando una solicitud no incluye un encabezado de cookie, el valor de este campo es un guion (-). Para obtener más información acerca de cookies, consulte Almacenamiento en caché de contenido en función de cookies.

14 **`x-edge-result-type`**

Cómo el servidor ha clasificado la respuesta después de que el último byte abandonara el servidor. En algunos casos, el tipo de resultado puede cambiar entre el momento en que el servidor está listo para enviar la respuesta y el momento en que termina el envío de la respuesta. Consulte también el campo `x-edge-response-result-type`.

Por ejemplo, en el streaming de HTTP, se supone que el servidor encuentra un segmento de la secuencia en la caché. En esta situación, el valor de este campo sería normalmente `Hit`. Sin embargo, si el lector cierra la conexión antes de que el servidor haya entregado todo el segmento, el tipo de resultado final (y el valor de este campo) es `Error`.

Las conexiones WebSocket y gRPC tendrán un valor de `Miss` para este campo porque el contenido no se puede almacenar en caché y se entrega directamente al origen.

Entre los valores posibles se incluyen:

- `Hit`: el servidor ofreció el objeto al lector desde la caché.
- `RefreshHit`: el servidor encontró el objeto en la caché pero el objeto había vencido, por lo que el servidor se puso en contacto con el origen para comprobar que la caché tenía la versión más reciente del objeto.
- `Miss`: un objeto en la caché no ha podido satisfacer la solicitud, así que el servidor la ha reenviado al origen y ha devuelto el resultado al lector.
- `LimitExceeded`: se ha denegado la solicitud porque se superó una cuota (antes denominada límite) de CloudFront.
- `CapacityExceeded`: el servidor ha devuelto un código de estado HTTP 503 porque no disponía de capacidad suficiente en el momento de la solicitud para prestar servicio al objeto.
- `Error`: normalmente, esto significa que la solicitud ha dado lugar a un error de cliente (el valor del campo `sc-status` está en el intervalo `4xx`) o un error de servidor (el valor del campo `sc-status` está en el intervalo `5xx`). Si el valor del campo `sc-status` es `200` o si el valor de este campo es `Error` y el valor del campo `x-edge-response-result-type` no es

`Error`, significa que la solicitud HTTP se ha realizado correctamente pero el cliente se ha desconectado antes de recibir todos los bytes.

- `Redirect`: el servidor ha redirigido al lector de HTTP a HTTPS de acuerdo con la configuración de distribución.
- `LambdaExecutionError`: la función de Lambda@Edge asociada con la distribución no se ha completado debido a una asociación incorrecta, al tiempo de espera de una función, a un problema de dependencia de AWS o a otro problema de disponibilidad general.

15. **`x-edge-request-id`**

    Una cadena opaca que identifica una solicitud de forma única. CloudFront también envía esta cadena en el encabezado de respuesta `x-amz-cf-id`.

16. **`x-host-header`**

    El valor que el lector ha incluido en el encabezado `Host` de la solicitud. Si utiliza el nombre de dominio CloudFront en las URL de los objetos (como d111111abcdef8.cloudfront.net), este campo contiene ese nombre de dominio. Si utiliza nombres de dominio alternativos (CNAME) en las URL de los objetos (como www.example.com), este campo contiene el nombre de dominio alternativo.

    Si está utilizando nombres de dominio alternativo, consulte `cs(Host)` en el campo 7 para ver el nombre de dominio asociado con su distribución.

17. **`cs-protocol`**

    El protocolo de la solicitud del lector (`http`, `https`, `grpcs`, `ws` o `wss`).

18. **`cs-bytes`**

    El número total de bytes de datos que el lector ha incluido en la solicitud, incluidos los encabezados. Para conexiones WebSocket y gRPC, se trata del número total de bytes enviados desde el cliente al servidor en la conexión.

19. **`time-taken`**

    El número de segundos (hasta la milésima de segundo, por ejemplo, 0,082) desde que el servidor recibe la solicitud del lector hasta que el servidor escribe el último byte de la respuesta en la cola de salida, según se mide en el servidor. Desde el punto de vista del lector, el tiempo total para obtener la respuesta completa será superior a este valor a causa de la latencia de la red y el almacenamiento en búfer de TCP.

20. **`x-forwarded-for`**

Si el lector ha utilizado un proxy HTTP o un balanceador de carga para enviar la solicitud, el valor del campo `c-ip` es la dirección IP del proxy o del balanceador de carga. En ese caso, este campo es la dirección IP del espectador que originó la solicitud. Este campo puede contener varias direcciones IP separadas por comas. Cada dirección IP puede ser una dirección IPv4 (por ejemplo, `192.0.2.183`) o una dirección IPv6 (por ejemplo, `2001:0db8:85a3::8a2e:0370:7334`).

Si el lector no utiliza un proxy HTTP o un balanceador de carga, el valor de este campo es un guion (-).

21 **`ssl-protocol`**

Cuando la solicitud ha utilizado HTTPS, este campo contiene el protocolo SSL/TLS que el lector y el servidor han negociado para transmitir la solicitud y la respuesta. Para obtener una lista de valores posibles, consulte los protocolos SSL/TLS compatibles en Protocolos y cifrados admitidos entre lectores y CloudFront.

Cuando `cs-protocol` en el campo 17 es `http`, el valor de este campo es un guion (-).

22 **`ssl-cipher`**

Cuando la solicitud ha utilizado HTTPS, este campo contiene el cifrado SSL/TLS que el lector y el servidor han negociado para cifrar la solicitud y la respuesta. Para obtener una lista de valores posibles, consulte los cifrados SSL/TLS compatibles en Protocolos y cifrados admitidos entre lectores y CloudFront.

Cuando `cs-protocol` en el campo 17 es `http`, el valor de este campo es un guion (-).

23 **`x-edge-response-result-type`**

Cómo el servidor ha clasificado la respuesta antes de devolver la respuesta al lector. Consulte también el campo `x-edge-result-type`. Entre los valores posibles se incluyen:

- `Hit`: el servidor ofreció el objeto al lector desde la caché.
- `RefreshHit`: el servidor encontró el objeto en la caché pero el objeto había vencido, por lo que el servidor se puso en contacto con el origen para comprobar que la caché tenía la versión más reciente del objeto.
- `Miss`: un objeto en la caché no ha podido satisfacer la solicitud, así que el servidor ha reenviado la solicitud al servidor de origen y ha devuelto el resultado al lector.

- `LimitExceeded`: se ha denegado la solicitud porque se superó una cuota (antes denominada límite) de CloudFront.
- `CapacityExceeded`: el servidor ha devuelto un error 503 porque no disponía de capacidad suficiente en el momento de la solicitud para prestar servicio al objeto.
- `Error`: normalmente, esto significa que la solicitud ha dado lugar a un error de cliente (el valor del campo `sc-status` está en el intervalo `4xx`) o un error de servidor (el valor del campo `sc-status` está en el intervalo `5xx`).

  Si el valor del campo `x-edge-result-type` es `Error` y el valor de este campo no es `Error`, el cliente se ha desconectado antes de finalizar la descarga.
- `Redirect`: el servidor ha redirigido al lector de HTTP a HTTPS de acuerdo con la configuración de distribución.
- `LambdaExecutionError`: la función de Lambda@Edge asociada con la distribución no se ha completado debido a una asociación incorrecta, al tiempo de espera de una función, a un problema de dependencia de AWS o a otro problema de disponibilidad general.

24. **`cs-protocol-version`**

    La versión de HTTP que el espectador especificó en la solicitud. Entre los valores posibles se incluyen `HTTP/0.9`, `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0` y `HTTP/3.0`.

25. **`fle-status`**

    Cuando se configura el cifrado en el nivel de campo para una distribución, este campo contiene un código que indica si el cuerpo de la solicitud se ha procesado correctamente. Cuando el servidor procesa correctamente el cuerpo de la solicitud, cifra los valores de los campos especificados y reenvía la solicitud al origen, el valor de este campo es `Processed`. El valor de `x-edge-result-type` todavía puede indicar un error del lado del cliente o del lado del servidor en este caso.

    Los valores posibles para este campo son:

    - `ForwardedByContentType`: el servidor ha reenviado la solicitud al origen sin analizar ni cifrar porque no se ha configurado ningún tipo de contenido.
    - `ForwardedByQueryArgs`: el servidor ha reenviado la solicitud al origen sin analizar ni cifrar porque la solicitud contiene un argumento de consulta que no estaba en la configuración de cifrado en el nivel de campo.

- `ForwardedDueToNoProfile`: el servidor ha reenviado la solicitud al origen sin analizar ni cifrar porque no se ha especificado ningún perfil en la configuración de cifrado en el nivel de campo.
- `MalformedContentTypeClientError`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque el valor del encabezado `Content-Type` estaba en un formato no válido.
- `MalformedInputClientError`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque el cuerpo de la solicitud estaba en un formato no válido.
- `MalformedQueryArgsClientError`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque un argumento de consulta estaba vacío o tenía un formato no válido.
- `RejectedByContentType`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque no se ha especificado ningún tipo de contenido en la configuración de cifrado en el nivel de campo.
- `RejectedByQueryArgs`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque no se ha especificado ningún argumento de consulta en la configuración de cifrado en el nivel de campo.
- `ServerError`: el servidor de origen ha devuelto un error.

Si la solicitud supera una cuota de cifrado en el nivel de campo (anteriormente denominada límite), este campo contiene uno de los siguientes códigos de error y el servidor devuelve el código de estado HTTP 400 al lector. Para obtener una lista de las cuotas actuales del cifrado en el nivel de campo, consulte Cuotas de cifrado en el nivel de campo.

- `FieldLengthLimitClientError`: un campo que se ha configurado como cifrado ha superado la longitud máxima permitida.
- `FieldNumberLimitClientError`: una solicitud que la distribución ha configurado para cifrar contiene un número de campos mayor del permitido.
- `RequestLengthLimitClientError`: la longitud del cuerpo de la solicitud ha superado el máximo permitido cuando se ha configurado el cifrado en el nivel de campo.

Si no se ha configurado el cifrado en el nivel de campo para la distribución, el valor de este campo es un guion (-).

26. **`fle-encrypted-fields`**

El número de campos de cifrado en el nivel de campo que el servidor ha cifrado y reenviado al origen. Los servidores de CloudFront transmiten la solicitud procesada al origen a medida que cifran los datos, por lo que este campo puede tener un valor incluso si el valor de `fle-status` es un error.

Si no se ha configurado el cifrado en el nivel de campo para la distribución, el valor de este campo es un guion (-).

27. **`c-port`**

    El número de puerto de la solicitud desde el espectador.

28. **`time-to-first-byte`**

    El número de segundos entre la recepción de la solicitud y la escritura del primer byte de la respuesta, medido en el servidor.

29. **`x-edge-detailed-result-type`**

    Este campo contiene el mismo valor que el campo `x-edge-result-type`, excepto en los siguientes casos:

    - Cuando el objeto se ha servido al lector desde la capa de Origin Shield, este campo contiene `OriginShieldHit`.
    - Cuando el objeto no estaba en la memoria caché de CloudFront y la respuesta se generó mediante una función Lambda@Edge de solicitud de origen, este campo contiene `MissGeneratedResponse`.
    - Cuando el valor del campo `x-edge-result-type` es `Error`, este campo contiene uno de los siguientes valores con más información sobre el error:
      - `AbortedOrigin`: el servidor ha encontrado un problema con el origen.
      - `ClientCommError`: la respuesta al lector se ha interrumpido debido a un problema de comunicación entre el servidor y el lector.
      - `ClientGeoBlocked`: la distribución está configurada para rechazar solicitudes desde la ubicación geográfica del lector.
      - `ClientHungUpRequest`: el espectador se ha detenido prematuramente mientras enviaba la solicitud.
      - `Error`: se ha producido un error cuyo tipo de error no se ajusta a ninguna de las otras categorías. Este tipo de error puede producirse cuando el servidor envía una respuesta de error desde la caché.

- `InvalidRequest`: el servidor ha recibido una solicitud no válida desde el lector.
- `InvalidRequestBlocked`: el acceso al recurso solicitado está bloqueado.
- `InvalidRequestCertificate`: la distribución no coincide con el certificado SSL/TLS para el que se ha establecido la conexión HTTPS.
- `InvalidRequestHeader`: la solicitud contenía un encabezado no válido.
- `InvalidRequestMethod`: la distribución no está configurada para gestionar el método de solicitud HTTP que se ha utilizado. Esto puede suceder cuando la distribución solo admite solicitudes que se pueden almacenar en caché.
- `OriginCommError`: se agotó el tiempo de espera de la solicitud al conectarse a un origen o al leer datos de un origen.
- `OriginConnectError`: el servidor no ha podido conectarse al origen.
- `OriginContentRangeLengthError`: el encabezado `Content-Length` de la respuesta del origen no coincide con la longitud del encabezado `Content-Range`.
- `OriginDnsError`: el servidor no ha podido resolver el nombre de dominio del origen.
- `OriginError`: el origen ha devuelto una respuesta incorrecta.
- `OriginHeaderTooBigError`: un encabezado devuelto por el origen es demasiado grande para que el servidor de borde lo procese.
- `OriginInvalidResponseError`: el origen ha devuelto una respuesta no válida.
- `OriginReadError`: el servidor no ha podido leer desde el origen.
- `OriginWriteError`: el servidor no ha podido escribir en el origen.
- `OriginZeroSizeObjectError`: un objeto de tamaño cero enviado desde el origen ha provocado un error.
- `SlowReaderOriginError`: el espectador ha sido al leer el mensaje que ha provocado el error de origen.

30 **`sc-content-type`**

El valor del encabezado HTTP `Content-Type` de la respuesta.

31 **`sc-content-len`**

El valor del encabezado HTTP `Content-Length` de la respuesta.

32 **`sc-range-start`**

Cuando la respuesta contiene el encabezado HTTP `Content-Range`, este campo contiene el valor inicial del intervalo.

33 **`sc-range-end`**

Cuando la respuesta contiene el encabezado HTTP `Content-Range`, este campo contiene el valor final del intervalo.

34 **`distribution-tenant-id`**

El ID del inquilino de la distribución.

35 **`connection-id`**

Un identificador único para la conexión TLS.

Debe habilitar los mTLS para las distribuciones antes de poder obtener información para este campo. Para obtener más información, consulte Autenticación TLS mutua con CloudFront (mTLS de espectador).

A continuación, se muestra un ejemplo de archivo de registro de una distribución.

```
#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 - -
```

Análisis de registros

Dado que puede recibir varios registros de acceso por hora, le recomendamos que combine en un mismo archivo todos los archivos de registro que reciba para un periodo determinado. Así podrá analizar los datos de ese periodo de forma más completa y precisa.

Una forma de analizar los registros de acceso consiste en utilizar Amazon Athena. Athena es un servicio de consultas interactivo que puede ayudarlo a analizar datos de los servicios de AWS, incluido CloudFront. Para obtener más información, consulte Consulta de los registros de Amazon CloudFront en la Guía del usuario de Amazon Athena.

Además, en las siguientes entradas del blog de AWS se explican algunas formas de analizar los registros de acceso.

- Amazon CloudFront Request Logging (para contenido enviado a través de HTTP)
- Enhanced CloudFront Logs, Now With Query Strings

Uso de registros de acceso en tiempo real

Con los registros de acceso en tiempo real de CloudFront, puede obtener información sobre las solicitudes realizadas a una distribución en tiempo real (los registros se envían en cuestión de segundos después de recibir las solicitudes). Puede usar los registros de acceso en tiempo real para supervisar, analizar y tomar medidas en función del rendimiento de entrega de contenido.

Los registros de acceso en tiempo real de CloudFront son configurables. Puede elegir:

- La frecuencia de muestreo de los registros en tiempo real, es decir, el porcentaje de solicitudes de las que desea recibir entradas de registro de acceso en tiempo real.
- Los campos específicos que desea recibir en los registros de log.
- Los comportamientos de caché específicos (patrones de ruta) para los que desea recibir registros en tiempo real.

Los registros de acceso en tiempo real de CloudFront se envían al flujo de datos de su elección en Amazon Kinesis Data Streams. Puede crear su propio consumidor de flujos de datos de Kinesis o utilizar Amazon Data Firehose para enviar los datos de registro a Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon OpenSearch Service (OpenSearch Service) o a un servicio de procesamiento de registros de terceros.

CloudFront aplica cargos por los registros de acceso en tiempo real, que se suman a los cargos que se aplican por el uso de Kinesis Data Streams. Para obtener más información acerca de los precios, consulte Precios de Amazon CloudFront y Precios de Amazon Kinesis Data Streams.

> **Important**
>
> Recomendamos utilizar los registros de acceso para comprender la naturaleza de las solicitudes hechas a su contenido y no como una relación exhaustiva de todas las solicitudes. CloudFront envía registros de acceso en tiempo real en la medida en que sea posible. La entrada de registro de una solicitud determinada puede entregarse mucho después de la solicitud se haya procesado realmente y, en casos contados, es probable que una entrada de registro no se entregue en absoluto. Cuando se omite una entrada de registro de los registros de acceso en tiempo real, la cantidad de entradas de los registros de acceso en tiempo real no coincide con el uso que aparece en los informes de facturación y de uso de AWS.

Temas

- Creación y uso de configuraciones de registro de acceso en tiempo real
- Descripción de las configuraciones de registros de acceso en tiempo real
- Creación de un consumidor de Kinesis Data Streams
- Resolución de problemas de registros de acceso en tiempo real

Creación y uso de configuraciones de registro de acceso en tiempo real

Para obtener información sobre las solicitudes realizadas a una distribución en tiempo real, puede usar configuraciones de registro de acceso en tiempo real. Los registros se entregan en cuestión de segundos después de recibir las solicitudes. Puede crear una configuración de registro de acceso en tiempo real en la consola de CloudFront, con AWS Command Line Interface (AWS CLI) o con la API de CloudFront.

Para utilizar una configuración de registro de acceso en tiempo real, puede asociarla a uno o más comportamientos de caché en una distribución de CloudFront.

Console

Creación de una configuración de registro de acceso en tiempo real

1. Inicie sesión en la Consola de administración de AWS y abra la página Logs (Registros) en la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home?#/logs.
2. Elija la pestaña Configuraciones en tiempo real.
3. Seleccione Crear configuración.
4. En Nombre, escriba un nombre para la configuración.
5. En Frecuencia de muestreo, introduzca el porcentaje de solicitudes de las que desea recibir entradas de registro.
6. En Campos, elija los campos que desee recibir en los registros de acceso en tiempo real.
   - Para incluir todos los campos de CMCD en los registros, elija Todas las claves de CMCD.
7. En Punto de conexión, elija uno o más flujos de datos de Kinesis para recibir registros de acceso en tiempo real.

> **Note**
>
> Los registros de acceso en tiempo real de CloudFront se envían al flujo de datos que especifique en Kinesis Data Streams. Para leer y analizar los registros de acceso en tiempo real, puede crear su propio consumidor de flujo de datos de Kinesis. También puede utilizar Firehose para enviar los datos de registro a Amazon S3, Amazon Redshift, Amazon OpenSearch Service o un servicio de procesamiento de registros de terceros.

8. En Rol de IAM, elija Crear un nuevo rol de servicio o elija un rol existente. Debe tener permiso para crear roles de IAM.
9. (Opcional) En Distribución, elija una distribución y el comportamiento de caché de CloudFront que desee asociar a la configuración de registro de acceso en tiempo real.
10. Seleccione Crear configuración.

Si se realiza correctamente, la consola muestra los detalles de la configuración de registro de acceso en tiempo real que acaba de crear.

Para obtener más información, consulte Descripción de las configuraciones de registros de acceso en tiempo real.

AWS CLI

Para crear una configuración de registro de acceso en tiempo real con la AWS CLI, utilice el comando aws cloudfront create-realtime-log-config. Puede utilizar un archivo de entrada para proporcionar los parámetros de entrada del comando, en lugar de especificar cada parámetro individual como entrada de línea de comandos.

Para crear una configuración de registro de acceso en tiempo real (CLI con archivo de entrada)

1. Utilice el siguiente comando para crear un archivo denominado `rtl-config.yaml` que contenga todos los parámetros de entrada del comando create-realtime-log-config.

```
aws cloudfront create-realtime-log-config --generate-cli-skeleton yaml-input >
 rtl-config.yaml
```

2. Abra el archivo llamado `rtl-config.yaml` que acaba de crear. Edite el archivo para especificar los ajustes de configuración del registro de acceso en tiempo real que desee y, a continuación, guarde el archivo. Tenga en cuenta lo siguiente:

   - Para `StreamType`, el único valor válido es `Kinesis`.

   Para obtener más información acerca de los ajustes de configuración largos en tiempo real, consulte Descripción de las configuraciones de registros de acceso en tiempo real.

3. Utilice el siguiente comando para crear la configuración de registro de acceso en tiempo real utilizando los parámetros de entrada del archivo de `rtl-config.yaml`.

```
aws cloudfront create-realtime-log-config --cli-input-yaml file://rtl-
config.yaml
```

Si se realiza correctamente, la salida del comando muestra los detalles de la configuración de registro de acceso en tiempo real que acaba de crear.

Para asociar una configuración de registro de acceso en tiempo real a una distribución existente (CLI con archivo de entrada)

1. Utilice el comando siguiente para guardar la configuración de distribución de la distribución de CloudFront que desea actualizar. Reemplace *`distribution_ID`* por el ID de la distribución.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Abra el archivo llamado `dist-config.yaml` que acaba de crear. Edite el archivo, realizando los siguientes cambios en cada comportamiento de caché que actualice para utilizar una configuración de registro de acceso en tiempo real.

   - En el comportamiento de caché, agregue un campo denominado `RealtimeLogConfigArn`. Para el valor del campo, utilice el ARN de la configuración de registro de acceso en tiempo real que desea asociar a este comportamiento de caché.
   - Cambie el nombre del campo `ETag` a `IfMatch`, pero no cambie el valor del campo.

Guarde el archivo cuando haya terminado.

3. Utilice el siguiente comando para actualizar la distribución para utilizar la configuración de registro de acceso en tiempo real. Reemplace *distribution_ID* por el ID de la distribución.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Si tiene éxito, la salida del comando muestra los detalles de la distribución que acaba de actualizar.

API

Para crear una configuración de registro de acceso en tiempo real con la API de CloudFront, utilice la operación de la API CreateRealtimeLogConfig. Para obtener más información sobre los parámetros que especifique en esta llamada a la API, consulte Descripción de las configuraciones de registros de acceso en tiempo real y la documentación de referencia de la API para su SDK de AWS u otro cliente de la API.

Después de crear una configuración de registro de acceso en tiempo real, puede asociarla a un comportamiento de caché mediante una de las siguientes operaciones de la API:

- Para asociarla a un comportamiento de caché en una distribución existente, utilice UpdateDistribution.
- Para asociarlo con un comportamiento de caché en una nueva distribución, utilice CreateDistribution.

Para ambas operaciones de la API, proporcione el ARN de la configuración de registro de acceso en tiempo real del campo `RealtimeLogConfigArn`, dentro de un comportamiento de caché. Para obtener más información sobre los otros campos que especifique en estas llamadas a la API, consulte Referencia de toda la configuración de distribución y la documentación de referencia de la API para el SDK de AWS u otro cliente de la API.

Descripción de las configuraciones de registros de acceso en tiempo real

Para utilizar registros de acceso en tiempo real de CloudFront, se debe comenzar por crear una configuración de registro de acceso en tiempo real. La configuración de registro de acceso en tiempo real contiene información acerca de los campos de registro que desea recibir, la frecuencia de muestreo de las entradas de registro y el flujo de datos de Kinesis en el que desea entregar los registros.

En concreto, una configuración de registro de acceso en tiempo real contiene los siguientes valores de configuración:

Contenido

- Nombre
- Frecuencia de muestreo
- Campos
- Punto de conexión (Kinesis Data Streams)
- rol de IAM

Nombre

Un nombre para identificar la configuración de registro de acceso en tiempo real.

Frecuencia de muestreo

La frecuencia de muestreo es un número entero entre 1 y 100 (inclusive) que determina el porcentaje de solicitudes de espectador que se envían a Kinesis Data Streams como entradas de registro de acceso en tiempo real. Para incluir todas las solicitudes de espectador en los registros en tiempo real, especifique 100 para la frecuencia de muestreo. Es posible que elija una frecuencia de muestreo más baja para reducir los costos mientras recibe un ejemplo representativo de datos de solicitudes en los registros de acceso en tiempo real.

Campos

Una lista de campos que se incluyen en cada entrada de registro de acceso en tiempo real. Cada registro de log puede contener hasta 40 campos y puede optar por recibir todos los campos disponibles, o solo los campos necesarios para monitorear y analizar el rendimiento.

La lista siguiente contiene el nombre de cada campo y una descripción de la información de ese campo. Los campos se muestran en el orden en que aparecen en las entradas de registros que se entregan a Kinesis Data Streams.

Los campos 46-63 son datos comunes de cliente multimedia (CMCD) que los clientes de reproductores multimedia pueden enviar a las CDN con cada solicitud. Puede utilizar estos datos para comprender cada solicitud, como el tipo de medio (audio o vídeo), la velocidad de reproducción y la duración del streaming. Estos campos solo aparecen en los registros de acceso en tiempo real si se envían a CloudFront.

1. **`timestamp`**

   La fecha y la hora a las que el servidor de borde ha terminado de responder a la solicitud.

2. **`c-ip`**

   La dirección IP del espectador que ha realizado la solicitud, por ejemplo, `192.0.2.183` o `2001:0db8:85a3::8a2e:0370:7334`. Si el lector ha utilizado un proxy HTTP o un equilibrador de carga para enviar la solicitud, el valor de este campo es la dirección IP del proxy o del balanceador de carga. Consulte también el campo `x-forwarded-for`.

3. **`s-ip`**

   La dirección IP del servidor de CloudFront que atendió la solicitud, por ejemplo, `192.0.2.183` o `2001:0db8:85a3::8a2e:0370:7334`.

4. **`time-to-first-byte`**

   El número de segundos entre la recepción de la solicitud y la escritura del primer byte de la respuesta, medido en el servidor.

5. **`sc-status`**

   El código de estado HTTP de la respuesta del servidor (por ejemplo, `200`).

6. **`sc-bytes`**

   El número total de bytes que el servidor ha enviado al lector en respuesta a la solicitud, incluidos los encabezados. Para conexiones WebSocket y gRPC, se trata del número total de bytes enviados desde el servidor al cliente a través de la conexión.

7. **`cs-method`**

   El método de solicitud HTTP recibido del lector.

8. **`cs-protocol`**

   El protocolo de la solicitud del lector (`http`, `https`, `grpcs`, `ws` o `wss`).

9. **`cs-host`**

   El valor que el lector ha incluido en el encabezado `Host` de la solicitud. Si utiliza el nombre de dominio CloudFront en las URL de los objetos (como d111111abcdef8.cloudfront.net), este campo contiene ese nombre de dominio. Si utiliza nombres de dominio alternativos (CNAME) en las URL de los objetos (como www.example.com), este campo contiene el nombre de dominio alternativo.

10. **`cs-uri-stem`**

   La dirección URL completa de la solicitud, incluida la cadena de consulta (si existe), pero sin el nombre de dominio. Por ejemplo, `/images/cat.jpg?mobile=true`.

   > **Note**
   >
   > En los registros estándar, el valor de `cs-uri-stem` no incluye la cadena de consulta.

11. **`cs-bytes`**

   El número total de bytes de datos que el lector ha incluido en la solicitud, incluidos los encabezados. Para conexiones WebSocket y gRPC, se trata del número total de bytes enviados desde el cliente al servidor en la conexión.

12. **`x-edge-location`**

   La ubicación de borde que atendió la solicitud. Cada ubicación periférica se identifica mediante un código de tres letras y un número asignado arbitrariamente (por ejemplo, DFW3). El código de tres letras normalmente se corresponde con el código del aeropuerto de la Asociación de Transporte Aéreo Internacional (IATA) más cercano a la ubicación geográfica de la ubicación periférica. Estas abreviaturas pueden cambiar en el futuro.

13. **`x-edge-request-id`**

   Una cadena opaca que identifica una solicitud de forma única. CloudFront también envía esta cadena en el encabezado de respuesta `x-amz-cf-id`.

14. **`x-host-header`**

   El nombre de dominio de la distribución de CloudFront (por ejemplo, d111111abcdef8.cloudfront.net).

15. **`time-taken`**

    El número de segundos (hasta la milésima de segundo, por ejemplo, 0,082) desde que el servidor recibe la solicitud del lector hasta que el servidor escribe el último byte de la respuesta en la cola de salida, según se mide en el servidor. Desde el punto de vista del lector, el tiempo total para obtener la respuesta completa será superior a este valor a causa de la latencia de la red y el almacenamiento en búfer de TCP.

16. **`cs-protocol-version`**

    La versión de HTTP que el espectador especificó en la solicitud. Entre los valores posibles se incluyen `HTTP/0.9`, `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0` y `HTTP/3.0`.

17. **`c-ip-version`**

    La versión IP de la solicitud (IPv4 o IPv6).

18. **`cs-user-agent`**

    El valor del encabezado `User-Agent` de la solicitud. El encabezado `User-Agent` identifica el origen de la solicitud, como el tipo de dispositivo y el navegador que enviaron la solicitud o, si la solicitud provino de un motor de búsqueda, de cuál.

19. **`cs-referer`**

    El valor del encabezado `Referer` de la solicitud. Este es el nombre del dominio que ha originado la solicitud. Entre los remitentes principales se incluyen motores de búsqueda, otros sitios web que enlazan directamente con sus objetos y su propio sitio web.

20. **`cs-cookie`**

    El encabezado `Cookie` de la solicitud, incluidos los pares nombre-valor y los atributos asociados.

    > **Note**
    >
    > Este campo se trunca en 800 bytes.

21. **`cs-uri-query`**

    La parte de la cadena de consulta de la URL, de haberla.

22. **`x-edge-response-result-type`**

Cómo el servidor ha clasificado la respuesta antes de devolver la respuesta al lector. Consulte también el campo `x-edge-result-type`. Entre los valores posibles se incluyen:

- `Hit`: el servidor ofreció el objeto al lector desde la caché.
- `RefreshHit`: el servidor encontró el objeto en la caché pero el objeto había vencido, por lo que el servidor se puso en contacto con el origen para comprobar que la caché tenía la versión más reciente del objeto.
- `Miss`: un objeto en la caché no ha podido satisfacer la solicitud, así que el servidor ha reenviado la solicitud al servidor de origen y ha devuelto el resultado al lector.
- `LimitExceeded`: se ha denegado la solicitud porque se superó una cuota (antes denominada límite) de CloudFront.
- `CapacityExceeded`: el servidor ha devuelto un error 503 porque no disponía de capacidad suficiente en el momento de la solicitud para prestar servicio al objeto.
- `Error`: normalmente, esto significa que la solicitud ha dado lugar a un error de cliente (el valor del campo `sc-status` está en el intervalo `4xx`) o un error de servidor (el valor del campo `sc-status` está en el intervalo `5xx`).

  Si el valor del campo `x-edge-result-type` es `Error` y el valor de este campo no es `Error`, el cliente se ha desconectado antes de finalizar la descarga.
- `Redirect`: el servidor ha redirigido al lector de HTTP a HTTPS de acuerdo con la configuración de distribución.
- `LambdaExecutionError`: la función de Lambda@Edge asociada con la distribución no se ha completado debido a una asociación incorrecta, al tiempo de espera de una función, a un problema de dependencia de AWS o a otro problema de disponibilidad general.

23 **`x-forwarded-for`**

Si el lector ha utilizado un proxy HTTP o un equilibrador de carga para enviar la solicitud, el valor del campo `c-ip` es la dirección IP del proxy o del balanceador de carga. En ese caso, este campo es la dirección IP del espectador que originó la solicitud. Este campo puede contener varias direcciones IP separadas por comas. Cada dirección IP puede ser una dirección IPv4 (por ejemplo, `192.0.2.183`) o una dirección IPv6 (por ejemplo, `2001:0db8:85a3::8a2e:0370:7334`).

24 **`ssl-protocol`**

Cuando la solicitud ha utilizado HTTPS, este campo contiene el protocolo SSL/TLS que el lector y el servidor han negociado para transmitir la solicitud y la respuesta. Para obtener una lista de

valores posibles, consulte los protocolos SSL/TLS compatibles en Protocolos y cifrados admitidos entre lectores y CloudFront.

25 **`ssl-cipher`**

Cuando la solicitud ha utilizado HTTPS, este campo contiene el cifrado SSL/TLS que el lector y el servidor han negociado para cifrar la solicitud y la respuesta. Para obtener una lista de valores posibles, consulte los cifrados SSL/TLS compatibles en Protocolos y cifrados admitidos entre lectores y CloudFront.

26 **`x-edge-result-type`**

Cómo el servidor ha clasificado la respuesta después de que el último byte abandonara el servidor. En algunos casos, el tipo de resultado puede cambiar entre el momento en que el servidor está listo para enviar la respuesta y el momento en que termina el envío de la respuesta. Consulte también el campo `x-edge-response-result-type`.

Por ejemplo, en el streaming de HTTP, se supone que el servidor encuentra un segmento de la secuencia en la caché. En esta situación, el valor de este campo sería normalmente `Hit`. Sin embargo, si el lector cierra la conexión antes de que el servidor haya entregado todo el segmento, el tipo de resultado final (y el valor de este campo) es `Error`.

Las conexiones WebSocket y gRPC tendrán un valor de `Miss` para este campo porque el contenido no se puede almacenar en caché y se entrega directamente al origen.

Entre los valores posibles se incluyen:

- `Hit`: el servidor ofreció el objeto al lector desde la caché.
- `RefreshHit`: el servidor encontró el objeto en la caché pero el objeto había vencido, por lo que el servidor se puso en contacto con el origen para comprobar que la caché tenía la versión más reciente del objeto.
- `Miss`: un objeto en la caché no ha podido satisfacer la solicitud, así que el servidor la ha reenviado al origen y ha devuelto el resultado al lector.
- `LimitExceeded`: se ha denegado la solicitud porque se superó una cuota (antes denominada límite) de CloudFront.
- `CapacityExceeded`: el servidor ha devuelto un código de estado HTTP 503 porque no disponía de capacidad suficiente en el momento de la solicitud para prestar servicio al objeto.
- `Error`: normalmente, esto significa que la solicitud ha dado lugar a un error de cliente (el valor del campo `sc-status` está en el intervalo `4xx`) o un error de servidor (el valor del campo

`sc-status` está en el intervalo `5xx`). Si el valor del campo `sc-status` es `200` o si el valor de este campo es `Error` y el valor del campo `x-edge-response-result-type` no es `Error`, significa que la solicitud HTTP se ha realizado correctamente pero el cliente se ha desconectado antes de recibir todos los bytes.

- `Redirect`: el servidor ha redirigido al lector de HTTP a HTTPS de acuerdo con la configuración de distribución.
- `LambdaExecutionError`: la función de Lambda@Edge asociada con la distribución no se ha completado debido a una asociación incorrecta, al tiempo de espera de una función, a un problema de dependencia de AWS o a otro problema de disponibilidad general.

27. **`fle-encrypted-fields`**

    El número de campos de cifrado en el nivel de campo que el servidor ha cifrado y reenviado al origen. Los servidores de CloudFront transmiten la solicitud procesada al origen a medida que cifran los datos, por lo que este campo puede tener un valor incluso si el valor de `fle-status` es un error.

28. **`fle-status`**

    Cuando se configura el cifrado en el nivel de campo para una distribución, este campo contiene un código que indica si el cuerpo de la solicitud se ha procesado correctamente. Cuando el servidor procesa correctamente el cuerpo de la solicitud, cifra los valores de los campos especificados y reenvía la solicitud al origen, el valor de este campo es `Processed`. El valor de `x-edge-result-type` todavía puede indicar un error del lado del cliente o del lado del servidor en este caso.

    Los valores posibles para este campo son:

    - `ForwardedByContentType`: el servidor ha reenviado la solicitud al origen sin analizar ni cifrar porque no se ha configurado ningún tipo de contenido.
    - `ForwardedByQueryArgs`: el servidor ha reenviado la solicitud al origen sin analizar ni cifrar porque la solicitud contiene un argumento de consulta que no estaba en la configuración de cifrado en el nivel de campo.
    - `ForwardedDueToNoProfile`: el servidor ha reenviado la solicitud al origen sin analizar ni cifrar porque no se ha especificado ningún perfil en la configuración de cifrado en el nivel de campo.
    - `MalformedContentTypeClientError`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque el valor del encabezado `Content-Type` estaba en un formato no válido.

- `MalformedInputClientError`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque el cuerpo de la solicitud estaba en un formato no válido.
- `MalformedQueryArgsClientError`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque un argumento de consulta estaba vacío o tenía un formato no válido.
- `RejectedByContentType`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque no se ha especificado ningún tipo de contenido en la configuración de cifrado en el nivel de campo.
- `RejectedByQueryArgs`: el servidor ha rechazado la solicitud y ha devuelto un código de estado HTTP 400 al lector porque no se ha especificado ningún argumento de consulta en la configuración de cifrado en el nivel de campo.
- `ServerError`: el servidor de origen ha devuelto un error.

Si la solicitud supera una cuota de cifrado en el nivel de campo (anteriormente denominada límite), este campo contiene uno de los siguientes códigos de error y el servidor devuelve el código de estado HTTP 400 al lector. Para obtener una lista de las cuotas actuales del cifrado en el nivel de campo, consulte Cuotas de cifrado en el nivel de campo.

- `FieldLengthLimitClientError`: un campo que se ha configurado como cifrado ha superado la longitud máxima permitida.
- `FieldNumberLimitClientError`: una solicitud que la distribución ha configurado para cifrar contiene un número de campos mayor del permitido.
- `RequestLengthLimitClientError`: la longitud del cuerpo de la solicitud ha superado el máximo permitido cuando se ha configurado el cifrado en el nivel de campo.

29 **`sc-content-type`**

El valor del encabezado HTTP `Content-Type` de la respuesta.

30 **`sc-content-len`**

El valor del encabezado HTTP `Content-Length` de la respuesta.

31 **`sc-range-start`**

Cuando la respuesta contiene el encabezado HTTP `Content-Range`, este campo contiene el valor inicial del intervalo.

32 **`sc-range-end`**

Cuando la respuesta contiene el encabezado HTTP `Content-Range`, este campo contiene el valor final del intervalo.

33 **`c-port`**

El número de puerto de la solicitud desde el espectador.

34 **`x-edge-detailed-result-type`**

Este campo contiene el mismo valor que el campo `x-edge-result-type`, excepto en los siguientes casos:

- Cuando el objeto se ha servido al lector desde la capa de Origin Shield, este campo contiene `OriginShieldHit`.
- Cuando el objeto no estaba en la memoria caché de CloudFront y la respuesta se generó mediante una función Lambda@Edge de solicitud de origen, este campo contiene `MissGeneratedResponse`.
- Cuando el valor del campo `x-edge-result-type` es `Error`, este campo contiene uno de los siguientes valores con más información sobre el error:
  - `AbortedOrigin`: el servidor ha encontrado un problema con el origen.
  - `ClientCommError`: la respuesta al lector se ha interrumpido debido a un problema de comunicación entre el servidor y el lector.
  - `ClientGeoBlocked`: la distribución está configurada para rechazar solicitudes desde la ubicación geográfica del lector.
  - `ClientHungUpRequest`: el espectador se ha detenido prematuramente mientras enviaba la solicitud.
  - `Error`: se ha producido un error cuyo tipo de error no se ajusta a ninguna de las otras categorías. Este tipo de error puede producirse cuando el servidor envía una respuesta de error desde la caché.
  - `InvalidRequest`: el servidor ha recibido una solicitud no válida desde el lector.
  - `InvalidRequestBlocked`: el acceso al recurso solicitado está bloqueado.
  - `InvalidRequestCertificate`: la distribución no coincide con el certificado SSL/TLS para el que se ha establecido la conexión HTTPS.
  - `InvalidRequestHeader`: la solicitud contenía un encabezado no válido.

- `InvalidRequestMethod`: la distribución no está configurada para gestionar el método de solicitud HTTP que se ha utilizado. Esto puede suceder cuando la distribución solo admite solicitudes que se pueden almacenar en caché.
- `OriginCommError`: se agotó el tiempo de espera de la solicitud al conectarse a un origen o al leer datos de un origen.
- `OriginConnectError`: el servidor no ha podido conectarse al origen.
- `OriginContentRangeLengthError`: el encabezado `Content-Length` de la respuesta del origen no coincide con la longitud del encabezado `Content-Range`.
- `OriginDnsError`: el servidor no ha podido resolver el nombre de dominio del origen.
- `OriginError`: el origen ha devuelto una respuesta incorrecta.
- `OriginHeaderTooBigError`: un encabezado devuelto por el origen es demasiado grande para que el servidor de borde lo procese.
- `OriginInvalidResponseError`: el origen ha devuelto una respuesta no válida.
- `OriginReadError`: el servidor no ha podido leer desde el origen.
- `OriginWriteError`: el servidor no ha podido escribir en el origen.
- `OriginZeroSizeObjectError`: un objeto de tamaño cero enviado desde el origen ha provocado un error.
- `SlowReaderOriginError`: el espectador ha sido al leer el mensaje que ha provocado el error de origen.

35. **`c-country`**

    Un código de país que representa la ubicación geográfica del lector, según lo determinado por la dirección IP del lector. Para obtener una lista de códigos de países, consulte ISO 3166-1 alpha-2.

36. **`cs-accept-encoding`**

    El valor del encabezado `Accept-Encoding` de la solicitud del lector.

37. **`cs-accept`**

    El valor del encabezado `Accept` de la solicitud del lector.

38. **`cache-behavior-path-pattern`**

    El patrón de ruta que identifica el comportamiento de caché que coincidió con la solicitud del lector.

39. **`cs-headers`**

Los encabezados HTTP (nombres y valores) en la solicitud del lector.

> **Note**
>
> Este campo se trunca en 800 bytes.

40. **`cs-header-names`**

    Los nombres de los encabezados HTTP (no los valores) en la solicitud del lector.

    > **Note**
    >
    > Este campo se trunca en 800 bytes.

41. **`cs-headers-count`**

    El número de encabezados HTTP en la solicitud del lector.

42. **`primary-distribution-id`**

    Cuando la implementación continua está habilitada, este ID identifica qué distribución es la principal en la distribución actual.

43. **`primary-distribution-dns-name`**

    Cuando la implementación continua está habilitada, este valor muestra el nombre de dominio principal que está relacionado con la distribución de CloudFront actual (por ejemplo, d111111abcdef8.cloudfront.net).

44. **`origin-fbl`**

    La cantidad de segundos de latencia del primer byte entre CloudFront y el origen.

45. **`origin-lbl`**

    La cantidad de segundos de latencia del último byte entre CloudFront y el origen.

46. **`asn`**

    El número de sistema autónomo (ASN) del espectador.

47.

> **Campos de CMCD en los registros de acceso en tiempo real**
>
> Para obtener más información sobre estos campos, consulte el documento CTA Specification Web Application Video Ecosystem - Common Media Client Data CTA-5004.

48. **`cmcd-encoded-bitrate`**

    La velocidad de bits codificada del objeto de audio o vídeo solicitado.

49. **`cmcd-buffer-length`**

    La longitud del búfer del objeto multimedia solicitado.

50. **`cmcd-buffer-starvation`**

    Indica si el búfer se ha agotado en algún momento entre la solicitud anterior y la solicitud de objeto. Esto puede provocar que el reproductor se encuentre en un estado de repetición de almacenamiento en búfer, lo que puede detener la reproducción de vídeo o audio.

51. **`cmcd-content-id`**

    Una cadena única que identifica el contenido actual.

52. **`cmcd-object-duration`**

    La duración de la reproducción del objeto solicitado (en milisegundos).

53. **`cmcd-deadline`**

    El plazo a partir de la hora de solicitud en que debe estar disponible la primera muestra de este objeto, de forma que se evite un estado de búfer insuficiente u otros problemas de reproducción.

54. **`cmcd-measured-throughput`**

    El rendimiento entre el cliente y el servidor, medido por el cliente.

55. **`cmcd-next-object-request`**

    La ruta relativa del siguiente objeto solicitado.

56. **`cmcd-next-range-request`**

    Si la siguiente solicitud es de objeto parcial, esta cadena indica el intervalo de bytes que debe solicitarse.

57. **`cmcd-object-type`**

El tipo de medio del objeto actual que se está solicitando.

58. **`cmcd-playback-rate`**

1 si es en tiempo real, 2 si es a doble velocidad, 0 si no se está reproduciendo.

59. **`cmcd-requested-maximum-throughput`**

El rendimiento máximo solicitado que el cliente considera suficiente para la entrega de recursos.

60. **`cmcd-streaming-format`**

El formato de streaming que define la solicitud actual.

61. **`cmcd-session-id`**

Un GUID que identifica la sesión de reproducción actual.

62. **`cmcd-stream-type`**

Token que identifica la disponibilidad de los segmentos. `v` = todos los segmentos están disponibles. `l` = los segmentos van estando disponibles con el tiempo.

63. **`cmcd-startup`**

La clave se incluye sin valor si el objeto se necesita de forma urgente durante el inicio, la búsqueda o la recuperación tras un evento de vaciado del búfer.

64. **`cmcd-top-bitrate`**

La representación con la tasa de bits más alta que el cliente puede reproducir.

65. **`cmcd-version`**

La versión de esta especificación utilizada para interpretar los nombres y valores de clave definidos. Si se omite esta clave, el cliente y el servidor deben interpretar los valores tal como los define la versión 1.

66. **`r-host`**

Este campo se envía para las solicitudes de origen e indica el dominio del servidor de origen utilizado para entregar el objeto. En caso de errores, puede usar este campo para buscar el último origen que se ha intentado, por ejemplo: `cd8jhdejh6a.mediapackagev2.us-east-1.amazonaws.com`.

67. **`sr-reason`**

Este campo proporciona el motivo por el que se seleccionó el origen. Está vacío cuando se realiza una solicitud al origen principal.

Si se produce una conmutación por error del origen, el campo contendrá el código de error HTTP que provocó la conmutación por error, como `Failover:403` o `Failover:502`. En caso de conmutación por error del origen, si la solicitud que se ha reintentado también falla y no ha configurado páginas de error personalizadas, `r-status` indica la respuesta del segundo origen. Sin embargo, si ha configurado páginas de error personalizadas junto con la conmutación por error del origen, contendrá la respuesta del segundo origen si la solicitud falló y, en su lugar, se devolvió una página de error personalizada.

Si no se produce ninguna conmutación por error del origen, pero se selecciona el origen mediante la resiliencia basada en la calidad multimedia (MQAR), se registrará como `MediaQuality`. Para obtener más información, consulte Resiliencia basada en la calidad multimedia.

68. **`x-edge-mqcs`**

Este campo indica la puntuación de confianza de la calidad multimedia (MQCS) (rango: 0-100) de los segmentos multimedia que CloudFront recuperó en los encabezados de respuesta de los CMSD de MediaPackage v2. Este campo está disponible para las solicitudes que coincidan con un comportamiento de caché que tenga un grupo de origen activado para MQAR. CloudFront registra este campo para los segmentos multimedia que también se entregan desde su caché, además de las solicitudes de origen. Para obtener más información, consulte Resiliencia basada en la calidad multimedia.

69. **`distribution-tenant-id`**

El ID del inquilino de la distribución.

70. **`connection-id`**

Un identificador único para la conexión TLS.

Debe habilitar los mTLS para las distribuciones antes de poder obtener información para este campo. Para obtener más información, consulte Autenticación TLS mutua con CloudFront (mTLS de espectador).

Punto de conexión (Kinesis Data Streams)

El punto de conexión contiene información sobre Kinesis Data Streams al que desea enviar registros en tiempo real. Se proporciona el nombre de recurso de Amazon (ARN) de la secuencia de datos.

Para obtener más información acerca de la creación de Kinesis Data Streams, consulte los siguientes temas en la Guía para desarrolladores de Amazon Kinesis Data Streams.

- Creación y administración de flujos
- Realización de operaciones básicas de Kinesis Data Streams con la AWS CLI
- Creación de un flujo (utiliza AWS SDK para Java)

Cuando crea una secuencia de datos, debe especificar el número de particiones. Utilice la siguiente información que le ayudará a estimar el número de particiones que necesita.

Para calcular el número de particiones para la secuencia de datos de Kinesis

1. Calcule (o estime) la cantidad de solicitudes por segundo que la distribución de CloudFront recibe.

   Puede utilizar los informes de uso de CloudFront (en la consola de CloudFront) y las métricas de CloudFront (en las consolas CloudFront y Amazon CloudWatch) que le ayudarán a calcular las solicitudes por segundo.
2. Determine el tamaño normal de una única entrada de registro de acceso en tiempo real.

   En general, un único registro de log es de unos 500 bytes. Un registro grande que incluye todos los campos suele pesar aproximadamente 1KB.

   Si no está seguro de cuál es el tamaño de su registro, puede habilitar los registros en tiempo real con una frecuencia de muestro baja (por ejemplo, 1 %) y luego calcular el promedio de tamaño de registro a través de los datos de supervisión en Kinesis Data Streams (total de bytes entrantes dividido por el número total de registros).
3. En la página de precios de Amazon Kinesis Data Streams, en Calculadora de precios de AWS, elija Crear el presupuesto personalizado ahora.

   - En la calculadora, introduzca el número de solicitudes (registros) por segundo.
   - Introduzca el tamaño medio de registro de un único registro.
   - Elija Mostrar cálculos.

La calculadora de precios le muestra el número de particiones que necesita y el costo estimado.

rol de IAM

El rol de AWS Identity and Access Management (IAM) que concede permiso de CloudFront para entregar registros de acceso en tiempo real al flujo de datos de Kinesis Data Stream.

Cuando se crea una configuración de registro de acceso en tiempo real con la consola de CloudFront, se puede elegir Crear un nuevo rol de servicio para permitir a la consola crear el rol de IAM automáticamente.

Cuando se crea una configuración de registro de acceso en tiempo real con AWS CloudFormation o la API de CloudFront (AWS CLI o SDK), uno mismo debe crear el rol de IAM y proporcionar el ARN del rol. Para crear el rol de IAM usted mismo, utilice las siguientes políticas.

Política de confianza del rol de IAM

Para utilizar la siguiente política de confianza de roles de IAM, sustituya *111122223333* por el número de Cuenta de AWS. El elemento `Condition` de esta política ayuda a prevenir el problema del suplente confuso porque CloudFront solo puede asumir este rol en nombre de una distribución de la Cuenta de AWS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                }
            }
        }
    ]
```

```
}
```

Política de permisos del rol de IAM para una secuencia de datos no cifrada

Para utilizar la siguiente política, reemplace *arn:aws:kinesis:us-east-2:123456789012:stream/StreamName* por el ARN de su Kinesis Data Streams.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStreamSummary",
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-east-2:123456789012:stream/StreamName"
            ]
        }
    ]
}
```

Política de permisos del rol de IAM para una secuencia de datos cifrada

Para utilizar la siguiente política, reemplace *arn:aws:kines:us-east-2:123456789012:Stream/StreamName* por el ARN de su Kinesis Data Streams y *arn:aws:kms:us-east- 2:123456789012:key/e58a3d0b-fe4f-4047-a495-ae03cc73d486* por el ARN de su AWS KMS key.

JSON

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

```
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStreamSummary",
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-east-2:123456789012:stream/StreamName"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/e58a3d0b-fe4f-4047-a495-
ae03cc73d486"
            ]
        }
    ]
}
```

Creación de un consumidor de Kinesis Data Streams

Para leer y analizar los registros de acceso en tiempo real, se crea o utiliza un consumidor de Kinesis Data Streams. Cuando se crea un consumidor para registros en tiempo real de CloudFront, es importante saber que los campos de cada entrada de registro de acceso en tiempo real siempre se envían en el mismo orden, como se muestra en la sección Campos. Asegúrese de crear su consumidor para acomodar este pedido fijo.

Por ejemplo, considere una configuración de registro de acceso en tiempo real que incluya solo estos tres campos: `time-to-first-byte`, `sc-status` y `c-country`. En este escenario, el último campo, `c-country`, siempre es el campo número 3 en cada registro de log. Sin embargo, si posteriormente agrega campos a la configuración de registro de acceso en tiempo real, la ubicación de cada campo en un registro puede cambiar.

Por ejemplo, si agrega los campos `sc-bytes` y `time-taken` a la configuración de registro de acceso en tiempo real, estos campos se insertan en cada entrada de registro según el orden mostrado en la sección Campos. El orden resultante de los cinco campos es `time-to-first-byte`, `sc-status`, `sc-bytes`, `time-taken` y `c-country`. El campo `c-country` era originalmente el campo número 3, pero ahora es el campo número 5. Asegúrese de que la aplicación de consumidor puede gestionar campos que cambian de posición en una entrada de registro, en caso de que agregue campos a su configuración de registro de acceso en tiempo real.

Resolución de problemas de registros de acceso en tiempo real

Después de crear una configuración de registro de acceso en tiempo real, es posible que encuentre que no se envían registros (o no todos los registros) a Kinesis Data Streams. En este caso, primero debe comprobar que la distribución de CloudFront recibe solicitudes de lector. Si es así, puede comprobar la siguiente configuración para continuar la solución de problemas.

Permisos de roles de IAM

Para enviar entradas de registros de acceso en tiempo real al flujo de datos de Kinesis, CloudFront utiliza el rol de IAM de la configuración de registro de acceso en tiempo real. Asegúrese de que la política de confianza de roles y la política de permisos de roles coinciden con las políticas mostradas en rol de IAM.

Limitación controlada de Kinesis Data Streams

Si CloudFront escribe entradas de registros de acceso en tiempo real en el flujo de datos de Kinesis más rápido de lo que el flujo puede manejar, es posible que Kinesis Data Streams limite las solicitudes de CloudFront. En este caso, puede aumentar el número de particiones en la secuencia de datos de Kinesis. Cada partición puede admitir escrituras de hasta 1000 registros por segundo, hasta un máximo de escritura de datos de 1 MB por segundo.

Registros de funciones perimetrales

Puede utilizar registros de Amazon CloudWatch para obtener registros de las funciones periféricas de Lambda@Edge y CloudFront Functions. Puede acceder a los registros mediante la consola de CloudWatch o la API de CloudWatch Logs.

> **Important**
>
> Recomendamos utilizar los registros de acceso para comprender la naturaleza de las solicitudes hechas a su contenido y no como una relación exhaustiva de todas las solicitudes.

CloudFront envía registros de funciones perimetrales en la medida en que sea posible. La entrada de registro de una solicitud determinada puede entregarse mucho después de la solicitud se haya procesado realmente y, en casos contados, es probable que una entrada de registro no se entregue en absoluto. Cuando se omite una entrada de registro de los registros de funciones perimetrales, la cantidad de entradas de los registros de funciones perimetrales no coincidirá con el uso que aparece en los informes de facturación y de uso de AWS.

Temas

- Registros de Lambda@Edge
- Registros de CloudFront Functions

Registros de Lambda@Edge

Lambda@Edge envía automáticamente registros de funciones a CloudWatch Logs, donde crea flujos de registro en las Regiones de AWS donde se invocan las funciones. Al crear o modificar una función en AWS Lambda, puede utilizar el nombre predeterminado del grupo de registro de CloudWatch o personalizarlo.

- El nombre predeterminado del grupo de registro es `/aws/lambda/<FunctionName>` donde `<FunctionName>` es el nombre que especificó al crear la función. Al enviar registros a CloudWatch, Lambda@Edge agregará automáticamente el prefijo `us-east-1` al nombre de la función, de modo que el nombre del grupo de registro sea `/aws/lambda/us-east-1.<FunctionName>`. Este prefijo corresponde a la Región de AWS donde se creó la función. Este prefijo sigue formando parte del nombre del grupo de registro, incluso en otras regiones en las que se invoque la función.
- Si especifica un nombre de grupo de registro personalizado, como `/MyLogGroup`, Lambda@Edge no agregará el prefijo de región. El nombre del grupo de registros permanece igual en todas las demás regiones en las que se invoca la función.

> **Note**
>
> Si crea un grupo de registro personalizado y especifica el mismo nombre que el predeterminado `/aws/lambda/<FunctionName>`, Lambda@Edge agrega el prefijo `us-east-1` al nombre de la función.

Además de personalizar el nombre del grupo de registros, las funciones de Lambda @Edge admiten los formatos de registro JSON y de texto sin formato, y el filtrado a nivel de registro. Para obtener más información, consulte Configuración de controles de registro avanzados para la función de Lambda en la Guía para desarrolladores de AWS Lambda.

> **Note**
>
> Lambda@Edge limita los registros en función del volumen de solicitudes y el tamaño de los registros.

Debe revisar los archivos de registro de CloudWatch en la región correcta de para ver sus archivos de registro de la función Lambda@Edge. Para ver las regiones donde la función de Lambda@Edge se está ejecutando, consulte los gráficos de métricas para la función en la consola de CloudFront. Las métricas se muestran para cada región de . En la misma página, puede elegir una región y, a continuación, consultar los archivos de registro para dicha región para investigar problemas.

Para obtener más información acerca cómo utilizar CloudWatch Logs con las funciones de Lambda@Edge, consulte los temas siguientes:

- Para empezar, puede usar los gráficos proporcionada en la sección Monitoring (Monitoreo) de la consola de CloudFront, consulte the section called “Supervisión de métricas de CloudFront con Amazon CloudWatch”.
- Para obtener información acerca de los permisos necesarios para enviar datos a CloudWatch Logs, consulte the section called “Configuración de permisos y roles de IAM”.
- Para obtener información sobre cómo agregar el registro a una función Lambda@Edge, consulte Registro de funciones AWS Lambda en Node.js o Registro de funciones AWS Lambda en Python en la Guía para desarrolladores de AWS Lambda.
- Para obtener información acerca de las cuotas de CloudWatch Logs (anteriormente conocidas como límites), consulte Cuotas de CloudWatch Logs en la Guía del usuario de Amazon CloudWatch Logs.

Registros de CloudFront Functions

Si el código de una función de CloudFront contiene instrucciones `console.log()`, CloudFront Functions envía automáticamente estas líneas de registro a CloudWatch Logs. Si no hay instrucciones `console.log()`, no se envía nada a CloudWatch Logs.

CloudFront Functions siempre crea flujos de registro en la región EE. UU. Este (Norte de Virginia) (`us-east-1`), independientemente de la ubicación de borde que ejecuta la función. El nombre del flujo de registro tiene el formato `YYYY/M/D/`*`UUID`*.

El nombre del grupo de registro utiliza el siguiente formato:

- Para CloudFront Functions por comportamiento de la caché, el formato es `/aws/cloudfront/function/`*`<FunctionName>`*
- Para CloudFront Functions por distribución (funciones de conexión), el formato es `/aws/cloudfront/connection-function/`*`<FunctionName>`*

`<FunctionName>` es el nombre que le dio a la función cuando la creó.

Example Solicitudes de espectadores

A continuación, se muestra un mensaje de registro de ejemplo enviado a CloudWatch Logs. Cada línea comienza con un ID que identifica de forma única una solicitud de CloudFront. El mensaje comienza con una línea `START` que incluye el ID de distribución de CloudFront y termina con una línea `END`. Entre las líneas `START` y `END`, se encuentran las líneas de registro que las instrucciones `console.log()` crearon en la función.

```
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== START DistributionID:
 E3E5D42GADAXZZ
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== Example function log output
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== END
```

Example Solicitudes de conexión

A continuación, se muestra un mensaje de registro de ejemplo enviado a CloudWatch Logs. Cada línea comienza con un ID que identifica de forma única una solicitud de CloudFront. El mensaje comienza con una línea `START` que incluye el ID de distribución de CloudFront y termina con una línea `END`. Entre las líneas `START` y `END`, se encuentran las líneas de registro que las instrucciones `console.log()` crearon en la función.

```
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== START DistributionID:
 E3E5D42GADA123
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== 1.2.3.4
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== END
```

> **Note**
>
> CloudFront Functions envía registros a CloudWatch solo para las funciones de la etapa `LIVE` que se ejecutan en respuesta a solicitudes y respuestas de producción. Al probar una función, CloudFront no envía ningún registro a CloudWatch. La salida de prueba contiene información sobre errores, uso de cómputo y registros de funciones (instrucciones `console.log()`), pero esta información no se envía a CloudWatch.

CloudFront Functions utiliza un rol vinculado a servicios de AWS Identity and Access Management (IAM) para enviar registros a CloudWatch Logs en su cuenta. Un rol vinculado a servicios es un rol de IAM que está vinculado directamente a un Servicio de AWS. El servicio predefine los roles vinculados a servicios, que incluyen todos los permisos que el servicio requiere para llamar a otros Servicios de AWS para usted. CloudFront Functions usa el rol vinculado a servicios AWSServiceRoleForCloudFrontLogger. Para obtener más información sobre este rol, consulte the section called “Roles vinculados a servicios para Lambda@Edge” (Lambda@Edge utiliza el mismo rol vinculado a servicios).

Cuando una función produce un error de validación o de ejecución, la información se registra en los registros estándar y en los registros en tiempo real. Para obtener información específica sobre el error, consulte los campos `x-edge-result-type`, `x-edge-response-result-type` y `x-edge-detailed-result-type`.

Registro de llamadas a la API de Amazon CloudFront con AWS CloudTrail

CloudFront se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un Servicio de AWS. CloudTrail captura como eventos todas las llamadas a la API de CloudFront. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de CloudFront, así como las llamadas de código realizadas a las operaciones de API de CloudFront. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a CloudFront, la dirección IP desde la que se realizó, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.

- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activado en la Cuenta de AWS cuando usted crea la cuenta y tiene acceso automático al Historial de eventos de CloudTrail. El Historial de eventos de CloudTrail proporciona un registro visible e inmutable, que se puede buscar y descargar, de los últimos 90 días de eventos de gestión registrados en una Región de AWS. Para obtener más información, consulte Trabajar con el historial de eventos de CloudTrail en la Guía del usuario de AWS CloudTrail. No se cobran cargos de CloudTrail por ver el Historial de eventos.

Para mantener un registro permanente de los eventos en su Cuenta de AWS más allá de los 90 días, cree un registro de seguimiento o un almacén de datos de eventos de CloudTrail Lake.

Registros de seguimiento de CloudTrail

Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. Todos los registros de seguimiento que cree con la Consola de administración de AWS son de varias regiones. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un registro de seguimiento de varias regiones, ya que registra actividad en todas las Regiones de AWS de su cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail.

Puede crear un registro de seguimiento para enviar una copia de los eventos de administración en curso en su bucket de Amazon S3 sin costo alguno desde CloudTrail; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

Almacenes de datos de eventos de CloudTrail Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL sobre los eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato ORC de Apache. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos

avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información acerca de CloudTrail Lake, consulte Trabajar con AWS CloudTrail Lake en la Guía del usuario de AWS CloudTrail.

Los almacenes de datos de eventos de CloudTrail Lake y las consultas generan costos adicionales. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

> **Note**
>
> CloudFront es un servicio global. CloudTrail registra eventos para CloudFront en la región Este de EE. UU. (Norte de Virginia). Para obtener más información, consulte Eventos de servicios globales en la Guía del usuario de AWS CloudTrail.
> Si utiliza credenciales de seguridad temporales mediante AWS Security Token Service, las llamadas a puntos de conexión regionales, como `us-west-2`, se registran en CloudTrail en la región correspondiente.
> Para obtener más información sobre los puntos de conexión de CloudFront, consulte CloudFront endpoints and quotas en Referencia general de AWS.

Eventos de datos de CloudFront en CloudTrail

Los eventos de datos proporcionan información sobre las operaciones de recursos realizadas en un recurso (por ejemplo, leer o escribir en una distribución de CloudFront) o dentro de él. Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen. De forma predeterminada, CloudTrail no registra eventos de datos. El Historial de eventos de CloudTrail no registra los eventos de datos.

Se aplican cargos adicionales a los eventos de datos. Para obtener más información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

Puede registrar eventos de datos para los tipos de recursos de CloudFront mediante la consola de CloudTrail, la AWS CLI o las operaciones de la API de CloudTrail. Para obtener más información sobre cómo registrar los eventos de datos, consulte Registro de eventos de datos con la Consola de

administración de AWS y Registro de eventos de datos con la AWS Command Line Interface en la Guía del usuario de AWS CloudTrail.

En la siguiente tabla se muestra los tipos de recursos de CloudFront para los que puede registrar eventos de datos. La columna Tipo de evento de datos (consola) muestra el valor que se debe elegir en la lista de tipos de eventos de datos de la consola de CloudTrail. La columna resources.type value muestra el valor de `resources.type`, que especificaría al configurar los selectores de eventos avanzados mediante la AWS CLI o las API de CloudTrail. La columna API de datos registradas en CloudTrail muestra las llamadas a la API registradas en CloudTrail para el tipo de recurso.

Tipo de evento de datos (consola)	resources.type value	API de datos registradas en CloudTrail
CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`	• DeleteKeys • DescribeKeyValueStore • GetKey • ListKeys • PutKeys • UpdateKeys

Puede configurar selectores de eventos avanzados para filtrar según los campos `eventName`, `readOnly` y `resources.ARN` y así registrar solo los eventos que son importantes para usted. Para obtener más información acerca de estos campos, consulte AdvancedFieldSelector en la Referencia de la API de AWS CloudTrail.

Eventos de administración de CloudFront en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se realizan en los recursos de su Cuenta de AWS. Se denominan también operaciones del plano de control. CloudTrail registra los eventos de administración de forma predeterminada.

Amazon CloudFront registra todas las operaciones de plano de control de CloudFront como eventos de administración. Para obtener una lista de las operaciones de plano de control de Amazon CloudFront que CloudFront registra en CloudTrail, consulte la Referencia de la API de Amazon CloudFront.

Ejemplos de eventos de CloudFront

Un evento representa una única solicitud de cualquier origen e incluye información sobre la operación de la API solicitada, la fecha y la hora de la operación o los parámetros de la solicitud, entre otras cosas. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas a la API públicas, por lo que los eventos no aparecen en un orden específico.

Contenido

- Ejemplo: UpdateDistribution
- Ejemplo: UpdateKeys

Ejemplo: UpdateDistribution

En el ejemplo que sigue se muestra un evento de CloudTrail que ilustra la operación UpdateDistribution.

Para las llamadas a la API de CloudFront, `eventSource` es `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"
}
```

Ejemplo: UpdateKeys

En el ejemplo que sigue se muestra un evento de CloudTrail que ilustra la operación UpdateKeys.

Para las llamadas a la API de CloudFront KeyValueStore, `eventSource` es `edgekeyvaluestore.amazonaws.com` en vez de `cloudfront.amazonaws.com`.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:role-session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/role-session-name",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2023-11-01T23:41:14Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-01T23:41:28Z",
    "eventSource": "edgekeyvaluestore.amazonaws.com",
```

```
    "eventName": "UpdateKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.235.183.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/121.0.0.0 Safari/537.36,
    "requestParameters": {
        "kvsARN": "arn:aws:cloudfront::111122223333:key-value-store/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "ifMatch": "KV3O6B1CX531EBP",
        "deletes": [
            {"key": "key1"}
        ]
    },
    "responseElements": {
        "itemCount": 0,
        "totalSizeInBytes": 0,
        "eTag": "KVDC9VEVZ71ZGO"
    },
    "requestID": "5ccf104c-acce-4ea1-b7fc-73e33example",
    "eventID": "a0b1b5c7-906c-439d-9925-90293example",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::CloudFront::KeyValueStore",
            "ARN": "arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "111122223333.cloudfront-kvs.global.api.aws"
    }
}
```

Para obtener información sobre el contenido de los registros de CloudTrail, consulte Contenido de los registros de CloudTrail en la Guía del usuario de AWS CloudTrail.

Realización de un seguimiento de los cambios en la configuración con AWS Config

Para registrar y evaluar las configuraciones de los recursos de AWS, puede utilizar AWS Config, que le proporciona una vista detallada de la configuración de las distribuciones. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, por lo que puede revisar los cambios a lo largo del tiempo.

También puede usar AWS Config para registrar cambios de configuración de la distribución de CloudFront. Puede capturar cambios en los estados de distribución, clases de precios, orígenes, configuración de restricciones geográficas y configuraciones de Lambda@Edge.

> **Note**
>
> AWS Config no registra etiquetas clave-valor para las distribuciones en streaming de CloudFront.

Contenido

- Configurar AWS Config con CloudFront
- Consultar historial de configuración de CloudFront
- Evaluación de las configuraciones de CloudFront con reglas de AWS Config

Configurar AWS Config con CloudFront

Cuando se configura AWS Config, puede elegir registrar todos los recursos de AWS compatibles o registrar solo determinados recursos como, por ejemplo, solo los cambios de CloudFront. Para consultar una lista de los recursos compatibles con CloudFront, consulte la sección Amazon CloudFront del tema Tipos de recursos admitidos en la Guía para desarrolladores de AWS Config.

> **Notas**
>
> - Para realizar un seguimiento de los cambios de configuración en la distribución de CloudFront, debe iniciar sesión en la consola de CloudFront en la Región de AWS Este de EE. UU. (Norte de Virginia).

- El registro de los recursos con AWS Config puede demorar. AWS Config registra los recursos solo después de que los detecta.

Console

Configuración de AWS Config con CloudFront

1. Inicie sesión en la Consola de administración de AWS y abra la consola de AWS Config.
2. Seleccione Get Started Now.
3. En la página Settings (Configuración), en Resource types to record (Tipos de recursos que registrar), especifique los tipos de recursos de AWS que desea que AWS Config registre. Si desea registrar solo los cambios de CloudFront, elija Specific types (Tipos específicos) y, a continuación, en CloudFront, elija la distribución o distribución de streaming para la que desea realizar un seguimiento de los cambios.

   Para añadir o cambiar las distribuciones en las que realizar un seguimiento, elija Settings (Configuración) a la izquierda, después de completar su configuración inicial.
4. Especifique las opciones necesarias adicionales para AWS Config: configure una notificación, especifique una ubicación para la información de configuración y agregue reglas para evaluar tipos de recursos.

Para obtener más información, consulte Configuración de AWS Config mediante la consola en la Guía para desarrolladores de AWS Config.

AWS CLI

Para configurar AWS Config con CloudFront mediante la AWS CLI, consulte Setting up AWS Config with the AWS CLI en la Guía para desarrolladores de AWS Config.

AWS Config API

Para configurar AWS Config con CloudFront mediante la API de AWS Config, consulte la operación de la API StartConfigurationRecorder en la Referencia de la API de AWS Config.

Consultar historial de configuración de CloudFront

Después de que AWS Config comience a registrar los cambios de configuración de sus distribuciones, puede obtener el historial de configuración de cualquier distribución que haya configurado para CloudFront.

Puede ver los historiales de configuración de cualquiera de las siguientes formas.

Console

Para cada recurso registrado, puede ver una página de escala de tiempo que proporciona un historial con detalles de la configuración. Para ver esta página, elija el icono gris en la columna Config Timeline (Escala de tiempo de configuración) de la página Dedicated Hosts (Hosts dedicados).

Para obtener más información, consulte Visualización de los detalles de la configuración en la consola de AWS Config en la guía para desarrolladores de AWS Config.

AWS CLI

Para obtener una lista de todas las distribuciones, ejecute el comando list-discovered-resources como se muestra en el siguiente ejemplo.

```
aws configservice list-discovered-resources --resource-type
 AWS::CloudFront::Distribution
```

Para obtener los detalles de configuración de una distribución para un intervalo de tiempo específico, ejecute el comando get-resource-config-history.

Para obtener más información, consulte Ver detalles de configuración mediante la CLI en la guía para desarrolladores de AWS Config.

AWS Config API

Para obtener una lista de todas las distribuciones, utilice la operación de la API ListDiscoveredResources.

Para obtener los detalles de configuración de una distribución para un intervalo de tiempo específico, utilice la operación de la API GetResourceConfigHistory. Para obtener más información, consulte la Referencia de la API de AWS Config.

Evaluación de las configuraciones de CloudFront con reglas de AWS Config

Puede evaluar las configuraciones comparándolas con las configuraciones deseadas con las reglas de AWS Config. Por ejemplo, las reglas de AWS Config le ayudan a evaluar si los recursos de CloudFront cumplen con las prácticas recomendadas de seguridad habituales. Puede elegir reglas administradas, como la política de lector HTTPS, SNI habilitado, OAC habilitado, conmutación por error de origen habilitada, AWS WAF WebACL o las políticas de recursos de AWS Shield Advanced que se activarán cuando cambie la configuración.

Las reglas administradas pueden ejecutar evaluaciones periódicamente, con la frecuencia que usted elija. AWS Firewall Manager se basa en AWS Config para alertas y correcciones automáticas. Para obtener más información, consulte Evaluación de recursos con reglas de AWS Config y Lista de reglas administradas por AWS Config en la Guía para desarrolladores de AWS Config.

Seguridad en Amazon CloudFront

La seguridad en la nube de AWS es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y el usuario. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener información sobre los programas de conformidad que se aplican a Amazon CloudFront, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo puede aplicar el modelo de responsabilidad compartida cuando se utiliza CloudFront. En los siguientes temas se muestra cómo configurar CloudFront para satisfacer los objetivos de seguridad y conformidad. También obtendrá información sobre cómo utilizar otros servicios de AWS que lo ayudarán a supervisar y proteger los recursos de CloudFront.

Temas

- Protección de datos en Amazon CloudFront
- Identity and Access Management para Amazon CloudFront
- Registro y monitoreo en Amazon CloudFront
- Validación de conformidad para Amazon CloudFront
- Resiliencia de Amazon CloudFront
- Seguridad de la infraestructura en Amazon CloudFront

Protección de datos en Amazon CloudFront

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Amazon CloudFront. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulte Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye el momento en el que trabaje con CloudFront u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los AWS SDK. Cualquier dato que introduzca

en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Amazon CloudFront ofrece varias opciones que puede utilizar para ayudar a proteger el contenido que ofrece:

- Configure las conexiones HTTPS.
- Configure el cifrado de nivel de campo para proporcionar mayor seguridad a datos específicos durante el tránsito.
- Restrinja el acceso al contenido de manera que solo determinadas personas o personas de un área específica, puedan verlo.

En los siguientes temas, se explican las opciones con más detalle.

Temas

- Cifrado en tránsito
- Cifrado en reposo
- Restricción del acceso a contenido

Cifrado en tránsito

Para cifrar los datos durante el transporte, configure Amazon CloudFront para solicitar que los lectores utilicen HTTPS para solicitar los archivos, de modo que las conexiones se cifren cuando CloudFront se comunique con los lectores. También puede configurar CloudFront para utilizar HTTPS para obtener archivos del origen, de modo que las conexiones se cifran cuando CloudFront se comunica con el origen.

Para obtener más información, consulte Uso de HTTPS con CloudFront.

El cifrado en el nivel de campo añade una capa de seguridad adicional que, junto con HTTPS, le permite proteger datos específicos durante su procesamiento en el sistema de forma que solo determinadas aplicaciones puedan verlos. Al configurar el cifrado en el nivel de campo en CloudFront, puede cargar de manera segura información confidencial enviada por el usuario a los servidores web. La información confidencial proporcionada por los clientes se cifra en el borde

más cercano al usuario. Sigue cifrada en toda la pila de aplicaciones, lo que garantiza que solo las aplicaciones que necesitan los datos y disponen de las credenciales para descifrarlos, son capaces de hacerlo.

Para obtener más información, consulte Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial.

Los puntos de enlace de la API de CloudFront `cloudfront.amazonaws.com` y `cloudfront-fips.amazonaws.com` solo aceptan tráfico HTTPS. Esto significa que cuando envía y recibe información mediante la API de CloudFront, sus datos, incluidas las configuraciones de distribución, las políticas de caché y las de solicitud de origen, los grupos de claves y las claves públicas y el código de función en CloudFront Functions, siempre se cifran en tránsito. Además, todas las solicitudes enviadas a los puntos de enlace de la API de CloudFront se firman con credenciales de AWS y se registran en AWS CloudTrail.

El código de función y la configuración en CloudFront Functions siempre se cifran en tránsito cuando se copian en los puntos de presencia (POP) de la ubicación de borde y entre otras ubicaciones de almacenamiento que utiliza CloudFront.

Cifrado en reposo

El código de función y la configuración en CloudFront Functions siempre se almacenan en un formato cifrado en los POP de ubicación periférica y en otras ubicaciones de almacenamiento que utilizada CloudFront.

Restricción del acceso a contenido

Muchas empresas que distribuyen contenido a través de Internet desean restringir el acceso a documentos, información corporativa, transmisiones multimedia o contenido destinado a una selección de usuarios. Para ofrecer de forma segura este contenido mediante Amazon CloudFront, puede elegir una o varias de las opciones siguientes:

Utilice URL o cookies firmadas

Puede restringir el acceso a contenido que está destinado a usuarios determinados, por ejemplo, que hayan pagado una tarifa, ofreciendo este contenido privado a través de CloudFront mediante URL firmadas o cookies firmadas. Para obtener más información, consulte Distribución de contenido privado con URL firmadas y cookies firmadas.

Restringir el acceso al contenido en los buckets de Amazon S3

Si restringe el acceso al contenido utilizando, por ejemplo, URL o cookies firmadas de CloudFront, tampoco querrá que nadie consulte los archivos utilizando la URL directa para el archivo. En su lugar, deseará que solo puedan obtener acceso a los archivos utilizando la URL de CloudFront, para que las medidas de protección funcionen.

Si utiliza un bucket de Amazon S3 como origen para una distribución de CloudFront, puede configurar un control de acceso de origen (OAC) que permita restringir el acceso al bucket de S3. Para obtener más información, consulte the section called “Restricción del acceso a un origen de Amazon S3”.

Restringir el acceso al contenido proporcionado por un balanceador de carga de aplicaciones

Cuando utiliza CloudFront con un balanceador de carga de aplicaciones en Elastic Load Balancing como origen, puede configurar CloudFront para evitar que los usuarios accedan directamente al balanceador de carga de aplicaciones. Esto permite a los usuarios acceder al balanceador de carga de aplicaciones solo a través de CloudFront, lo que garantiza que obtenga los beneficios de utilizar CloudFront. Para obtener más información, consulte Restricción del acceso a Application Load Balancer.

Utilice ACL de web de AWS WAF

Puede utilizar AWS WAF, un servicio de firewall de aplicación web, para crear una lista de control de acceso web (ACL de web) para restringir el acceso al contenido. En función de las condiciones que especifique, como las direcciones IP de las que provienen las solicitudes o los valores de las cadenas de consulta, CloudFront responde a las solicitudes con el contenido solicitado o con un código de estado HTTP 403 (Prohibido). Para obtener más información, consulte Uso de protecciones de AWS WAF.

Restricción geográfica

Puede usar geo restriction (restricción geográfica), también conocida como geo blocking (bloqueo geográfico), para evitar que usuarios de ubicaciones geográficas específicas obtengan acceso a contenido que ofrece a través de una distribución de CloudFront. Existen varias opciones entre las que elegir al configurar restricciones geográficas. Para obtener más información, consulte Restricción de la distribución geográfica de su contenido.

Identity and Access Management para Amazon CloudFront

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de CloudFront. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas
- Cómo funciona Amazon CloudFront con IAM
- Ejemplos de políticas basadas en identidades para Amazon CloudFront
- AWSPolíticas administradas de para Amazon CloudFront
- Uso de roles vinculados a servicios para CloudFront
- Resolución de problemas de identidad y acceso de Amazon CloudFront

Público

La forma de utilizar AWS Identity and Access Management (IAM) varía en función del rol:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Resolución de problemas de identidad y acceso de Amazon CloudFront).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo funciona Amazon CloudFront con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en identidades para Amazon CloudFront).

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe autenticarse como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Se puede iniciar sesión como una identidad federada con las credenciales de un origen de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las

credenciales de Google/Facebook. Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Para el acceso mediante programación, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Usuario raíz de la Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario raíz de la Cuenta de AWS que tiene acceso completo a todos los Servicios de AWS y recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS con credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, proveedor de identidad web o Directory Service que accede a los Servicios de AWS mediante credenciales de un origen de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir que los usuarios humanos utilicen la federación con un proveedor de identidades para acceder a AWS con credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Se puede asumir un rol cambiando de un usuario a un rol de IAM (consola) o llamando a una operación de la API de la AWS CLI o AWS. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política define los permisos cuando se asocia a una identidad o un recurso. AWS evalúa estas políticas cuando una entidad principal realiza una solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se pueden utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer el máximo de permisos concedidos por los tipos de políticas más frecuentes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon CloudFront con IAM

Antes de utilizar IAM para administrar el acceso a CloudFront, obtenga información sobre qué características de IAM se pueden utilizar con CloudFront.

Características de IAM que puede utilizar con Amazon CloudFront

Característica de IAM	Compatibilidad de CloudFront
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	No
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una perspectiva general sobre cómo funcionan CloudFront y otros servicios de AWS con la mayoría de características de IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades para CloudFront

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para CloudFront

Para ver ejemplos de políticas basadas en identidad de CloudFront, consulte Ejemplos de políticas basadas en identidades para Amazon CloudFront.

Políticas basadas en recursos dentro de CloudFront

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de política para CloudFront

Compatibilidad con las acciones de políticas: sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de acciones de CloudFront, consulte Acciones definidas por Amazon CloudFront en la Referencia de autorizaciones de servicio.

Las acciones de políticas de CloudFront utilizan el siguiente prefijo antes de la acción:

```
cloudfront
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas basadas en identidad de CloudFront, consulte Ejemplos de políticas basadas en identidades para Amazon CloudFront.

Recursos de política para CloudFront

Compatibilidad con los recursos de políticas: sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Para las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de tipos de recursos de CloudFront y los ARN, consulte Recursos definidos por Amazon CloudFront en la Referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon CloudFront.

Para ver ejemplos de políticas basadas en identidad de CloudFront, consulte Ejemplos de políticas basadas en identidades para Amazon CloudFront.

Claves de condición de política para CloudFront

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de CloudFront, consulte Claves de condición para Amazon CloudFront en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon CloudFront.

Para ver ejemplos de políticas basadas en identidad de CloudFront, consulte Ejemplos de políticas basadas en identidades para Amazon CloudFront.

ACL en CloudFront

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con CloudFront

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede asociar etiquetas a entidades de IAM y recursos de AWS y, a continuación, diseñar políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

CloudFront admite ABAC para los recursos de CloudFront que admiten etiquetas, como distribuciones, inquilinos o almacenes de confianza.

Uso de credenciales temporales con CloudFront

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a corto plazo a los recursos de AWS y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Sesiones de acceso directo para CloudFront

Compatibilidad con las sesiones de acceso directo (FAS): no

Las sesiones de acceso directo (FAS) utilizan los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Roles de servicio para CloudFront

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Es posible que cambiar los permisos de un rol de servicio interrumpa la funcionalidad de CloudFront. Edite los roles de servicio solo cuando CloudFront proporcione orientación para hacerlo.

Roles vinculados a servicios para CloudFront

Compatible con roles vinculados al servicio: sí

Un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

CloudFront usa roles vinculados a servicios para realizar acciones por usted. Para obtener más información sobre cómo crear o administrar roles vinculados a servicios de CloudFront, consulte Uso de roles vinculados a servicios para CloudFront. Para obtener información sobre cómo crear o administrar roles vinculados a servicios de Lambda@Edge, consulte Roles vinculados a servicios para Lambda@Edge.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades para Amazon CloudFront

De forma predeterminada, los usuarios y roles no tienen permiso para crear o modificar recursos de CloudFront. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por CloudFront, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición de Amazon CloudFront en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Cómo permitir a los usuarios consultar sus propios permisos
- Permisos para acceder a CloudFront mediante programación
- Permisos necesarios para utilizar la consola de CloudFront
- Ejemplos de políticas administradas por el cliente

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, eliminar o acceder a los recursos de CloudFront de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience a utilizar las políticas administradas de AWS y avance hacia permisos de privilegios mínimos. Para empezar a conceder permisos a los usuarios y cargas de trabajo, utilice las políticas administradas de AWS que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado como, por ejemplo, CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas

nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesite usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para obtener una mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de 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": "*"
        }
    ]
}
```

Permisos para acceder a CloudFront mediante programación

A continuación se muestra una política de permisos. El `Sid` o ID de instrucción es opcional.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "AllowAllCloudFrontPermissions",
         "Effect": "Allow",
         "Action": ["cloudfront:*"],
         "Resource": "*"
      }
   ]
}
```

La política concede permisos para realizar todas las operaciones de CloudFront, que son suficientes para acceder a CloudFront mediante programación. Si utiliza la consola para acceder a CloudFront, consulte Permisos necesarios para utilizar la consola de CloudFront.

Para consultar una lista de acciones y el ARN a especificar para conceder o denegar permisos para ejecutar cada acción, consulte Acciones, recursos y claves de condición para Amazon CloudFront en la Referencia de autorización de servicios.

Permisos necesarios para utilizar la consola de CloudFront

Para conceder acceso completo a la consola de CloudFront, debe conceder los permisos en la siguiente política de permisos:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:*",
            "cloudwatch:DescribeAlarms",
            "cloudwatch:PutMetricAlarm",
            "cloudwatch:GetMetricStatistics",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets",
            "s3:PutBucketPolicy"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Aquí se explica por qué son necesarios los permisos:

`acm:ListCertificates`

Al crear y actualizar distribuciones desde la consola de CloudFront, si desea configurar CloudFront para que requiera HTTPS entre el lector y CloudFront o entre CloudFront y el origen, este permiso le permite ver una lista de certificados de ACM.

Este permiso no es necesario si no utiliza la consola de CloudFront.

`cloudfront:*`

Le permite realizar todas las acciones de CloudFront.

`cloudwatch:DescribeAlarms` y **`cloudwatch:PutMetricAlarm`**

Le permite crear y ver alarmas de CloudWatch en la consola de CloudFront. Consulte también `sns:ListSubscriptionsByTopic` y `sns:ListTopics`.

Estos permisos no son necesarios si no utiliza la consola de CloudFront.

`cloudwatch:GetMetricStatistics`

Permite a CloudFront representar las métricas de CloudWatch en la consola de CloudFront.

Este permiso no es necesario si no utiliza la consola de CloudFront.

`elasticloadbalancing:DescribeLoadBalancers`

Al crear y actualizar las distribuciones, le permite ver una lista de balanceadores de carga Elastic Load Balancing en la lista de orígenes disponibles.

Este permiso no es necesario si no utiliza la consola de CloudFront.

`iam:ListServerCertificates`

Al crear y actualizar distribuciones desde la consola de CloudFront, si desea configurar CloudFront para que requiera HTTPS entre el lector y CloudFront o entre CloudFront y el origen, este permiso le permite ver una lista de certificados del almacén de certificados de IAM.

Este permiso no es necesario si no utiliza la consola de CloudFront.

`s3:ListAllMyBuckets`

Al crear y actualizar las distribuciones, le permite realizar las siguientes operaciones:

- Ver una lista de buckets de S3 en la lista de orígenes disponibles
- Ver una lista de buckets de S3 en los que se puede ahorrar registros de acceso

Este permiso no es necesario si no utiliza la consola de CloudFront.

`S3:PutBucketPolicy`

Al crear o actualizar distribuciones que restringen el acceso a buckets de S3, le permite a un usuario actualizar la política del bucket para conceder acceso a la identidad de acceso de origen de CloudFront. Para obtener más información, consulte the section called “Uso de una identidad de acceso de origen (heredado, no recomendado)”.

Este permiso no es necesario si no utiliza la consola de CloudFront.

`sns:ListSubscriptionsByTopic` y **`sns:ListTopics`**

Cuando crea alarmas de CloudWatch en la consola de CloudFront, le permite elegir un tema de SNS para las notificaciones.

Estos permisos no son necesarios si no utiliza la consola de CloudFront.

`waf:GetWebACL` y **`waf:ListWebACLs`**

Le permite ver una lista de ACL web de AWS WAF en la consola de CloudFront.

Estos permisos no son necesarios si no utiliza la consola de CloudFront.

Acciones de solo permiso para la consola de CloudFront

Puede realizar las siguientes acciones de CloudFront en la página Paquete de promociones en seguridad de CloudFront. Las acciones de la API no están diseñadas para que puedan invocarse desde el código y no están incluidas en la AWS CLI o los SDK de AWS.

Action	Descripción
`CreateSavingsPlan`	Concede permiso para crear un nuevo plan de ahorro.
`GetSavingsPlan`	Concede permiso para obtener un plan de ahorro.
`ListRateCards`	Concede permiso para enumerar las tarjetas de tarifas de CloudFront para la cuenta.
`ListSavingsPlans`	Concede permiso para enumerar los planes de ahorro de la cuenta.

Action	Descripción
`ListUsages`	Concede permiso para mostrar el uso de CloudFront.
`UpdateSavingsPlan`	Concede permiso para actualizar un plan de ahorro.

Notas

- Para obtener más información sobre los Savings Plans de CloudFront, consulte la sección Paquete de promociones en seguridad de CloudFront de las Preguntas frecuentes sobre Amazon CloudFront.
- Si crea un plan de ahorro para CloudFront y luego quiere eliminarlo más adelante, póngase en contacto con AWS Support.

Ejemplos de políticas administradas por el cliente

Puede crear sus propias políticas de IAM personalizadas con el fin de conceder permisos para realizar acciones de la API de CloudFront. Puede asociar estas políticas personalizadas a los usuarios o grupos de IAM que requieran los permisos especificados. Estas políticas funcionan cuando se utiliza la API de CloudFront, los SDK de AWS o la AWS CLI. A continuación se muestran algunos ejemplos de permisos en algunos casos de uso comunes. Para obtener más información acerca de la política que concede acceso total a los usuarios de CloudFront, consulte Permisos necesarios para utilizar la consola de CloudFront.

Ejemplos

- Ejemplo 1: permitir acceso de lectura a todas las distribuciones
- Ejemplo 2: Creación, actualización y eliminación de distribuciones
- Ejemplo 3: Permitir crear y publicar invalidaciones
- Ejemplo 4: Permitir la creación de una distribución

Ejemplo 1: permitir acceso de lectura a todas las distribuciones

La siguiente política de permisos concede al usuario permisos para ver todas las distribuciones en la consola de CloudFront:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Ejemplo 2: Creación, actualización y eliminación de distribuciones

La siguiente política de permisos permite a los usuarios crear, actualizar y eliminar distribuciones a través de la consola de CloudFront:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:CreateDistribution",
            "cloudfront:DeleteDistribution",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:UpdateDistribution",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets",
            "s3:PutBucketPolicy"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

`cloudfront:ListCloudFrontOriginAccessIdentities` permite a los usuarios conceder permiso automáticamente a una identidad de acceso de origen existente para obtener acceso a objetos en un bucket de Amazon S3. Si desea que los usuarios puedan crear identidades de acceso de origen, también es necesario conceder el permiso `cloudfront:CreateCloudFrontOriginAccessIdentity`.

Ejemplo 3: Permitir crear y publicar invalidaciones

La siguiente política de permisos concede a los usuarios permiso para crear y enumerar invalidaciones. Incluye acceso de lectura a las distribuciones de CloudFront, ya que para crear y visualizar invalidaciones, primero se muestra la configuración de una distribución:

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:GetDistribution",
            "cloudfront:GetStreamingDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "cloudfront:CreateInvalidation",
            "cloudfront:GetInvalidation",
            "cloudfront:ListInvalidations",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Ejemplo 4: Permitir la creación de una distribución

La siguiente política de permisos concede al usuario permiso para ver todas las distribuciones en la consola de CloudFront. Para la acción `CreateDistribution`, especifique el carácter comodín (*) para `Resource` en lugar de un comodín para el ARN (`arn:aws:cloudfront::123456789012:distribution/*`) de distribución. Para obtener más información acerca del elemento `Resource`, consulte Elementos de política JSON de IAM: Resource en la Guía del usuario de IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "cloudfront:CreateDistribution",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "cloudfront:ListDistributions",
            "Resource": "*"
        }
    ]
}
```

AWSPolíticas administradas de para Amazon CloudFront

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas de IAM administradas por el cliente que proporcionen a los usuarios solo los permisos necesarios. Para comenzar rápidamente, puede utilizar nuestras políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más

información acerca de las políticas administradas de AWS, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas de AWS. No puede cambiar los permisos de las políticas administradas de AWS. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada de AWS cuando se lanza una característica nueva o cuando se ofrecen nuevos permisos. Los servicios no eliminan permisos de una política administrada de AWS, de modo que las actualizaciones de las políticas no modificarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada de AWS ReadOnlyAccess proporciona acceso de solo lectura a todos los servicios y los recursos de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Temas

- AWSPolítica administrada de : CloudFrontReadOnlyAccess
- AWSPolítica administrada de : CloudFrontFullAccess
- AWSPolítica administrada de : AWSCloudFrontLogger
- AWSPolítica administrada de : AWSLambdaReplicator
- Política administrada de AWS: AWSCloudFrontVPCOriginServiceRolePolicy
- Actualizaciones de CloudFront en políticas administradas de AWS

AWSPolítica administrada de : CloudFrontReadOnlyAccess

Puede adjuntar la política CloudFrontReadOnlyAccess a las identidades de IAM. Esta política concede permisos de solo lectura para los recursos de CloudFront. También concede permisos de solo lectura para otros recursos de servicios de AWS que estén relacionados con CloudFront y sean visibles en la consola de CloudFront.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `cloudfront:Describe*`: permite a las entidades principales obtener información acerca de los metadatos de los recursos de CloudFront.
- `cloudfront:Get*`: permite a las entidades principales obtener información y configuraciones detalladas para los recursos de CloudFront.
- `cloudfront:List*`: permite a las entidades principales obtener listas de recursos de CloudFront.
- `cloudfront-keyvaluestore:Describe*`: permite a las entidades principales obtener información sobre el almacén de clave-valor.
- `cloudfront-keyvaluestore:Get*`: permite a las entidades principales obtener información y configuraciones detalladas para el almacén de clave-valor.
- `cloudfront-keyvaluestore:List*`: permite a las entidades principales obtener listas de los almacenes de clave-valor.
- `acm:DescribeCertificate`: permite a las entidades principales obtener detalles sobre un certificado de ACM.
- `acm:ListCertificates`: permite a las entidades principales obtener una lista de certificados de ACM.
- `iam:ListServerCertificates`: permite a las entidades principales obtener una lista de certificados de servidor almacenados en IAM.
- `route53:List*`: permite a las entidades principales obtener listas de recursos de Route 53.
- `waf:ListWebACLs` – permite a las entidades principales obtener una lista de ACL web de AWS WAF.
- `waf:GetWebACL` – permite a las entidades principales obtener información detallada acerca de ACL web de AWS WAF.
- `wafv2:ListWebACLs` – permite a las entidades principales obtener una lista de ACL web de AWS WAF.
- `wafv2:GetWebACL` – permite a las entidades principales obtener información detallada acerca de ACL web de AWS WAF.
- `pricingplanmanager:GetSubscription`: permite a las entidades principales acceso de solo lectura para obtener detalles sobre las suscripciones al plan de precios.
- `pricingplanmanager:ListSubscriptions`: permite a las entidades principales acceso de solo lectura para mostrar las suscripciones al plan de precios.

- `ec2:DescribeIpamPools`: permite a las entidades principales obtener información detallada acerca de los grupos de IPAM.
- `ec2:GetIpamPoolCidrs`: permite a las entidades principales obtener los CIDR aprovisionados en un grupo de IPAM.

Para ver los permisos de esta política, consulte CloudFrontReadOnlyAccess en la Referencia de políticas administrada de AWS.

AWSPolítica administrada de : CloudFrontFullAccess

Puede adjuntar la política CloudFrontFullAccess a las identidades de IAM. Esta política concede permisos administrativos para los recursos de CloudFront. También concede permisos de solo lectura para otros recursos de servicios de AWS que estén relacionados con CloudFront y sean visibles en la consola de CloudFront.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `s3:ListAllMyBuckets`: permite a las entidades principales obtener una lista de todos los buckets de Amazon S3.
- `acm:DescribeCertificate`: permite a las entidades principales obtener detalles sobre un certificado de ACM.
- `acm:ListCertificates`: permite a las entidades principales obtener una lista de certificados de ACM.
- `acm:RequestCertificate`: permite a las entidades principales solicitar certificados administrados de ACM.
- `cloudfront:*`: permite a las entidades principales realizar todas las acciones en todos los recursos de CloudFront.
- `cloudfront-keyvaluestore:*`: permite a las entidades principales realizar todas las acciones en el almacén de clave-valor.
- `iam:ListServerCertificates`: permite a las entidades principales obtener una lista de certificados de servidor almacenados en IAM.
- `waf:ListWebACLs` – permite a las entidades principales obtener una lista de ACL web de AWS WAF.

- `waf:GetWebACL` – permite a las entidades principales obtener información detallada acerca de ACL web de AWS WAF.
- `waf:CreateWebACLs`: permite a las entidades principales crear una ACL web en AWS WAF.
- `wafv2:ListWebACLs` – permite a las entidades principales obtener una lista de ACL web de AWS WAF.
- `wafv2:GetWebACL` – permite a las entidades principales obtener información detallada acerca de ACL web de AWS WAF.
- `kinesis:ListStreams`: permite a las entidades principales obtener una lista de los flujos de Amazon Kinesis.
- `elasticloadbalancing:DescribeLoadBalancers`: permite a las entidades principales obtener información detallada sobre los equilibradores de carga de Elastic Load Balancing.
- `kinesis:DescribeStream`: permite a las entidades principales obtener información detallada acerca de un flujo de Kinesis.
- `iam:ListRoles`: permite a las entidades principales obtener una lista de roles de IAM.
- `pricingplanmanager:AssociateResourcesToSubscription`: permite a las entidades principales asociar recursos a una suscripción. Esto permite cubrir los recursos con el plan de precios de la suscripción.
- `pricingplanmanager:CancelSubscription`: permite a las entidades principales cancelar una suscripción existente.
- `pricingplanmanager:CancelSubscriptionChange`: permite a las entidades principales cancelar un cambio pendiente en una suscripción existente, como una actualización de plan, antes de que se aplique el cambio.
- `pricingplanmanager:CreateSubscription`: permite a las entidades principales crear una suscripción a un plan de precios.
- `pricingplanmanager:DisassociateResourcesFromSubscription`: permite a las entidades principales eliminar la asociación entre los recursos y una suscripción existente.
- `pricingplanmanager:UpdateSubscription`: permite a las entidades principales modificar una suscripción existente, por ejemplo, cambiar el plan de precios.
- `pricingplanmanager:GetSubscription`: permite a las entidades principales acceso de solo lectura para obtener detalles sobre las suscripciones al plan de precios.
- `pricingplanmanager:ListSubscriptions`: permite a las entidades principales acceso de solo lectura para mostrar las suscripciones al plan de precios.

- `ec2:DescribeInstances`: permite a las entidades principales obtener información detallada sobre las instancias de Amazon EC2.
- `ec2:DescribeInternetGateways`: permite a las entidades principales obtener información detallada sobre las puertas de enlace de Internet de Amazon EC2.
- `ec2:DescribeIpamPools`: permite a las entidades principales obtener información detallada acerca de los grupos de IPAM.
- `ec2:GetIpamPoolCidrs`: permite a las entidades principales obtener los CIDR aprovisionados en un grupo de IPAM.

Para ver los permisos de esta política, consulte CloudFrontFullAccess en la Referencia de políticas administrada de AWS.

> **Important**
>
> Si desea que CloudFront cree y guarde registros de acceso, debe conceder permisos adicionales. Para obtener más información, consulte Permisos.

AWSPolítica administrada de : AWSCloudFrontLogger

No puede adjuntar la política AWSCloudFrontFullAccess a las identidades de IAM. Esta política va adjunta a un rol vinculado a servicio que permite a CloudFront realizar acciones en su nombre. Para obtener más información, consulte the section called “Roles vinculados a servicios para Lambda@Edge”.

Esta política permite a CloudFront insertar archivos de registro en Amazon CloudWatch. Para obtener más detalles acerca de los permisos incluidos en esta política, consulte the section called “Permisos de rol vinculado a servicio para el registrador de CloudFront”.

Para ver los permisos de esta política, consulte AWSCloudFrontLogger en la Referencia de políticas administradas de AWS.

AWSPolítica administrada de : AWSLambdaReplicator

No puede adjuntar la política AWSLambdaReplicator a las identidades de IAM. Esta política va adjunta a un rol vinculado a servicio que permite a CloudFront realizar acciones en su nombre. Para obtener más información, consulte the section called “Roles vinculados a servicios para Lambda@Edge”.

Esta política permite a CloudFront crear, eliminar y desactivar funciones en AWS Lambda para replicar las funciones Lambda@Edge a Regiones de AWS. Para obtener más detalles acerca de los permisos incluidos en esta política, consulte the section called “Permisos del rol vinculado a servicio para el replicador de Lambda”.

Para ver los permisos de esta política, consulte AWSLambdaReplicator en la Referencia de políticas administradas de AWS.

Política administrada de AWS: AWSCloudFrontVPCOriginServiceRolePolicy

No se puede asociar la política AWSCloudFrontVPCOriginServiceRolePolicy a las entidades de IAM. Esta política va adjunta a un rol vinculado a servicio que permite a CloudFront realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para CloudFront.

Esta política permite a CloudFront administrar las interfaces de red elásticas y los grupos de seguridad de EC2 en su nombre. Para obtener más detalles acerca de los permisos incluidos en esta política, consulte the section called “Permisos de rol vinculado al servicio para el registrador de Orígenes de la VPC de CloudFront”.

Para ver los permisos de esta política, consulte AWSCloudFrontVPCOriginServiceRolePolicy en la Referencia de políticas administradas de AWS.

Actualizaciones de CloudFront en políticas administradas de AWS

Vea los detalles de las actualizaciones de las políticas administradas de AWS para CloudFront desde que este servicio comenzó a hacer un seguimiento de los cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página Historial de revisión de CloudFront.

Cambio	Descripción	Fecha
CloudFrontReadOnlyAccess: actualización de una política actual	CloudFront ha agregado nuevos permisos para Amazon EC2. Los nuevos permisos permiten a las entidades principal es utilizar las acciones	24 de noviembre de 2025

Cambio	Descripción	Fecha
	`ec2:DescribeIpamPools` y `ec2:GetIpamPoolCidrs`.	
CloudFrontFullAccess: actualización de una política actual	CloudFront ha agregado nuevos permisos para Amazon EC2. Los nuevos permisos permiten a las entidades principales utilizar las acciones `ec2:DescribeIpamPools` y `ec2:GetIpamPoolCidrs`.	24 de noviembre de 2025
CloudFrontFullAccess: actualización de una política actual	CloudFront ha agregado un nuevo permiso para crear un recurso de ACL de AWS WAF y ha agregado permisos de creación, actualización, eliminación y lectura a AWS Pricing Plan Manager.	18 de noviembre de 2025
CloudFrontFullAccess: actualización de una política actual	CloudFront ha agregado un nuevo permiso para crear un recurso de ACL de AWS WAF y ha agregado permisos de creación, actualización, eliminación y lectura a AWS Pricing Plan Manager.	18 de noviembre de 2025
CloudFrontReadOnlyAccess: actualización de una política actual	CloudFront ha agregado nuevos permisos para el acceso de solo lectura a AWS Pricing Plan Manager.	18 de noviembre de 2025

Cambio	Descripción	Fecha
CloudFrontReadOnlyAccess: actualización de una política actual	CloudFront ha agregado nuevos permisos para el acceso de solo lectura a AWS Pricing Plan Manager.	18 de noviembre de 2025
CloudFrontReadOnlyAccess: actualización de una política actual	CloudFront agregó un nuevo permiso para ACM. El nuevo permiso permite a las entidades principales obtener detalles sobre un certificado de ACM.	28 de abril de 2025
CloudFrontFullAccess: actualización de una política actual	CloudFront ha agregado nuevos permisos para ACM. Los nuevos permisos permiten a las entidades principales obtener detalles sobre un certificado de ACM y solicitar un certificado administrado de ACM.	28 de abril de 2025
CloudFrontFullAccess: actualización de una política actual	CloudFront agregó nuevos permisos para Amazon EC2 y Elastic Load Balancing. Los nuevos permisos permiten a CloudFront obtener información detallada sobre los equilibradores de carga en Elastic Load Balancing y las instancias y puertas de enlace de Internet en Amazon EC2.	20 de noviembre de 2024

Cambio	Descripción	Fecha
AWSCloudFrontVPCOriginServiceRolePolicy: política nueva	CloudFront agregó una nueva política. Esta política permite a CloudFront administrar las interfaces de red elásticas y los grupos de seguridad de EC2 en su nombre.	20 de noviembre de 2024
CloudFrontReadOnlyAccess y CloudFrontFullAccess: actualización de dos políticas existentes	CloudFront ha agregado nuevos permisos para los almacenes de clave-valor. Los nuevos permisos permiten a los usuarios obtener información sobre los almacenes de clave-valor y tomar medidas al respecto.	19 de diciembre de 2023
CloudFrontReadOnlyAccess: actualización de una política existente	CloudFront incorporó un nuevo permiso para describir CloudFront Functions. Con este permiso, el usuario, el grupo o el rol puede leer información y metadatos sobre una función, pero no el código de la función.	8 de septiembre de 2021
CloudFront comenzó hacer un seguimiento de los cambios	CloudFront comenzó a hacer un seguimiento de los cambios de sus políticas administradas de AWS.	8 de septiembre de 2021

Uso de roles vinculados a servicios para CloudFront

Amazon CloudFront utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a CloudFront. Los roles vinculados a servicios están predefinidos por CloudFront e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a servicios simplifica la configuración de CloudFront porque ya no tendrá que agregar de forma manual los permisos necesarios. CloudFront define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo CloudFront puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de CloudFront, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestren Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculado al servicio para el registrador de Orígenes de la VPC de CloudFront

Orígenes de la VPC de CloudFront usa el rol vinculado a servicios denominado AWSServiceRoleForCloudFrontVPCOrigin: permite a CloudFront administrar los grupos de seguridad e interfaces de red elásticas de EC2 en su nombre.

El rol vinculado al servicio AWSServiceRoleForCloudFrontVPCOrigin depende de los siguientes servicios para asumir el rol:

- `vpcorigin.cloudfront.amazonaws.com`

La política de permisos del rol denominada AWSCloudFrontVPCOriginServiceRolePolicy permite que Orígenes de la VPC de CloudFront pueda realizar las siguientes acciones en los recursos especificados:

- Acción: `ec2:CreateNetworkInterface` en `arn:aws:ec2:*:*:network-interface/*`

- Acción: `ec2:CreateNetworkInterface` en `arn:aws:ec2:*:*:subnet/*` y `arn:aws:ec2:*:*:security-group/*`
- Acción: `ec2:CreateSecurityGroup` en `arn:aws:ec2:*:*:security-group/*`
- Acción: `ec2:CreateSecurityGroup` en `arn:aws:ec2:*:*:vpc/*`
- Acción: `ec2:ModifyNetworkInterfaceAttribute`, `ec2:DeleteNetworkInterface`, `ec2:DeleteSecurityGroup`, `ec2:AssignIpv6Addresses` y `ec2:UnassignIpv6Addresses` en `supported AWS resources that have the aws:ResourceTag/aws.cloudfront.vpcorigin tag enabled`
- Action: `ec2:DescribeNetworkInterfaces`, `ec2:DescribeSecurityGroups`, `ec2:DescribeInstances`, `ec2:DescribeInternetGateways`, `ec2:DescribeSubnets`, `ec2:DescribeRegions` y `ec2:DescribeAddresses` en `all AWS resources that the actions support`
- Acción: `ec2:CreateTags` en `arn:aws:ec2:*:*:security-group/*` y `arn:aws:ec2:*:*:network-interface/*`
- Acción: `elasticloadbalancing:DescribeLoadBalancers`, `elasticloadbalancing:DescribeListeners` y `elasticloadbalancing:DescribeTargetGroups` en `all AWS resources that the actions support`

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios de Orígenes de la VPC de CloudFront

No necesita crear manualmente un rol vinculado a servicios. Al crear un origen de la VPC en la Consola de administración de AWS, la AWS CLI o la API de AWS, Orígenes de la VPC de CloudFront crea el rol vinculado a servicios en su nombre.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un origen de la VPC, Orígenes de la VPC de CloudFront crea el rol vinculado a servicios en su nombre de nuevo.

Edición de un rol vinculado a servicios de Orígenes de la VPC de CloudFront

Orígenes de la VPC de CloudFront no le permite editar el rol vinculado a servicios AWSServiceRoleForCloudFrontVPCOrigin. Después de crear un rol vinculado al servicio, no podrá

cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios de Orígenes de la VPC de CloudFront

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio de CloudFront utiliza el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Orígenes de la VPC de CloudFront que utiliza AWSServiceRoleForCloudFrontVPCOrigin

- Elimine los recursos de origen de la VPC de su cuenta.
  - CloudFront puede tardar un tiempo en terminar de eliminar los recursos de su cuenta. Si no puede eliminar el rol vinculado a servicios de inmediato, espere e inténtelo de nuevo.

Para eliminar manualmente el rol vinculado al servicio mediante IAM

Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a un servicio de AWSServiceRoleForCloudFrontVPCOrigin. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para roles vinculados a servicios de Orígenes de la VPC de CloudFront

Orígenes de la VPC de CloudFront no permite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Puede usar el rol AWSServiceRoleForCloudFrontVPCOrigin en las siguientes regiones.

Nombre de la región	Identidad de la región	Compatibilidad en CloudFront
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	Sí
EE. UU Oeste (Norte de California)	us-west-1 (excepto AZ usw1-az2)	Sí
Oeste de EE. UU. (Oregón)	us-west-2	Sí
África (Ciudad del Cabo)	af-south-1	Sí
Asia-Pacífico (Hong Kong)	ap-east-1	Sí
Asia-Pacífico (Yakarta)	ap-southeast-3	Sí
Asia-Pacífico (Melbourne)	ap-southeast-4	Sí
Asia-Pacífico (Mumbai)	ap-south-1	Sí
Asia-Pacífico (Hyderabad)	ap-south-2	Sí
Asia-Pacífico (Osaka)	ap-northeast-3	Sí
Asia-Pacífico (Seúl)	ap-northeast-2	Sí
Asia-Pacífico (Singapur)	ap-southeast-1	Sí
Asia-Pacífico (Sídney)	ap-southeast-2	Sí
Asia-Pacífico (Tokio)	ap-northeast-1 (excepto AZ apne1-az3)	Sí
Canadá (centro)	ca-central-1 (excepto AZ cac1-az3)	Sí
Oeste de Canadá (Calgary)	ca-west-1	Sí
Europa (Fráncfort)	eu-central-1	Sí

Nombre de la región	Identidad de la región	Compatibilidad en CloudFront
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí
Europa (Milán)	eu-south-1	Sí
Europa (París)	eu-west-3	Sí
Europa (España)	eu-south-2	Sí
Europa (Estocolmo)	eu-north-1	Sí
Europa (Zúrich)	eu-central-2	Sí
Israel (Tel Aviv)	il-central-1	Sí
Medio Oriente (Baréin)	me-south-1	Sí
Medio Oriente (EAU)	me-central-1	Sí
América del Sur (São Paulo)	sa-east-1	Sí

Resolución de problemas de identidad y acceso de Amazon CloudFront

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que pueden surgir al trabajar con CloudFront e IAM.

Temas

- No tengo autorización para realizar una acción en CloudFront
- No estoy autorizado a realizar la operación iam:PassRole
- Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de CloudFront

No tengo autorización para realizar una acción en CloudFront

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `cloudfront:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `cloudfront:`*`GetWidget`*.

Si necesita ayuda, contacte con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar la operación iam:PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas se deben actualizar a fin de permitirle pasar un rol a CloudFront.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en CloudFront. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de CloudFront

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para

que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si CloudFront admite estas características, consulte Cómo funciona Amazon CloudFront con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra cuenta de Cuenta de AWS propia en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a sus recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Registro y monitoreo en Amazon CloudFront

El monitoreo es una parte importante del mantenimiento de la disponibilidad y el rendimiento de CloudFront y sus soluciones de AWS. Debe recopilar datos de monitoreo de todas las partes de su solución de AWS para que pueda depurar más fácilmente un error multipunto si se produce. AWS proporciona varias herramientas para monitorear sus recursos de CloudFront y responder a posibles incidentes:

Alarmas de Amazon CloudWatch

Las alarmas de Amazon CloudWatch le permiten ver una sola métrica durante el período de tiempo que especifique. Si la métrica supera un límite determinado, se envía una notificación a un tema de Amazon SNS o a una política de AWS Auto Scaling. Las alarmas de CloudWatch no invocan acciones cuando una métrica se encuentra en un estado determinado. En su lugar, el estado debe haber cambiado y debe mantenerse durante el número de periodos especificado.

Para obtener más información, consulte Supervisión de métricas de CloudFront con Amazon CloudWatch.

AWS CloudTrailRegistros de

CloudTrail proporciona un registro de las medidas de la API adoptadas por un usuario, un rol o un servicio de AWS en CloudFront. Mediante la información recopilada por CloudTrail, puede determinar la solicitud de la API que se realizó a CloudFront, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información, consulte Registro de llamadas a la API de Amazon CloudFront con AWS CloudTrail.

Registros estándar y registros de acceso en tiempo real de CloudFront

Los registros de CloudFront proporcionan registros detallados sobre las solicitudes que se realizan a una distribución. Los registros resultan útiles para muchas aplicaciones. Por ejemplo, la información del registro puede ser útil en auditorías de acceso y seguridad.

Para obtener más información, consulte Registros de acceso (registros estándar) y Creación y uso de configuraciones de registro de acceso en tiempo real.

Registros de funciones perimetrales

Los registros generados por funciones perimetrales, CloudFront Functions y Lambda@Edge, se envían directamente a registros de Amazon CloudWatch y CloudFront no los almacena en ningún lugar. CloudFront Functions utiliza un rol vinculado al servicio de AWS Identity and Access Management (IAM) para enviar registros generados por el cliente directamente a CloudWatch Logs en la cuenta.

Para obtener más información, consulte Registros de funciones perimetrales.

Informes de la consola de CloudFront

La consola de CloudFront incluye una serie de informes, incluido el informe de estadísticas de caché, el informe de objetos populares y el informe de remitentes principales. La mayoría de los informes de la consola de CloudFront se basan en los datos de los registros de acceso de CloudFront, que contienen información detallada sobre cada solicitud de usuario que CloudFront recibe. No obstante, no es necesario habilitar los registros de acceso para ver los informes.

Para obtener más información, consulte Visualización de informes de CloudFront en la consola.

Validación de conformidad para Amazon CloudFront

Auditores externos evalúan la seguridad y la conformidad de Amazon CloudFront en distintos programas de conformidad de AWS. Esto incluye SOC, PCI, HIPAA y otros.

Para obtener una lista de los servicios que AWS incluyen los programas de conformidad específicos, consulte los servicios AWS incluidos en cada programa de conformidad. Para obtener información general, consulte Programas de conformidad de AWS.

Se puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

La responsabilidad en torno a la conformidad al utilizar CloudFront está determinada por la confidencialidad de los datos, los objetivos de conformidad de la empresa y la legislación y normativa aplicables. AWS proporciona los siguientes recursos para ayudar con los requisitos de conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Arquitectura para seguridad y conformidad de HIPAA en AWS: en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con la ley HIPAA.

  El programa de conformidad con HIPAA de AWS incluye CloudFront (excepto la entrega de contenido a través de puntos de presencia incrustados de CloudFront) como un servicio válido de HIPAA. Si ha firmado un anexo para socios empresariales (BAA) con AWS, puede utilizar CloudFront (excepto la entrega de contenido a través de puntos de presencia incrustados de CloudFront) para entregar contenido que incluya información sanitaria protegida (PHI). Para obtener más información, consulte Conformidad con HIPAA.
- AWSRecursos de conformidad: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- AWS Config: este servicio de AWS evalúa en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y la normativa.
- AWS Security Hub CSPM: este servicio de AWS utiliza controles de seguridad para evaluar las configuraciones de los recursos y los estándares de seguridad para ayudarle a cumplir con varios marcos de conformidad. Para obtener más información sobre el uso del CSPM del centro de seguridad para evaluar los recursos de CloudFront, consulte controles de Amazon CloudFront en la Guía del usuario de AWS Security Hub CSPM.

Prácticas recomendadas de conformidad de CloudFront

En esta sección se ofrecen prácticas recomendadas y recomendaciones sobre conformidad cuando se utiliza Amazon CloudFront para servir contenido.

Si ejecuta cargas de trabajo conformes con HIPAA o PCI basadas en el Modelo de responsabilidad compartida de AWS, recomendamos que registre los datos de uso de CloudFront de los últimos 365 días para posibles auditorías futuras. Para registrar datos de uso, puede hacer lo siguiente:

- Habilitar registros de acceso de CloudFront Para obtener más información, consulte Registros de acceso (registros estándar).
- Capture las solicitudes que se envían a la API de CloudFront. Para obtener más información, consulte Registro de llamadas a la API de Amazon CloudFront con AWS CloudTrail.

Además, consulte lo siguiente para obtener más información acerca de cómo CloudFront cumple con los estándares PCI DSS y SOC.

La norma de seguridad de datos del sector de pagos con tarjeta (PCI DSS)

CloudFront (excepto la entrega de contenido a través de los puntos de presencia incrustados de CloudFront) admite el procesamiento, el almacenamiento y la transmisión de datos de tarjetas de crédito por parte de un comerciante o proveedor de servicios, y se ha validado como conforme con el Estándar de Seguridad de los Datos de la Industria de las Tarjetas de Pago (DSS PCI). Para obtener más información acerca de PCI DSS, incluido cómo solicitar una copia del Paquete de conformidad con PCI de AWS, consulte PCI DSS Nivel 1.

Como práctica recomendada de seguridad, le recomendamos que no almacene información de la tarjeta de crédito en las cachés perimetrales de CloudFront. Por ejemplo, puede configurar el origen para que incluya un encabezado `Cache-Control:no-cache="field-name"` en las respuestas que contengan información de la tarjeta de crédito, como por ejemplo, los últimos cuatro dígitos de un número de tarjeta de crédito y la información de contacto del titular de la tarjeta.

Controles del Sistema y Organizaciones (System and Organization Controls, SOC)

CloudFront (excepto la entrega de contenido a través de puntos de presencia incrustados de CloudFront) cumple con las medidas de Controles del Sistema y Organizaciones (System and Organization Control, SOC), incluidos SOC 1, SOC 2 y SOC 3. Los informes SOC son informes de análisis independientes de terceros que muestran cómo AWS logra los controles y objetivos clave

de conformidad. Estas auditorías garantizan que contamos con los mecanismos de seguridad y los procedimientos adecuados para protegernos frente a los riesgos que puedan afectar a la seguridad, la confidencialidad y la disponibilidad de los datos de clientes y negocios. Los resultados de estas auditorías de terceros están disponibles en el sitio web de conformidad de AWS SOC, donde los clientes pueden ver los informes publicados para obtener más información acerca de los controles que respaldan las operaciones y la conformidad de AWS.

Resiliencia de Amazon CloudFront

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Conmutación por error de CloudFront

Además de la compatibilidad con la infraestructura global de AWS, Amazon CloudFront ofrece una función de conmutación por error en el origen para ayudar a satisfacer sus necesidades de resiliencia de datos. CloudFront es un servicio global que proporciona su contenido a través de una red mundial de centros de datos denominada ubicaciones de borde o puntos de presencia (POP). Si el contenido aún no se ha almacenado en la caché en una ubicación de borde, CloudFront lo recupera de un origen que haya identificado como origen para la versión definitiva del contenido.

Puede mejorar la resiliencia y aumentar la disponibilidad para situaciones específicas configurando CloudFront con la conmutación por error en el origen. Para empezar, cree un grupo de orígenes en el que designe un origen principal para CloudFront además de un segundo origen. CloudFront cambia automáticamente al segundo origen cuando el origen principal devuelve respuestas de error de código de estado HTTP específicas. Para obtener más información, consulte Optimización de alta disponibilidad con conmutación por error de origen de CloudFront.

Seguridad de la infraestructura en Amazon CloudFront

Como se trata de un servicio administrado, Amazon CloudFront está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS siguiendo las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas de AWS para obtener acceso a CloudFront a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

CloudFront Functions utiliza una barrera de aislamiento muy segura entre cuentas de AWS, lo que garantiza que los entornos de los clientes estén seguros frente a ataques de canal lateral como Spectre y Meltdown. Functions no puede acceder a los datos que pertenecen a otros clientes ni modificarlos. Functions se ejecuta en un proceso dedicado de un solo subproceso en una CPU específica sin Hyper-Threading. En cualquier punto de presencia (POP) de ubicación de borde de CloudFront determinado, CloudFront Functions solo presta servicios a un cliente a la vez y todos los datos específicos de dicho cliente se borran entre ejecuciones de funciones.

Solución de problemas

Utilice esta sección para solucionar problemas comunes que puede encontrar al configurar Amazon CloudFront para distribuir el contenido.

En este tema se proporciona una guía detallada para identificar la causa principal de los problemas más comunes e instrucciones paso a paso para resolverlos.

Temas

- Solucionar problemas de distribuciones
- Solución de problemas de códigos de estado de respuesta a errores en CloudFront
- Pruebas de carga de CloudFront

Solucionar problemas de distribuciones

Utilice la información de este tema para diagnosticar y solucionar los errores de certificados, los problemas de acceso denegado u otros problemas comunes que puedan surgir al configurar un sitio web o una aplicación con distribuciones de Amazon CloudFront.

Temas

- CloudFront devuelve un error Access Denied
- CloudFront devuelve un error InvalidViewerCertificate al intentar agregar un nombre de dominio alternativo
- CloudFront devuelve un error de registro DNS mal configurado al intentar agregar un nuevo CNAME
- No puedo ver los archivos de mi distribución
- Mensaje de error: Certificate: <id-certificado> is being used by CloudFront

CloudFront devuelve un error Access Denied

Si utiliza un bucket de Amazon S3 como origen de su distribución de CloudFront, puede que aparezca un mensaje de error Access Denied (403) en los ejemplos siguientes.

Contenido

- Ha especificado un objeto que faltaba en el origen de Amazon S3
- A su origen de Amazon S3 le faltan permisos de IAM
- Está utilizando credenciales no válidas o no tiene permisos suficientes

Ha especificado un objeto que faltaba en el origen de Amazon S3

Compruebe que exista el objeto solicitado en su bucket. Los nombres de objetos distinguen entre mayúsculas y minúsculas. Si se introduce un nombre de objeto no válido, es posible que devuelva un código de error de acceso denegado.

Por ejemplo, si sigue el tutorial de CloudFront para crear una distribución básica, debe crear un bucket de Amazon S3 como origen y cargar un archivo `index.html` de ejemplo.

En su navegador web, si introduce `https://d111111abcdef8.cloudfront.net/INDEX.HTML` en lugar de `https://d111111abcdef8.cloudfront.net/index.html`, es posible que vea un mensaje similar porque el archivo `index.html` de la ruta URL distingue entre mayúsculas y minúsculas.

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>22Q367AHT7Y1ABCD</RequestId>
<HostId>
ABCDE/Vg+7PSNa/d/IfFQ8Fb92TGQ0KH0ZwG5iEKbc6+e06DdMS1ZW+ryB9GFRIVtS66rSSy6So=
</HostId>
</Error>
```

A su origen de Amazon S3 le faltan permisos de IAM

Compruebe que ha seleccionado el bucket de Amazon S3 correcto como nombre y dominio de origen. El origen (Amazon S3) debe contar con los permisos correctos.

Si no especifica los permisos correctos, un mensaje de `AccessDenied` puede aparecer para los espectadores.

Cuando distribuye contenido desde Amazon S3 y también utiliza el cifrado del servicio (SSE-KMS) de AWS Key Management Service (AWS KMS), hay permisos de IAM adicionales que debe especificar para la clave de KMS y el bucket de Amazon S3. Su distribución de CloudFront necesita estos permisos para usar la clave de KMS, que se usa para cifrar el bucket de Amazon S3 de origen.

Las configuraciones de la política del bucket de Amazon S3 permiten a la distribución de CloudFront recuperar los objetos cifrados para la entrega de contenido.

Verificación de los permisos del bucket de Amazon S3 y de la clave de KMS

1. Compruebe que la clave de KMS que utiliza es la misma clave que utiliza su bucket de Amazon S3 para el cifrado predeterminado. Para obtener más información, consulte Uso del cifrado del servidor con AWS KMS (SSE-KMS) en la Guía del usuario de Amazon Simple Storage Service.
2. Compruebe que los objetos del bucket estén cifrados con la misma clave de KMS. Puede seleccionar cualquier objeto del bucket de Amazon S3 y comprobar la configuración de cifrado del servidor para verificar el ARN de la clave de KMS.
3. Edite la política del bucket de Amazon S3 para conceder a CloudFront permiso para llamar a la operación de la API `GetObject` desde el bucket de Amazon S3. Para ver un ejemplo de política del bucket de Amazon S3 que utiliza el control de acceso de origen, consulte Concesión de permiso de CloudFront para acceder al bucket de S3.
4. Edite la política de claves de KMS para conceder a CloudFront permiso para realizar las acciones `Encrypt`, `Decrypt` y `GenerateDataKey*`. Para ajustarse al permiso de privilegios mínimos, especifique un elemento `Condition` para que solo la distribución de CloudFront especificada pueda realizar las acciones enumeradas. Puede personalizar la política para su política de AWS KMS actual. Para ver una política de claves de ejemplo de KMS, consulte SSE-KMS.

Si utiliza la identidad de acceso de origen (OAI) en lugar de OAC, los permisos para el bucket de Amazon S3 son ligeramente diferentes, porque concede permiso a una identidad en lugar de al Servicio de AWS. Para obtener más información, consulte Concesión de un permiso de identidad de acceso de origen para leer archivos en el bucket de Amazon S3.

Si sigue sin poder ver los archivos de su distribución, consulte No puedo ver los archivos de mi distribución.

Está utilizando credenciales no válidas o no tiene permisos suficientes

Puede aparecer un mensaje de error Access Denied si utiliza credenciales de AWS SCT incorrectas o caducadas (clave de acceso y clave secreta) o si a su rol o usuario de IAM le falta el permiso necesario para realizar una acción en un recurso de CloudFront. Para obtener más información sobre los mensajes de error de acceso denegado, consulte Solución de problemas de mensajes de error de acceso denegado en la Guía del usuario de IAM.

Para obtener información acerca de cómo funciona IAM con CloudFront, consulte Identity and Access Management para Amazon CloudFront.

CloudFront devuelve un error InvalidViewerCertificate al intentar agregar un nombre de dominio alternativo

Si CloudFront devuelve un error `InvalidViewerCertificate` al intentar agregar un nombre de dominio alternativo (CNAME) a la distribución, revise la siguiente información para ayudarle a solucionar el problema. Este error puede indicar que es necesario resolver uno de los problemas siguientes para poder añadir el nombre de dominio alternativo.

Los siguientes errores se enumeran en el orden en que CloudFront comprueba la autorización para agregar un nombre de dominio alternativo. Esto puede ayudarle a solucionar problemas porque puede saber qué comprobaciones de verificación se han realizado correctamente en función del error que devuelva CloudFront.

There's no certificate attached to your distribution. (No hay ningún certificado asociado a la distribución).

> Para añadir un nombre de dominio alternativo (CNAME), debe asociar un certificado de confianza válido a la distribución. Revise los requisitos, obtenga un certificado válido que los cumpla, asócielo a la distribución e inténtelo de nuevo. Para obtener más información, consulte Requisitos para el uso de nombres de dominio alternativos.

There are too many certificates in the certificate chain for the certificate that you've attached. (Hay demasiados certificados en la cadena de certificados del certificado que ha asociado).

> Solo puede tener cinco certificados como máximo en una cadena de certificados. Reduzca el número de certificados de la cadena y, a continuación, vuelva a intentarlo.

The certificate chain includes one or more certificates that aren't valid for the current date. (La cadena de certificados incluye uno o varios certificados que no son válidos para la fecha actual).

> La cadena de certificados de un certificado que ha añadido tiene uno o varios certificados que no son válidos, ya sea porque un certificado todavía no es válida o porque un certificado ha caducado. Compruebe los campos Not Valid Before (No válido antes del) y Not Valid After (No válido después del) en los certificados de la cadena de certificados para asegurarse de que todos los certificados son válidos para las fechas que ha indicado.

The certificate that you've attached isn't signed by a trusted Certificate Authority (CA). (El certificado que ha asociado no está firmado por una entidad de certificación (CA) de confianza).

El certificado que se asocia a CloudFront para verificar un nombre de dominio alternativo no puede ser un certificado autofirmado. Debe estar firmado por una CA de confianza. Para obtener más información, consulte Requisitos para el uso de nombres de dominio alternativos.

The certificate that you've attached isn't formatted correctly (El certificado que ha asociado no tiene el formato correcto)

El formato del nombre de dominio y de la dirección IP que se incluyen en el certificado y el formato del certificado deben seguir el estándar para los certificados.

Se produjo un error interno de CloudFront.

CloudFront se ha bloqueado por un problema interno y no puede hacer las comprobaciones de validación de los certificados. En este caso, CloudFront devuelve un código de estado HTTP 500 e indica que hay un problema interno de CloudFront al asociar el certificado. Espere unos minutos y vuelva a intentar añadir el nombre de dominio alternativo con el certificado.

El certificado que ha asociado no cubre el nombre de dominio alternativo que intenta agregar.

Para cada nombre de dominio alternativo que agregue, CloudFront requiere que asocie un certificado SSL/TLS válido de una entidad de certificación (CA) de confianza que cubra el nombre de dominio, para validar su autorización para utilizarlo. Actualice el certificado para que incluya un nombre de dominio que cubra el CNAME que intenta agregar. Para obtener más información y ejemplos de uso de nombres de dominio con caracteres comodín, consulte Requisitos para el uso de nombres de dominio alternativos.

CloudFront devuelve un error de registro DNS mal configurado al intentar agregar un nuevo CNAME

Cuando tiene una entrada de DNS comodín existente que apunta a una distribución de CloudFront, si intenta agregar un nuevo CNAME con un nombre más específico, es posible que encuentre el siguiente error:

```
One or more aliases specified for the distribution includes an incorrectly configured
 DNS record that points to another CloudFront distribution. You must update the DNS
 record to correct the problem.
```

Este error se produce porque CloudFront consulta el DNS con el CNAME y la entrada de DNS comodín se resuelve en otra distribución.

Para resolver este problema, primero cree otra distribución y, a continuación, cree una entrada de DNS que apunte a la nueva distribución. Por último, agregue el CNAME más específico. Para obtener más información acerca de cómo agregar CNAME, consulte Adición de un nombre de dominio alternativo.

No puedo ver los archivos de mi distribución

Si no puede ver los archivos en la distribución de CloudFront, consulte los temas siguientes para encontrar soluciones comunes.

¿Se ha registrado en CloudFront y Amazon S3?

Para utilizar Amazon CloudFront con un origen de Amazon S3, debe registrarse en CloudFront y Amazon S3 por separado. Para obtener más información sobre cómo registrarse en CloudFront y Amazon S3, consulte Configuración de su Cuenta de AWS.

¿Están el bucket de Amazon S3 y los permisos de objetos establecidos correctamente?

Si utiliza CloudFront con un origen de Amazon S3, las versiones originales del contenido se almacenan en un bucket de S3. Para servir el contenido a los lectores, le recomendamos que utilice el control de acceso al origen (OAC) de CloudFront para asegurar el acceso al bucket de S3 de Amazon. Esto significa que el bucket de S3 es accesible solo a través de CloudFront. OAC controla el acceso de los lectores y la entrega segura a través de CloudFront. Para obtener más información sobre OAC, consulte the section called “Restricción del acceso a un origen de Amazon S3”.

Para obtener más información sobre cómo administrar el acceso al bucket, consulte Bloqueo del acceso público al almacenamiento de Amazon S3 en la Guía del usuario de Amazon S3.

Las propiedades del objeto y las del bucket son independientes. Debe otorgar privilegios de forma explícita a cada uno de los objetos de Amazon S3. Los objetos no heredan las propiedades de los buckets y las propiedades de los objetos deben establecerse de forma independiente del bucket.

¿Está su nombre de dominio alternativo (CNAME) configurado correctamente?

Si ya tiene un registro de CNAME para su nombre de dominio, actualice dicho registro o sustitúyalo por uno nuevo que apunte al nombre de dominio de su distribución.

Asimismo, asegúrese de que su registro de CNAME apunte al nombre de dominio de su distribución y no a su bucket de Amazon S3. Puede comprobar si el registro CNAME de su sistema DNS apunta al nombre de dominio de su distribución. Para ello, utilice una herramienta de DNS como dig.

El siguiente ejemplo muestra una solicitud de dig de un nombre de dominio llamado `images.example.com` y la parte pertinente de la respuesta. En `ANSWER SECTION`, consulte la línea que contiene `CNAME`. El registro de CNAME de su nombre de dominio estará configurado correctamente si el valor a la derecha de CNAME es el nombre de dominio de su distribución de CloudFront. Si aparece el bucket del servidor de origen de Amazon S3 o cualquier otro nombre de dominio, el registro de CNAME está configurado incorrectamente.

```
[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.
...
...
```

Para obtener más información acerca de CNAME, consulte Uso de URL personalizadas añadiendo nombres de dominio alternativos (CNAME).

¿Está haciendo referencia a la URL correcta de la distribución de CloudFront?

Asegúrese de que la URL a la que está haciendo referencia utilice el nombre de dominio (o CNAME) de la distribución de CloudFront y no del bucket de Amazon S3 o de un origen personalizado.

¿Necesita ayuda para solucionar un problema con un origen personalizado?

Si necesita que AWS le ayude a solucionar un problema con un origen personalizado, quizá necesitemos inspeccionar las entradas del encabezado `X-Amz-Cf-Id` de sus solicitudes. Si todavía no está registrando estas entradas, le recomendamos que considere hacerlo. Para obtener más información, consulte the section called “Uso de Amazon EC2 (u otro origen personalizado)”. Para obtener ayuda adicional, consulte el AWSCentro de soporte de .

Mensaje de error: Certificate: <id-certificado> is being used by CloudFront

Problema: está intentando eliminar un certificado SSL/TLS del almacén de certificados de IAM y recibe el mensaje "Certificate: <id-certificado> is being used by CloudFront".

Solución: cada distribución de CloudFront debe asociarse al certificado predeterminado de CloudFront o a un certificado SSL/TLS personalizado. Antes de eliminar un certificado SSL/TLS, deberá rotar el certificado (sustituir el certificado SSL/TLS personalizado por otro certificado SSL/TLS personalizado) o volver a usar el certificado de CloudFront predeterminado. Para solucionarlo, realice los pasos de uno de los procedimientos siguientes:

- Rotación de certificados SSL/TLS
- Reversión de un certificado SSL/TLS personalizado al certificado de CloudFront predeterminado

Solución de problemas de códigos de estado de respuesta a errores en CloudFront

Si CloudFront solicita un objeto desde su origen y el origen devuelve un código de estado HTTP 4xx o 5xx, hay un problema con la comunicación entre CloudFront y el origen.

En este tema también se incluyen pasos de solución de problemas para estos códigos de estado al utilizar Lambda@Edge o CloudFront Functions.

En los siguientes temas se proporcionan explicaciones detalladas de las posibles causas que subyacen a estas respuestas de error y se ofrece una guía paso a paso sobre cómo diagnosticar y resolver los problemas subyacentes.

Temas

- Código de estado HTTP 400 (Solicitud errónea)
- Código de estado HTTP 401 (sin autorización)
- Código de estado HTTP 403 (método no válido)
- Código de estado HTTP 403 (permiso denegado)
- Código de estado HTTP 404 (no encontrado)
- Código de estado HTTP 412 (condición previa con error)
- Código de estado HTTP 500 (error de servidor interno)
- Código de estado HTTP 502 (Puerta de enlace incorrecta)

- Código de estado HTTP 503 (Servicio no disponible)
- Código de estado HTTP 504 (Tiempo de espera de puerta de enlace agotado)

Código de estado HTTP 400 (Solicitud errónea)

CloudFront devuelve una solicitud errónea 400 cuando el cliente envía algún dato no válido en la solicitud, como la falta de contenido o contenido incorrecto en la carga útil o en los parámetros. Esto también podría representar un error de cliente genérico.

El origen de Amazon S3 devuelve un error 400

Si utiliza un origen de Amazon S3 con la distribución de CloudFront, es posible que la distribución envíe respuestas de error con el código de estado HTTP 400 Solicitud incorrecta y un mensaje similar al siguiente:

El encabezado de autorización tiene una estructura incorrecta; la región '*<AWS región>*' es incorrecta; se esperaba '*<AWS región>*'

Por ejemplo:

El encabezado de autorización tiene una estructura incorrecta; la región «us-east-1» es incorrecta; se esperaba «us-west-2'

Este problema puede producirse en la siguiente situación:

1. El origen de su distribución de CloudFront es un bucket de Amazon S3.
2. Ha movido el bucket de S3 de una región de AWS a otra. Es decir, eliminó el bucket de S3 y, a continuación, creó un nuevo bucket con el mismo nombre de bucket, pero en una región de AWS diferente a la ubicación del bucket de S3 original.

Para solucionar este error, actualice la distribución de CloudFront para que encuentre el bucket de S3 en la región de AWS actual del bucket.

Para actualizar la distribución de CloudFront

1. Inicie sesión en Consola de administración de AWS y abra la consola de CloudFront en https://console.aws.amazon.com/cloudfront/v4/home.
2. Elija la distribución que produce este error.

3. Elija Origins and Origin Groups (Orígenes y grupos de origen).
4. Busque el origen del bucket de S3 que movió. Seleccione la casilla de verificación situada junto a este origen y, a continuación, elija Edit (Editar).
5. Elija Yes, Edit (Sí, editar). No es necesario cambiar ninguna configuración antes de elegir Yes, Edit (Sí, Editar).

Cuando complete estos pasos, CloudFront volverá a implementar la distribución. Mientras la distribución se está implementando, verá el estado Implementando en la columna Última modificación. Una vez finalizada la implementación, debe dejar de recibir las respuestas de error `AuthorizationHeaderMalformed`.

El origen del equilibrador de carga de aplicación devuelve un error 400

Si está utilizando un origen de equilibrador de carga de aplicación con la distribución de CloudFront, entre las posibles causas de un error 400 se incluyen las siguientes:

- El cliente envió una solicitud incorrecta que no se ajusta a la especificación de HTTP.
- El encabezado de la solicitud supera los 16 KB por línea de solicitud, los 16 KB por encabezado único o los 64 KB para el encabezado completo de la solicitud.
- El cliente cerró la conexión antes de enviar el cuerpo completo de la solicitud.

Código de estado HTTP 401 (sin autorización)

Un código de estado de respuesta 401 sin autorización indica que la solicitud del cliente no se ha completado porque carece de credenciales de autenticación válidas para el recurso solicitado. Este código de estado se envía con un encabezado de respuesta `WWW-Authenticate` de HTTP que contiene información sobre cómo el cliente puede volver a solicitar el recurso después de pedir al usuario las credenciales de autenticación. Para obtener más información, consulte 401 sin autorización.

En CloudFront, si el origen espera un encabezado `Authorization` para autenticar las solicitudes, CloudFront necesita reenviar el encabezado `Authorization` al origen para evitar un error 401 sin autorización. Cuando CloudFront reenvía una solicitud del lector a su origen, CloudFront elimina algunos encabezados de lector de forma predeterminada, incluido el encabezado `Authorization`. Para asegurarse de que su origen siempre recibe el encabezado `Authorization` en las solicitudes de origen, tiene las siguientes opciones:

- Agregue el encabezado `Authorization` a la clave de caché mediante una política de caché. Todos los encabezados de la clave de caché se incluyen automáticamente en las solicitudes de origen. Para obtener más información, consulte Control de la clave de caché con una política.
- Utilice una política de solicitud de origen que reenvíe todos los encabezados del lector al origen. No puede reenviar el encabezado `Authorization` individualmente en una política de solicitud de origen, pero, cuando reenvíe todos los encabezados del lector, CloudFront incluye el encabezado `Authorization` en las solicitudes de lector. CloudFront proporciona la política de solicitud de origen `AllViewer` administrada para este caso de uso. Para obtener más información, consulte Uso de políticas de solicitudes de origen administradas.

Para obtener más información, consulte How can I configure CloudFront to forward the Authorization header to the origin?

Código de estado HTTP 403 (método no válido)

CloudFront devuelve un error 403 (método no permitido) si intenta utilizar un método HTTP que no ha especificado en la distribución de CloudFront. Puede especificar una de las siguientes opciones para la distribución:

- CloudFront solo reenvía las solicitudes `GET` y `HEAD`.
- CloudFront solo reenvía las solicitudes `GET`, `HEAD` y `OPTIONS`.
- CloudFront reenvía las solicitudes `GET`, `HEAD`, `OPTIONS`, `PUT`, `PATCH`, `POST` y `DELETE`. (Si selecciona esta opción, es posible que tenga que restringir el acceso al bucket de Amazon S3 o al origen personalizado para que los usuarios no puedan realizar operaciones que usted no desea. Por ejemplo, es posible que no desee que los usuarios tengan permisos para eliminar objetos de su origen.

Código de estado HTTP 403 (permiso denegado)

Un error HTTP 403 significa que el cliente no tiene autorización para acceder al recurso solicitado. El cliente entiende la solicitud, pero no puede autorizar el acceso del lector. Las siguientes son causas comunes cuando CloudFront devuelve este código de estado:

Temas

- El CNAME alternativo está configurado incorrectamente
- AWS WAF se configura en la distribución de CloudFront o en el origen

- El origen personalizado devuelve un error 403
- El origen de Amazon S3 devuelve un error 403
- Las restricciones geográficas devuelven un error 403
- La configuración de URL firmada o cookie firmada devuelve un error 403
- Las distribuciones apiladas provocan un error 403

El CNAME alternativo está configurado incorrectamente

Compruebe que ha especificado el CNAME correcto para nuestra distribución. Para utilizar un CNAME alternativo en lugar de la URL predeterminada de CloudFront:

1. Cree un registro CNAME en el DNS para apuntar el CNAME a la URL de distribución de CloudFront.
2. Agregue el CNAME en la configuración de la distribución de CloudFront.

Si crea el registro DNS pero no agrega el CNAME en la configuración de la distribución de CloudFront, la solicitud devolverá un error 403. Para obtener más información sobre la configuración de un CNAME personalizado, consulte Uso de URL personalizadas añadiendo nombres de dominio alternativos (CNAME).

AWS WAF se configura en la distribución de CloudFront o en el origen

Cuando AWS WAF se sitúa entre el cliente y CloudFront, CloudFront no puede distinguir entre un código de error 403 devuelto por el origen y un código de error 403 devuelto por AWS WAF cuando se bloquea una solicitud.

Para encontrar el origen del código de estado 403, busque en la regla de la lista de control de acceso (ACL) web de AWS WAF una solicitud bloqueada. Para obtener más información, consulte los temas siguientes:

- AWS WAF Listas de control de acceso web (ACL web) de)
- Prueba y ajuste de las protecciones de AWS WAF

El origen personalizado devuelve un error 403

Si utiliza un origen personalizado, es posible que aparezca un error 403 si tiene una configuración de firewall personalizada en el origen. Para solucionar el problema, efectúe la solicitud directamente al

origen. Si puede reproducir el error sin CloudFront, significa que el origen está provocando el error 403.

Si el origen personalizado provoca el error, consulte los registros del origen para identificar la posible causa del error. Para obtener más información, consulte los siguientes temas de solución de problemas:

- Cómo soluciono los errores HTTP 403 de API Gateway?
- Cómo soluciono los errores de prohibición HTTP 403 del equilibrador de carga de aplicación?

El origen de Amazon S3 devuelve un error 403

Es posible que vea un error 403 por las siguientes razones:

- CloudFront no tiene acceso al bucket de Amazon S3. Esto puede ocurrir si la identidad de acceso de origen (OAI) o el control de acceso de origen (OAC) no están habilitados para la distribución y el bucket es privado.
- La ruta especificada en la URL solicitada no es correcta.
- El objeto solicitado no existe.
- El encabezado del host se ha reenviado con el punto de conexión de la API de REST. Para obtener más información, consulte Especificación de bucket de encabezado de host HTTP en la Guía del usuario de Amazon Simple Storage Service.
- Ha configurado páginas de error personalizadas. Para obtener más información, consulte Cómo CloudFront procesa los errores cuando las páginas de error personalizadas están configuradas.

Las restricciones geográficas devuelven un error 403

Si ha habilitado las restricciones geográficas (también conocidas como bloqueo geográfico) para evitar que los usuarios de ubicaciones geográficas específicas accedan al contenido que está distribuyendo a través de una distribución de CloudFront, los usuarios bloqueados recibirán un error 403.

Para obtener más información, consulte Restricción de la distribución geográfica de su contenido.

La configuración de URL firmada o cookie firmada devuelve un error 403

Si ha habilitado la opción Restringir el acceso de lector en la configuración de comportamiento de la distribución, las solicitudes que no utilicen cookies ni URL firmadas producirán un error 403. Para obtener más información, consulte los temas siguientes:

- Distribución de contenido privado con URL firmadas y cookies firmadas
- Cómo soluciono los problemas relacionados con una URL o cookies firmadas en CloudFront?

Las distribuciones apiladas provocan un error 403

Si tiene dos o más distribuciones en una cadena de solicitudes al punto de conexión de origen, CloudFront devuelve un error 403. No recomendamos anteponer una distribución a otra.

Código de estado HTTP 404 (no encontrado)

CloudFront devuelve un error 404 (no encontrado) cuando el cliente intenta acceder a un recurso que no existe. Si recibe este error con la distribución de CloudFront, las causas más comunes son las siguientes:

- El recurso no existe.
- La URL es incorrecta.
- El origen personalizado devuelve un error 404.
- Las páginas de error personalizadas devuelven un error 404. (Cualquier código de error puede traducirse a 404). Para obtener más información, consulte Cómo CloudFront procesa los errores cuando las páginas de error personalizadas están configuradas.
- La página de error personalizada se ha eliminado accidentalmente, lo que provoca un error 404 porque la solicitud busca la página de error personalizada eliminada. Para obtener más información, consulte Cómo CloudFront procesa los errores si no ha configurado las páginas de error personalizadas.
- Ruta de origen incorrecta. Si se rellena la ruta de origen, el valor se adjunta a la ruta de cada solicitud del navegador antes de que la solicitud se reenvíe al origen. Para obtener más información, consulte Ruta de origen.

Código de estado HTTP 412 (condición previa con error)

CloudFront devuelve un código de error 412 (condición previa con error) cuando se ha denegado el acceso al recurso de destino. En algunos casos, un servidor está configurado para aceptar solicitudes solo después de que se cumplan determinadas condiciones. Si no se cumple alguna de las condiciones especificadas, el servidor no permite que el cliente acceda al recurso indicado. En su lugar, el servidor responde con un código de error 412.

Entre las causas comunes de un error 412 en CloudFront se incluyen:

- Solicitudes condicionales en métodos distintos de `GET` o `HEAD` cuando no se cumple la condición definida por los encabezados `If-Unmodified-Since` o `If-None-Match`. En ese caso, la solicitud, normalmente una carga o una modificación de un recurso, no se puede realizar.
- Una condición en uno o más de los campos de solicitud de la operación de la API UpdateDistribution de CloudFront se evalúa como falsa.

Código de estado HTTP 500 (error de servidor interno)

Un código de estado HTTP 500 (error de servidor interno) indica que el servidor ha encontrado una condición inesperada que le ha impedido satisfacer la solicitud. A continuación, se indican algunas causas comunes de los errores 500 en Amazon CloudFront.

Temas

- El servidor de origen devuelve el error 500 a CloudFront

El servidor de origen devuelve el error 500 a CloudFront

Es posible que el servidor de origen esté devolviendo un error 500 a CloudFront. Consulte los siguientes temas de solución de problemas para obtener más información:

- Si Amazon S3 devuelve un error 500, consulte ¿Cómo soluciono un error HTTP 500 o 503 de Amazon S3?
- Si API Gateway devuelve un error 500, consulte ¿Cómo soluciono los errores 5xx de la API de REST de API Gateway?
- Si Elastic Load Balancing devuelve un error 500, consulte HTTP 500: Internal server error en la Guía del usuario para equilibradores de carga de aplicación.

Si la lista anterior no resuelve el error 500, es posible que el problema se deba a que un punto de presencia de CloudFront devuelve un error de servidor interno. Puede contactar con Soporte si necesita ayuda.

Código de estado HTTP 502 (Puerta de enlace incorrecta)

CloudFront devuelve un código de estado HTTP 502 (puerta de enlace incorrecta) cuando CloudFront no ha podido servir el objeto solicitado porque no se ha podido conectar con el servidor de origen.

Si utiliza Lambda@Edge, puede que el problema sea un error de validación de Lambda. Si recibe un error HTTP 502 con el código de error `NonS3OriginDnsError`, posiblemente hay un problema de configuración de DNS que impide que CloudFront se conecte al origen.

Temas

- Error de negociación SSL/TLS entre CloudFront y un servidor de origen personalizado
- El origen no responde con protocolos ni cifrados admitidos
- El certificado SSL/TLS del origen ha caducado, no es válido, es autofirmado o el orden de la cadena de certificados es incorrecto
- El origen no responde en puertos especificados en la configuración de origen
- Error de validación de Lambda
- Error de validación de la función de CloudFront
- Error de DNS (NonS3OriginDnsError)
- Error 502 originado por el equilibrador de carga de aplicación
- Error 502 de origen de API Gateway

Error de negociación SSL/TLS entre CloudFront y un servidor de origen personalizado

Si utiliza un origen personalizado que requiere HTTPS entre CloudFront y el origen, los nombres de dominio no coincidentes podrían causar errores. El certificado SSL/TLS del origen debe incluir un nombre de dominio que coincida con el Dominio de origen que especificó para la distribución de CloudFront o con el encabezado `Host` de la solicitud de origen.

Si los nombres de dominio no coinciden, el protocolo SSL/TLS devuelve un error, y CloudFront devuelve un código de estado HTTP 502 (gateway incorrecta) y establece el encabezado `X-Cache` en `Error from cloudfront`.

Para determinar si los nombres de dominio del certificado coinciden con el Dominio de origen en la distribución o con el encabezado `Host`, utilice un comprobador de SSL en línea u OpenSSL. Si los nombres de dominio no coinciden, tiene dos opciones:

- Obtener un nuevo certificado SSL/TLS que incluya los nombres de dominio aplicables.

  Si utiliza AWS Certificate Manager (ACM), consulte Solicitar un certificado público en la Guía del usuario de AWS Certificate Manager para solicitar un certificado nuevo.
- Cambie la configuración de la distribución para que CloudFront deje de intentar utilizar SSL para conectarse al origen.

Comprobador de SSL en línea

Para encontrar una herramienta de comprobación de SSL, busque en Internet "comprobador ssl online". Por lo general, especifica el nombre de su dominio y la herramienta devuelve información acerca de su certificado SSL/TLS. Compruebe que el certificado contenga su nombre de dominio en los campos Nombre común o Nombres alternativos de sujeto.

OpenSSL

Como ayuda para solucionar los errores HTTP 502 desde CloudFront, puede utilizar OpenSSL para intentar realizar una conexión SSL/TLS con el servidor de origen. Si OpenSSL no puede establecer una conexión, puede indicar un problema con la configuración de SSL/TLS del servidor de origen. Si OpenSSL puede establecer una conexión, devuelve información sobre el certificado del servidor de origen, incluido el nombre común (campo `Subject CN`) y el nombre alternativo del sujeto (campo `Subject Alternative Name`) del certificado.

Utilice el siguiente comando de OpenSSL para probar la conexión con el servidor de origen (sustituya *`dominio de origen`* por el nombre de dominio del servidor de origen, como example.com):

```
openssl s_client -connect origin domain name:443
```

Si se cumplen las siguientes condiciones:

- El servidor de origen admite varios nombres de dominio con varios certificados SSL/TLS
- Su distribución está configurada para reenviar el encabezado `Host` al origen

Agregue la opción `-servername` al comando OpenSSL, como en el siguiente ejemplo (sustituya *`CNAME`* por el CNAME configurado en la distribución):

```
openssl s_client -connect origin domain name:443 -servername CNAME
```

El origen no responde con protocolos ni cifrados admitidos

CloudFront se conecta con servidores de origen a través de códigos cifrados y protocolos. Para obtener una lista de los algoritmos criptográficos y protocolos que CloudFront admite, consulte the section called “Protocolos y cifrados admitidos entre CloudFront y el origen”. Si el origen no responde con uno de estos algoritmos criptográficos o protocolos en el intercambio SSL/TLS, CloudFront no puede conectarse. Use una herramienta en línea como SSL Labs para comprobar si el origen es compatible con los cifrados y protocolos. Escriba el nombre de dominio del origen en el campo Hostname (Nombre de host) y, a continuación, elija Submit (Enviar). Revise los campos Common names (Nombres comunes) y Alternative names (Nombres alternativos) de la prueba para ver si coinciden con el nombre de dominio del origen. Una vez finalizada la prueba, busque las secciones Protocols (Protocolos) y Cipher Suites (Conjuntos de cifrado) del resultado de las pruebas para saber qué protocolos o cifrados admite el origen. Compárelos con la lista que aparece en the section called “Protocolos y cifrados admitidos entre CloudFront y el origen”.

El certificado SSL/TLS del origen ha caducado, no es válido, es autofirmado o el orden de la cadena de certificados es incorrecto

Si el servidor de origen devuelve lo siguiente, CloudFront interrumpe la conexión TCP, devuelve el código de estado HTTP 502 (gateway incorrecta) y establece el encabezado `X-Cache` en `Error from cloudfront`:

- Un certificado caducado
- Un certificado no válido
- Un certificado autofirmado
- Orden incorrecto en una cadena de certificados

> **Note**
>
> Si no está presente la cadena completa de certificados, incluidos los certificados intermedios, CloudFront interrumpe la conexión TCP.

Para obtener más información acerca de cómo instalar un certificado SSL/TLS en su servidor de origen personalizado, consulte the section called “Exigencia de HTTPS en un origen personalizado”.

El origen no responde en puertos especificados en la configuración de origen

Al crear un origen en la distribución de CloudFront, puede definir los puertos que CloudFront conecta con el origen para el tráfico HTTP y HTTPS. De forma predeterminada, estos son 80/443 TCP. Puede modificar estos puertos. Si el origen rechaza el tráfico en estos puertos por cualquier motivo, o si el servidor backend no está respondiendo en los puertos, CloudFront no se conectará.

Para solucionar estos problemas, revise los firewalls de su infraestructura y compruebe que no estén bloqueando los rangos de IP admitidos. Para obtener más información, consulte Rangos de dirección IP de AWS en la Guía del usuario de Amazon VPC. Compruebe también si su servidor web se ejecuta en el origen.

Error de validación de Lambda

Si utiliza Lambda@Edge, un código de estado HTTP 502 puede indicar que la respuesta de la función Lambda tenía un formato incorrecto o incluía contenido no válido. Para obtener más información sobre la resolución de errores Lambda@Edge, consulte Prueba y depuración de funciones de Lambda@Edge.

Error de validación de la función de CloudFront

Si utiliza CloudFront Functions, un código de estado HTTP 502 puede indicar que la función de CloudFront intenta agregar, eliminar o cambiar un encabezado de solo lectura. Este error no aparece durante las pruebas, pero aparecerá después de implementar la función y ejecutar la solicitud. Para corregir este error, compruebe y actualice la función de CloudFront. Para obtener más información, consulte Actualización de funciones.

Error de DNS (`NonS3OriginDnsError`)

Un error HTTP 502 con el código de error `NonS3OriginDnsError` indica que hay un problema de configuración de DNS que impide que CloudFront se conecte al origen. Si recibe este error de CloudFront, asegúrese de que la configuración de DNS del origen es correcta y funciona.

Cuando CloudFront recibe una solicitud de un objeto que ha caducado o que no está en su caché, realiza una solicitud al origen para obtener el objeto. Para que la solicitud al origen se complete correctamente, CloudFront realiza una resolución de DNS en el dominio de origen. Si el servicio de DNS para el dominio tiene problemas, CloudFront no puede resolver el nombre de dominio para obtener la dirección IP, lo que se traduce en un error HTTP 502 (`NonS3OriginDnsError`). Para solucionar este problema, contacte con el proveedor de DNS o, si está utilizando Amazon Route 53, consulte ¿Por qué no puedo acceder a mi sitio web que utiliza los servicios DNS de Route 53?

Para solucionar este problema, asegúrese de que los servidores de nombres autoritativos del dominio raíz o ápex de zona (como `example.com`) del origen funcionan correctamente. Puede utilizar los siguientes comandos para encontrar los servidores de nombres del origen de ápex, con una herramienta como dig o nslookup:

```
dig OriginAPEXDomainName NS +short
```

```
nslookup -query=NS OriginAPEXDomainName
```

Una vez tenga los nombres de los servidores de nombres, utilice los siguientes comandos para consultar el nombre de dominio del origen ante ellos para asegurarse de que cada uno de ellos genera una respuesta:

```
dig OriginDomainName @NameServer
```

```
nslookup OriginDomainName NameServer
```

> **Important**
>
> Asegúrese de realizar esta solución de problemas de DNS con un equipo que esté conectado a la Internet pública. CloudFront resuelve el dominio de origen mediante un DNS público en Internet, por lo que es importante solucionar los problemas en un contexto similar.

Si el origen es un subdominio cuya autoridad de DNS está delegada en un servidor de nombres diferente al dominio raíz, asegúrese de que los registros del servidor de nombres (`NS`) y el inicio de la autoridad (`SOA`) estén configurados correctamente para el subdominio. Puede comprobar estos registros mediante comandos similares a los de los ejemplos anteriores.

Para obtener más información sobre DNS, consulte los conceptos del sistema de nombres de dominio (DNS) en la documentación de Amazon Route 53.

Error 502 originado por el equilibrador de carga de aplicación

Si utiliza equilibrador de carga de aplicación como origen y recibe un error 502, consulte ¿Cómo soluciono los errores HTTP 502 del equilibrador de carga de aplicación?.

Error 502 de origen de API Gateway

Si utiliza API Gateway y recibe un error 502, consulte ¿Cómo resuelvo los errores HTTP 502 de las API de REST de API Gateway con la integración de proxy de Lambda?.

Código de estado HTTP 503 (Servicio no disponible)

El código de estado HTTP 503 (Servicio no disponible) suele indicar un problema de desempeño en el servidor de origen. En casos excepcionales, indica que CloudFront no puede satisfacer temporalmente una solicitud debido a restricciones de recursos en una ubicación periférica.

Si utiliza Lambda@Edge o CloudFront Functions, puede que el problema se deba a un error de ejecución o a un error de superación de límite de Lambda@Edge.

Temas

- El servidor de origen no tiene capacidad suficiente para soportar la tasa de solicitudes
- CloudFront ha causado el error debido a las restricciones de recursos en la ubicación de borde
- Error de ejecución de la Lambda@Edge o CloudFront Function
- Superación del límite de Lambda@Edge

El servidor de origen no tiene capacidad suficiente para soportar la tasa de solicitudes

Cuando un servidor de origen no está disponible o no puede atender solicitudes entrantes, devuelve un código de estado HTTP 503 (servicio no disponible). En ese caso, CloudFront devuelve el error al usuario. Para resolver este problema, pruebe lo siguiente:

- Si utiliza Amazon S3 como servidor de origen:
  - puede realizar al 3500 solicitudes PUT/COPY/POST/DELETE o 5500 solicitudes GET/HEAD por segundo y prefijo de Amazon S3 dividido. Cuando Amazon S3 devuelve una respuesta 503 Slow Down, normalmente indica una tasa de solicitudes excesiva con respecto a un prefijo de Amazon S3 específico.

    Como las tasas de solicitud se aplican por prefijo en un bucket de S3, los objetos deben distribuirse entre varios prefijos. A medida que la tasa de solicitudes de los prefijos aumenta gradualmente, Amazon S3 se escala para gestionar las solicitudes de cada uno de los prefijos por separado. Como resultado, la tasa general de solicitudes que gestiona el bucket es un múltiplo del número de prefijos.

  - Para obtener más información, consulte Optimizar el rendimiento de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.
- Si utiliza Elastic Load Balancing como servidor de origen:
  - Asegúrese de que sus instancias de backend puedan responder a las comprobaciones de estado.
  - Asegúrate de que el equilibrador de carga y las instancias de backend puedan gestionar la carga.

  Para obtener más información, consulte:

  - Cómo puedo solucionar los errores 503 devueltos al utilizar un equilibrador de carga clásico?
  - How do I troubleshoot 503 (service unavailable) errors from my Application Load Balancer?
- Si utiliza un origen personalizado:
  - Revise los registros la aplicación para garantizar que su origen cuenta con suficientes recursos, como memoria, CPU y tamaño de disco.
  - Si utiliza Amazon EC2 como backend, asegúrese de que el tipo de instancia cuente con los recursos apropiados para responder adecuadamente a las solicitudes entrantes. Para obtener más información, consulte Tipos de instancia en la Guía del usuario de Amazon EC2.
- Si utiliza API Gateway:
  - Este error está relacionado con la integración del backend cuando la API de API Gateway no puede recibir una respuesta. El servidor backend:
    - Podría estar sobrecargado por encima de su capacidad y no puede procesar las solicitudes de nuevos clientes.
    - Podría estar en mantenimiento temporal.
  - Para resolver este error, consulte los registros de las aplicaciones de API Gateway para determinar si hay algún problema con la capacidad del backend, la integración o algún otro problema.

CloudFront ha causado el error debido a las restricciones de recursos en la ubicación de borde

Recibirá este error en la improbable situación de que CloudFront no pueda dirigir las solicitudes hacia la siguiente mejor ubicación periférica disponible y, por tanto, no pueda satisfacer una solicitud. Este es un error común al realizar pruebas de carga en la distribución de CloudFront. Para ayudar

a evitarlo, siga las instrucciones de the section called “Pruebas de carga de CloudFront” para evitar errores 503 (Capacidad superada).

Si esto ocurre en su entorno de producción, póngase en contacto con Soporte.

Error de ejecución de la Lambda@Edge o CloudFront Function

Si utiliza Lambda@Edge o CloudFront Functions, un código de estado HTTP 503 puede indicar que la función de ha devuelto un error de ejecución.

Para obtener más información acerca de cómo identificar y resolver errores de Lambda@Edge, consulte Prueba y depuración de funciones de Lambda@Edge.

Para obtener más información acerca de las pruebas de CloudFront Functions, consulte Prueba de funciones.

Superación del límite de Lambda@Edge

Si utiliza Lambda@Edge, un código de estado HTTP 503 puede indicar que Lambda ha devuelto un error. Esto podría deberse a una de las siguientes causas:

- El número de ejecuciones de la función superó una de las cuotas que Lambda establece para restringir las ejecuciones en una Región de AWS (ejecuciones simultáneas o frecuencia de invocación).
- La función superó la cuota de tiempo de espera de la función Lambda.

Para obtener más información sobre las cuotas de Lambda@Edge, consulte Cuotas de Lambda@Edge. Para obtener más información acerca de cómo identificar y resolver errores de Lambda@Edge, consulte the section called “Prueba y depuración”. También puede consultar las cuotas del servicio Lambda en la Guía para desarrolladores de AWS Lambda.

Código de estado HTTP 504 (Tiempo de espera de puerta de enlace agotado)

Un código de estado HTTP 504 (tiempo de espera de puerta de enlace superado) indica que cuando CloudFront reenvió una solicitud al origen (porque el objeto solicitado no estaba en la caché perimetral), se produjo alguna de las siguientes circunstancias:

- El origen devolvió un código de estado HTTP 504 a CloudFront.
- El origen no respondió antes de que la solicitud caducara.

CloudFront devolverá un código de estado HTTP 504 si un firewall o grupo de seguridad bloquea el tráfico al origen o si el origen no es accesible en Internet. Compruebe en primer lugar si ocurren estos problemas. A continuación, si el acceso no es el problema, explore los retrasos de la aplicación y los tiempos de espera del servidor para ayudarle a identificar y corregir los problemas.

Temas

- Configurar el firewall en su servidor de origen para permitir el tráfico de CloudFront
- Configurar los grupos de seguridad en su servidor de origen para permitir el tráfico de CloudFront
- Hacer que su servidor de origen personalizado sea accessible en Internet
- Buscar y corregir respuestas con retardo desde aplicaciones en su servidor de origen

Configurar el firewall en su servidor de origen para permitir el tráfico de CloudFront

Si el firewall en el servidor de origen bloquea el tráfico de CloudFront, CloudFront devuelve un código de estado HTTP 504, por lo que es recomendable asegurarse de que este no es el problema antes de comprobar otros problemas.

El método que se utiliza para determinar si se trata de un problema con su firewall depende del sistema que utiliza su servidor de origen:

- Si utiliza un firewall IPTable en un servidor Linux, puede buscar herramientas e información para ayudarle a trabajar con IPTables.
- Si utiliza Windows Firewall en un servidor de Windows, consulte Agregar o editar regla de firewall en la documentación de Microsoft.

Al evaluar la configuración del firewall en su servidor de origen, busque las reglas de firewalls o de seguridad que bloquean el tráfico desde ubicaciones de borde de CloudFront, en función del intervalo de direcciones IP publicado. Para obtener más información, consulte Ubicaciones e intervalos de direcciones IP de servidores de borde de CloudFront.

Si el intervalo de direcciones IP de CloudFront tiene permiso para conectarse al servidor de origen, asegúrese de actualizar las reglas de seguridad del servidor para incorporar los cambios. Puede suscribirse a un tema de Amazon SNS y recibir notificaciones cuando se actualiza el archivo del rango de direcciones IP. Después de recibir la notificación, puede utilizar código para recuperar el archivo, analizarlo y realizar ajustes para el entorno local. Para obtener más información, consulte Suscribirse a cambios de direcciones IP públicas de AWS mediante Amazon SNS en el blog de noticias de AWS.

Configurar los grupos de seguridad en su servidor de origen para permitir el tráfico de CloudFront

Si su origen usa Elastic Load Balancing, revise los grupos de seguridad de ELB y asegúrese de que los grupos de seguridad permiten el tráfico de entrada desde CloudFront.

También puede utilizar AWS Lambda para actualizar de manera automática sus grupos de seguridad para permitir el tráfico entrante desde CloudFront.

Hacer que su servidor de origen personalizado sea accessible en Internet

Si CloudFront no puede acceder al servidor de origen personalizado porque no está disponible públicamente en Internet, devuelve un error HTTP 504.

Las ubicaciones de borde de CloudFront se conectan con los servidores de origen a través de Internet. Si el origen personalizado se encuentra en una red privada, CloudFront no puede tener acceso a él. Por este motivo, no puede utilizar servidores privados, incluidos equilibradores de carga clásicos internos, como servidores de origen con CloudFront.

Para comprobar que el tráfico de Internet puede conectarse a su servidor de origen, ejecute los siguientes comandos (donde *`OriginDomainName`* es el nombre de dominio de su servidor):

Para tráfico HTTPS:

- nc -zv *`OriginDomainName`* 443
- telnet *`OriginDomainName`* 443

Para el tráfico HTTP:

- nc -zv *`OriginDomainName`* 80
- telnet *`OriginDomainName`* 80

Buscar y corregir respuestas con retardo desde aplicaciones en su servidor de origen

Los tiempos de espera superados del servidor suelen deberse a que la aplicación tarda mucho en responder o a que se ha establecido un valor de tiempo de espera demasiado bajo.

Una solución rápida que ayuda a evitar errores HTTP 504 consiste sencillamente en establecer un valor de tiempo de espera de CloudFront mayor para su distribución. Sin embargo, le recomendamos

que primero se asegure de corregir los problemas de desempeño y de latencia con la aplicación y el servidor de origen. A continuación, puede establecer un valor de tiempo de espera razonable que ayude a evitar errores HTTP 504 y proporcione buena capacidad de respuesta a los usuarios.

A continuación, se muestra información general de los pasos que puede seguir para buscar problemas de desempeño y corregirlos:

1. Mida la latencia típica y de carga elevada (capacidad de respuesta) de su aplicación web.
2. Añada recursos adicionales, como CPU o memoria, si es necesario. Tome otras medidas para corregir problemas como, por ejemplo, ajuste de consultas de base de datos para dar cabida a supuestos de carga elevada.
3. Si es necesario, ajuste el valor de tiempo de espera de su distribución de CloudFront.

A continuación se muestran los detalles de cada paso.

Medir la latencia típica y de carga elevada

Para determinar si uno o más servidores de aplicación web de backend experimentan una alta latencia, ejecute el siguiente comando curl de Linux en cada servidor:

```
curl -w "DNS Lookup Time: %{time_namelookup} \nConnect time: %{time_connect}
 \nTLS Setup: %{time_appconnect} \nRedirect Time: %{time_redirect} \nTime to first
 byte: %{time_starttransfer} \nTotal time: %{time_total} \n" -o /dev/null https://
www.example.com/yourobject
```

> **Note**
>
> Si ejecuta Windows en sus servidores, puede buscar y descargar curl para Windows para ejecutar un comando similar.

A medida que mide y evalúa la latencia de una aplicación que se ejecuta en su servidor, tenga en cuenta lo siguiente:

- Los valores de latencia son relativos a cada aplicación. Sin embargo, un valor de Tiempo hasta el primer byte en milisegundos en lugar de segundos o más, es razonable.
- Si mide la latencia de la aplicación con carga normal y está bien, tenga en cuenta que es posible que los espectadores sigan sufriendo tiempos de espera con cargas elevadas. Cuando hay una

demanda alta, es posible que los servidores tengan respuestas con retraso o que no respondan. Para ayudarle a evitar problemas de latencia de carga elevada, compruebe los recursos del servidor tales como CPU, memoria y lecturas y escrituras en disco para asegurarse de que los servidores tengan la capacidad de escalar una carga elevada.

Puede ejecutar los siguientes comandos de Linux para comprobar la memoria que utilizan los procesos de Apache:

```
watch -n 1 "echo -n 'Apache Processes: ' && ps -C apache2 --no-headers |
wc -l && free -m"
```

- Una utilización de CPU alta en el servidor puede reducir notablemente el desempeño de una aplicación. Si utiliza una instancia Amazon EC2 para su servidor backend, revise las métricas de CloudWatch del servidor para comprobar la utilización de la CPU. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch. O bien, si está utilizando un servidor propio, consulte la documentación de ayuda del servidor para obtener instrucciones sobre cómo comprobar el uso de la CPU.
- Compruebe si hay otros posibles problemas con cargas elevadas, como, por ejemplo, consultas de base de datos que se ejecutan lentamente cuando hay un gran volumen de solicitudes.

Agregar recursos y ajustar servidores y bases de datos

Después de evaluar la capacidad de respuesta de las aplicaciones y servidores, asegúrese de que dispone de recursos suficientes para las situaciones de tráfico normal y de carga elevada:

- Si tiene su propio servidor, asegúrese de tener suficiente CPU, memoria y espacio en disco para gestionar las solicitudes de los espectadores, en función de su evaluación.
- Si utiliza una instancia Amazon EC2 como servidor backend, asegúrese de que el tipo de instancia cuente con los recursos apropiados para responder adecuadamente a las solicitudes entrantes. Para obtener más información, consulte Tipos de instancia en la Guía del usuario de Amazon EC2.

Además, tenga en cuenta los siguientes pasos de ajuste para ayudar a evitar tiempos de espera:

- Si el valor Tiempo hasta el primer byte que devuelve el comando curl parece alto, tome medidas para mejorar el desempeño de su aplicación. Mejorar la capacidad de respuesta de la aplicación a su vez reduce los errores de tiempo de espera.
- Ajuste las consultas de la base de datos para asegurarse de que puedan administrar volúmenes de solicitudes elevados sin un desempeño lento.

- Configure conexiones keep-alive (persistente) en su servidor de backend. Esta opción ayuda a evitar las latencias que se producen cuando las conexiones deben volver a establecerse para las solicitudes o usuarios posteriores.
- Si utiliza Elastic Load Balancing como origen, las siguientes son las posibles causas de un error 504:
  - El equilibrador de carga no consigue establecer una conexión con el destino antes de que expire el tiempo de espera de la conexión (10 segundos).
  - El equilibrador de carga establece una conexión con el destino pero este no responde antes de que transcurra el periodo de tiempo de espera de inactividad.
  - La lista de control de acceso (ACL) de red para la subred no permite el tráfico desde los destinos a los nodos del equilibrador de carga en los puertos efímeros (1024-65535).
  - El destino devuelve un encabezado de longitud de contenido que es mayor que el cuerpo de la entidad. Se agota el tiempo del equilibrador de carga a la espera de los bytes que faltan.
  - El destino es una función de Lambda y Lambda no responde antes de que se agote el tiempo de espera de la conexión.

  Para obtener más información sobre cómo reducir la latencia, consulte ¿Cómo soluciono una alta latencia en mi equilibrador de carga clásico de ELB?
- Si utiliza MediaTailor como origen, las siguientes son las posibles causas de un error 504:
  - Si se gestionan mal las URL relativas, MediaTailor puede recibir URL con formato incorrecto de los reproductores.
  - Si MediaPackage es el origen del manifiesto para MediaTailor, los errores de manifiesto 404 de MediaPackage pueden provocar que MediaTailor devuelva un error 504.
  - La solicitud al servidor de origen MediaTailor tarda más de dos segundos en completarse.
- Si utiliza Amazon API Gateway como origen, la siguiente es una posible causa de un error 504:
  - Una solicitud de integración tarda más que su parámetro de tiempo máximo de integración de la API de REST de API Gateway. Para obtener más información, consulte ¿Cómo soluciono los errores de tiempo de espera HTTP 504 de la API con API Gateway?

Si es necesario, ajuste el valor de tiempo de espera de CloudFront

Si ha evaluado y solucionado el desempeño de aplicaciones lento, la capacidad del servidor de origen y otros problemas, pero los espectadores siguen experimentando errores HTTP 504, entonces debería plantearse cambiar el tiempo especificado en su distribución para tiempo de espera de

respuesta de origen. Para obtener más información, consulte the section called “Tiempo de espera de respuesta”.

Pruebas de carga de CloudFront

Los métodos de pruebas de carga tradicionales no funcionan bien con CloudFront porque CloudFront utiliza DNS para balancear las cargas entre ubicaciones de borde geográficamente dispersas y dentro de cada ubicación de borde. Cuando un cliente solicita contenido desde CloudFront, el cliente recibe una respuesta de DNS que incluye un conjunto de direcciones IP. Si realiza las pruebas enviando solicitudes a tan solo una de las direcciones IP que DNS devuelve, estará probando solo un pequeño subconjunto de los recursos de una ubicación de borde de CloudFront, lo que no representa de forma precisa los patrones de tráfico reales. En función del volumen de datos solicitados, este método de prueba puede sobrecargar y degradar el rendimiento de ese pequeño subconjunto de servidores de CloudFront.

CloudFront se ha diseñado para escalarse en función de los lectores que tienen diferentes direcciones IP de cliente y diferentes resoluciones de DNS en varias regiones geográficas. Para realizar pruebas de carga que evalúen el rendimiento de CloudFront con precisión, le recomendamos que haga todo lo siguiente:

- Envíe solicitudes de clientes desde varias regiones geográficas.
- Configure la prueba para que cada cliente realice una solicitud de DNS independiente. Así, cada cliente recibirá un conjunto distinto de direcciones IP de DNS.
- Por cada cliente que se realice solicitudes, distribuya las solicitudes de clientes en todo el conjunto de direcciones IP devueltas por DNS. Esto que garantiza que la carga se distribuye en varios servidores en una ubicación periférica de CloudFront.

> **Notas**
>
> - Las pruebas de carga no están permitidas en los comportamientos de caché que tienen desencadenantes de solicitud de visualizador o de respuesta de visualizador de Lambda@Edge.
> - Las pruebas de carga no están permitidas en los orígenes que tienen habilitado Origin Shield.

Cuotas

Puede solicitar un aumento de la cuota de CloudFront mediante las siguientes opciones:

- Puede utilizar la consola de Service Quotas o la AWS Command Line Interface. Para obtener más información, consulte los temas siguientes:
  - Solicitud de aumento de cuota en la Guía del usuario de Service Quotas
  - request-service-quota-increase en la Referencia de comandos de AWS CLI
- Si una cuota de CloudFront no está disponible en Service Quotas, utilice la AWS Support Center Console para crear un caso de incremento de la cuota de servicio.

CloudFront está supeditado a las siguientes cuotas.

Temas

- Cuotas generales
- Cuotas generales de distribuciones
- Cuotas generales de políticas
- Cuotas en mTLS y almacenes de confianza
- Cuotas en CloudFront Functions
- Cuotas en funciones de conexión
- Cuotas en almacenes de clave-valor
- Cuotas de Lambda@Edge
- Cuotas en certificados SSL
- Cuotas de invalidaciones
- Cuotas en grupos de claves
- Cuotas de conexiones WebSocket
- Cuotas de cifrado en el nivel de campo
- Cuotas en cookies (configuración de caché heredada)
- Cuotas en cadenas de consulta (configuración de caché heredada)
- Cuotas en encabezados
- Cuotas en distribuciones de varios inquilinos
- Información relacionada

Cuotas generales

Entidad	Cuota predeterminada
Tasa de transferencia de datos por distribución (Esta cuota no se aplica a las distribuciones suscritas a planes de precios de tarifa fija de CloudFront. Para obtener más información, consulte ???).	150 Gbps Solicitar una ampliación de la cuota
Solicitudes por segundo por distribución (Esta cuota no se aplica a las distribuciones suscritas a planes de precios de tarifa fija de CloudFront. Para obtener más información, consulte ???).	250.000 Solicitar una ampliación de la cuota
Etiquetas que se pueden agregar a una distribución	50 Solicitar una ampliación de la cuota
Archivos que puede ofrecer por distribución	Sin cuota
Longitud máxima de una solicitud o una respuesta de origen, incluidos los encabezados y las cadenas de consulta, pero sin incluir el contenido del cuerpo	20 480 bytes
Longitud máxima de una URL	8192 bytes
Número máximo de configuraciones de entrega de registros de acceso en tiempo real por Cuenta de AWS	150
Número máximo de asociaciones por ACL web	100 Solicitar una ampliación de la cuota

Cuotas generales de distribuciones

Entidad	Cuota predeterminada
Nombres de dominio alternativos (CNAME) por distribución Para obtener más información, consulte Uso de URL personalizadas añadiendo nombres de dominio alternativos (CNAME).	100 Solicitar una ampliación de la cuota
Comportamientos de la caché por distribución	75 Solicitar una ampliación de la cuota
Intentos de conexión por origen Para obtener más información, consulte Intentos de conexión.	1-3
Tiempo de espera de conexión por origen Para obtener más información, consulte Tiempo de espera de conexión.	1-10 segundos
Tiempo de espera de respuesta por origen Esto también se conoce como tiempo de espera de lectura del origen o tiempo de espera de la solicitud del origen. Para obtener más informaci ón, consulte Tiempo de espera de respuesta.	1-120 segundos Solicitar una ampliación de la cuota
Tiempo de espera activo por origen Para obtener más información, consulte Tiempo de espera de keep-alive (solo orígenes personalizados y de VPC).	1-120 segundos Solicitar una ampliación de la cuota
Distribuciones por Cuenta de AWS Para obtener más información, consulte Creación de una distribución.	500 Solicitar una ampliación de la cuota
Distribuciones por control de acceso de origen	100

Entidad	Cuota predeterminada
	Solicitar una ampliación de la cuota
Distribuciones en la cadena de solicitudes al punto de conexión de origen No recomendamos anteponer una distribución a otra. Si se supera esta cuota, se produce un error 403.	2
Compresión de archivos: intervalo de tamaños de archivos que CloudFront comprime Para obtener más información, consulte Ofrecimiento de archivos comprimidos.	1000 a 10 000 000 bytes
Tamaño máximo de archivo que se puede almacenar en caché por respuesta HTTP GET. Solo se almacenan en caché las respuestas para un HTTP GET. Las respuestas para POST o PUT no se almacenan en caché.	50 GB
Controles de acceso de origen por Cuenta de AWS	100 Solicitar una ampliación de la cuota
Identidades de acceso de origen por Cuenta de AWS	100 Solicitar una ampliación de la cuota
Orígenes por distribución	100 Solicitar una ampliación de la cuota

Entidad	Cuota predeterminada
Grupos de origen por distribución	10 Solicitar una ampliación de la cuota
Distribuciones provisionales por Cuenta de AWS Para obtener más información, consulte the section called “Uso de la implementación continua para probar de forma segura los cambios”.	20 Solicitar una ampliación de la cuota
Distribuciones asociadas al mismo origen de la VPC	50
Orígenes de la VPC por Cuenta de AWS	25 Solicitar una ampliación de la cuota
Número máximo de distribuciones que pueden asociarse a una única lista de direcciones IP estáticas de anycast.	100 Solicitar una ampliación de la cuota

Cuotas generales de políticas

Entidad	Cuota predeterminada
Políticas de caché personalizadas por Cuenta de AWS (No se aplica a las políticas de caché administradas de CloudFront)	20 Solicitar una ampliación de la cuota
Distribuciones asociadas con la misma política de caché	100
Cadenas de consulta por política de caché	10 Solicitar una ampliación de la cuota

Entidad	Cuota predeterminada
Encabezados por política de caché	10 Solicitar una ampliación de la cuota
Cookies por política de caché	10 Solicitar una ampliación de la cuota
Longitud total combinada de todos los nombres de cadenas de consulta, encabezados y cookies en una política de caché	1024
Políticas de solicitud de origen personalizadas por Cuenta de AWS (No se aplica a las políticas de solicitud de origen administradas de CloudFront)	20 Solicitar una ampliación de la cuota
Distribuciones asociadas con la misma política de solicitud de origen	100
Cadenas de consulta por política de solicitud de origen	10 Solicitar una ampliación de la cuota
Encabezados por política de solicitud de origen	10 Solicitar una ampliación de la cuota
Cookies por política de solicitud de origen	10 Solicitar una ampliación de la cuota
Longitud total combinada de todos los nombres de cadenas de consulta, encabezados y cookies en una política de solicitud de origen	1024

Entidad	Cuota predeterminada
Política de encabezados de respuesta personalizadas por Cuenta de AWS (No se aplica a las políticas de encabezados de respuesta administradas de CloudFront)	20 Solicitar una ampliación de la cuota
Distribuciones asociadas con la misma política de encabezados de respuesta	100 Solicitar una ampliación de la cuota
Política de encabezados de respuesta por encabezados personalizados	10 Solicitar una ampliación de la cuota
Políticas de implementación continua por Cuenta de AWS	20 Solicitar una ampliación de la cuota

Cuotas en mTLS y almacenes de confianza

Entidad	Cuota predeterminada
Almacenes de confianza por Cuenta de AWS	20 Solicitar una ampliación de la cuota
Distribuciones por almacén de confianza	25
Tamaño del paquete de CA	64 KB Solicitar una ampliación de la cuota

Entidad	Cuota predeterminada
Tamaño del certificado en el paquete de CA	16384 Solicitar una ampliación de la cuota
Número de certificados en el paquete de CA	25
Profundidad de la cadena de certificados	4

Cuotas en CloudFront Functions

Entidad	Cuota predeterminada
Funciones por Cuenta de AWS	100
Tamaño máximo de la función Esta cuota no se puede ajustar. Para almacenar datos adicionales para las CloudFront Functions, cree un almacén de clave-valor y agregue los pares clave-valor. Para obtener más información, consulte Amazon CloudFront KeyValueStore.	10 KB
Memoria máxima de la función	2 MB
Distribuciones asociadas con la misma función	100

Además de estas cuotas, existen algunas otras restricciones al utilizar CloudFront Functions. Para obtener más información, consulte Restricciones en CloudFront Functions.

Cuotas en funciones de conexión

Entidad	Cuota predeterminada
Funciones de conexión por Cuenta de AWS	0

Entidad	Cuota predeterminada
Para obtener más información, consulte Solicitud de un aumento de la cuota de la función de conexión.	
Tamaño máximo de la función de conexión Esta cuota no se puede ajustar. Para almacenar datos adicionales para las funciones de conexión, cree un almacén de valor de claves y agregue los pares clave-valor. Para obtener más información, consulte Amazon CloudFront KeyValueStore.	10 KB
Memoria máxima de la función de conexión	2 MB
Distribuciones asociadas a la misma función de conexión	100

Además de estas cuotas, existen algunas otras restricciones al utilizar funciones de CloudFront. Para obtener más información, consulte Asociación de una función de conexión de CloudFront.

Cuotas en almacenes de clave-valor

Entidad	Cuota predeterminada
Tamaño máximo de una clave en un par clave-valor	512 bytes
Tamaño máximo de un valor en un par clave-valor	1 KB
Número máximo de pares clave-valor que puede actualizar en una sola solicitud de API	50 claves o 3 MB de carga útil, lo que se alcance primero
El tamaño máximo de un almacén de clave-valor individual	5 MB
Número máximo de funciones a las que se puede asociar un único almacén de clave-valor	10
Número máximo de almacenes de clave-valor por función	1
Número máximo de almacenes de clave-valor por cuenta	50

Entidad	Cuota predeterminada
	Solicitar una ampliación de la cuota

Cuotas de Lambda@Edge

Cuotas generales

Entidad	Cuota predeterminada
Distribuciones por Cuenta de AWS que pueden tener funciones Lambda@Edge	500 Solicitar una ampliación de la cuota
Funciones Lambda@Edge por distribución	100 Solicitar una ampliación de la cuota
Ejecuciones simultáneas Notas • AWS Lambda administra las cuotas de simultaneidad para Lambda@Edge. Todas las funciones de Lambda en la Región de AWS comparten esta cuota. • Recomendamos que se revise la cuota de ejecuciones simultáneas en todas las Regiones de AWS de donde espere que procedan las solicitudes de los espectadores. Además, cada instancia de la función de Lambda@Edge puede atender hasta 10 solicitudes por segundo. El límite total de invocacio nes es 10 veces más alto que el límite de simultaneidad.	1000 (en cada Región de AWS) Solicitar una ampliación de la cuota

Entidad	Cuota predeterminada
Para obtener más información, consulte los siguientes temas de la Guía para desarrolladores de AWS Lambda: • Comprender el escalado de la función de Lambda • Solicitudes de la API de Lambda	
Distribuciones asociadas con la misma función	500
Tamaño comprimido máximo de una función Lambda y cualquier biblioteca incluida	50 MB
Solicitudes de Lambda@Edge por segundo (cada Región de AWS admitida). Para obtener más información, consulte Cuotas de simultaneidad en la Guía para desarrolladores de AWS Lambda.	10 000

Cuotas que difieren según el tipo de evento

Entidad	Tiempo de espera de los eventos de solicitud de lector y respuesta al lector de .	Eventos de solicitud al origen y respuesta del origen
Tamaño de memoria de función	128 MB	Igual que las cuotas de Lambda
Tiempo de espera de la función. La función puede realizar llamadas de red a recursos como buckets de Amazon S3, tablas de DynamoDB o instancias Amazon EC2 en Regiones de AWS.	30 segundos	30 segundos

Entidad	Tiempo de espera de los eventos de solicitud de lector y respuesta al lector de .	Eventos de solicitud al origen y respuesta del origen
Tamaño de una respuesta generada por una función Lambda, incluidos los encabezados y el cuerpo	40 KB	1 MB

Notas

- Para obtener una lista de cuotas adicionales de Lambda@Edge que se pueden aumentar desde Service Quotas, consulte Puntos de conexión y cuotas de Amazon CloudFront en la Guía para desarrolladores de Referencia general de AWS.
- Además de estas cuotas, existen algunas otras restricciones al utilizar las funciones de Lambda@Edge. Para obtener más información, consulte Restricciones de Lambda @Edge.

Cuotas en certificados SSL

Entidad	Cuota predeterminada
Certificados SSL por Cuenta de AWS cuando las solicitudes HTTPS se distribuyen mediante direcciones IP dedicadas (sin cuota si las solicitud es HTTPS se distribuyen mediante SNI) Para obtener más información, consulte Uso de HTTPS con CloudFront.	2 Solicitar una ampliación de la cuota
Certificados SSL que pueden asociarse a una distribución de CloudFront	1

Si su certificado SSL es específico para la comunicación HTTPS entre los lecotres y CloudFront, y si utilizó AWS Certificate Manager (ACM) o el almacén de certificados de IAM para aprovisionar

o importar su certificado, se aplicarán cuotas adicionales. Para obtener más información, consulte Cuotas al usar certificados SSL/TLS con CloudFront (solo HTTPS entre lectores y CloudFront).

También hay cuotas en cuanto a la cantidad de certificados SSL que puede importar a AWS Certificate Manager (ACM) o cargar en AWS Identity and Access Management (IAM). Para obtener más información, consulte Aumento de las cuotas de certificados SSL/TLS.

Cuotas de invalidaciones

Entidad	Cuota predeterminada
Invalidación de archivos: cantidad máxima de archivos permitidos en solicitudes de invalidación activas, excepto invalidaciones comodín Para obtener más información, consulte Invalidación de archivos para eliminar el contenido.	3000
Invalidación de archivos: cantidad máxima de anulaciones comodín activas permitidas	15
Invalidación de archivos: cantidad máxima de archivos que puede procesar una invalidación comodín	Sin cuota

Cuotas en grupos de claves

Entidad	Cuota predeterminada
Claves públicas en un solo grupo de claves	5 Solicitar una ampliación de la cuota
Grupos de claves asociados con un solo comportamiento de la caché	4 Solicitar una ampliación de la cuota
Grupos de claves por Cuenta de AWS	10

Entidad	Cuota predeterminada
	Solicitar una ampliación de la cuota
Distribuciones asociadas con un solo grupo de claves	100 Solicitar una ampliación de la cuota

Cuotas de conexiones WebSocket

Entidad	Cuota predeterminada
Tiempo de espera de respuesta de origen (tiempo de espera de inactividad)	10 minutos Si CloudFront no ha detectado ningún byte enviado desde el origen al cliente en los últimos 10 minutos, se presupone que la conexión esta inactiva y se cierra.

Cuotas de cifrado en el nivel de campo

Entidad	Cuota predeterminada
Longitud máxima del campo que se va a cifrar Para obtener más información, consulte Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial.	16 KB
Número máximo de campos en un cuerpo de la solicitud cuando está configurado el cifrado en el nivel de campo	10

Entidad	Cuota predeterminada
Longitud máxima de un cuerpo de la solicitud cuando está configurado el cifrado en el nivel de campo	1 MB
Número máximo de configuraciones de cifrado en el nivel de campo que pueden asociarse a una sola Cuenta de AWS	10
Número máximo de perfiles de cifrado en el nivel de campo que pueden asociarse a una sola Cuenta de AWS	10
Número máximo de claves públicas que se pueden añadir a una sola Cuenta de AWS	10
Número máximo de campos para cifrar que se pueden especificar en un perfil	10
Número máximo de distribuciones de CloudFront que pueden asociarse a una configuración de cifrado en el nivel de campo	20
Número máximo de asignaciones de perfil del argumento de consulta que se pueden incluir en una configuración de cifrado en el nivel de campo	5

Cuotas en cookies (configuración de caché heredada)

Estas cuotas se aplican a la configuración de caché heredada de CloudFront. Se recomienda utilizar una política de caché o una política de solicitud de origen en lugar de la configuración heredada.

Entidad	Cuota predeterminada
Cookies por comportamiento de la caché Para obtener más información, consulte Almacenamiento en caché de contenido en función de cookies.	10 Solicitar una ampliación de la cuota
Cantidad total de bytes en nombres de cookies (no es aplicable si configura CloudFront para reenviar todas las cookies al origen)	512 menos el número de cookies

Cuotas en cadenas de consulta (configuración de caché heredada)

Estas cuotas se aplican a la configuración de caché heredada de CloudFront. Se recomienda utilizar una política de caché o una política de solicitud de origen en lugar de la configuración heredada.

Entidad	Cuota predeterminada
Número máximo de caracteres en una cadena de consulta	128 caracteres
Número máximo de caracteres en total para todas las cadenas de consulta en el mismo parámetro	512 caracteres
Cadenas de consulta por comportamiento de la caché Para obtener más información, consulte Almacenamiento en caché de contenido en función de parámetros de cadenas de consulta.	10 Solicitar una ampliación de la cuota

Cuotas en encabezados

Entidad	Cuota predeterminada
Encabezados por comportamiento de la caché (configuración de caché heredada) Para obtener más información, consulte the section called “Almacena miento en caché de contenido en función de encabezados de solicitud”.	10 Solicitar una ampliación de la cuota
Reenvío de encabezados por comportamiento de caché	25 Solicitar una ampliación de la cuota
Encabezados personalizados: cantidad máxima de encabezados personalizados que puede configurar en CloudFront para que el servicio los agregue a solicitudes de origen Para obtener más información, consulte the section called “Añadido de encabezados personalizados a solicitudes de origen”.	30 Solicitar una ampliación de la cuota

Entidad	Cuota predeterminada
Encabezados personalizados: cantidad máxima de encabezados personalizados que puede agregar a una política de encabezados de respuesta	10 Solicitar una ampliación de la cuota
Encabezados personalizados: longitud máxima de un nombre de encabezado	256 caracteres
Encabezados personalizados: longitud máxima de un valor de encabezado	1,783 caracteres
Encabezados personalizados: longitud máxima de todos los nombres y valores de encabezados combinados	10 240 caracteres
Longitud máxima del valor del encabezado `Content-Security-Policy`	1783 caracteres Solicitar una ampliación de la cuota
Longitud máxima del valor de un encabezado `CORS (Access-Control-Allow-Origin)`	1783 caracteres

Cuotas en distribuciones de varios inquilinos

Entidad	Cuota predeterminada
Cantidad máxima de inquilinos de distribución por Cuenta de AWS	10 000 Solicitar una ampliación de la cuota
Cantidad máxima de distribuciones de varios inquilinos por Cuenta de AWS	20 Solicitar una ampliación de la cuota
Cantidad máxima de grupos de conexión por Cuenta de AWS	100

Entidad	Cuota predeterminada
	Solicitar una ampliación de la cuota
Cantidad máxima de alias por inquilino de distribución	100 Solicitar una ampliación de la cuota
Cantidad máxima de parámetros por inquilino de distribución	5 Solicitar una ampliación de la cuota
Cantidad máxima de parámetros por distribución de varios inquilinos	5 Solicitar una ampliación de la cuota
Cantidad máxima de parámetros en un campo en una distribución de varios inquilinos	2 Solicitar una ampliación de la cuota
Cantidad máxima de grupos de conexiones por lista de IP estáticas de Anycast	5 Solicitar una ampliación de la cuota

Para obtener más información acerca de las distribuciones de varios inquilinos, consulte Introducción al funcionamiento de las distribuciones de varios inquilinos.

Información relacionada

Para obtener más información, consulte Puntos de conexión de Amazon CloudFront y cuotas en Referencia general de AWS.

Ejemplos de código para CloudFront usando SDK de AWS

Los siguientes ejemplos de código indican cómo utilizar CloudFront con un kit de desarrollo de software (SDK) de AWS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- Ejemplos básicos de CloudFront mediante los AWS SDK
  - Acciones para CloudFront usando SDK de AWS
    - Uso de CreateDistribution con un AWS SDK o una CLI
    - Uso de CreateFunction con un SDK de AWS
    - Utilizar CreateInvalidation con una CLI
    - Uso de CreateKeyGroup con un SDK de AWS
    - Uso de CreatePublicKey con un SDK de AWS o la CLI
    - Uso de DeleteDistribution con un SDK de AWS o la CLI
    - Utilizar GetCloudFrontOriginAccessIdentity con una CLI
    - Utilizar GetCloudFrontOriginAccessIdentityConfig con una CLI
    - Utilizar GetDistribution con una CLI
    - Uso de GetDistributionConfig con un SDK de AWS o la CLI
    - Utilizar ListCloudFrontOriginAccessIdentities con una CLI
    - Uso de ListDistributions con un SDK de AWS o la CLI
    - Uso de UpdateDistribution con un SDK de AWS o la CLI
- Escenarios para CloudFront usando SDK de AWS
  - Creación de un SDK de recursos para administradores de AWS SaaS

- Eliminar los recursos de firma de CloudFront usando un SDK de AWS
- Introducción a una distribución de CloudFront básica con la CLI
- Crear URL y cookies firmadas usando un SDK de AWS
- Ejemplos de CloudFront Functions para CloudFront
  - Añadir encabezados de seguridad HTTP a un evento de respuesta del visor de CloudFront Functions
  - Añadir un encabezado CORS a un evento de respuesta del visor de CloudFront Functions
  - Añadir un encabezado de control de caché a un evento de respuesta del visor de CloudFront Functions
  - Agregar un encabezado True-Client-IP a un evento de solicitud de visor de CloudFront Functions
  - Añadir un encabezado True-Client-IP a un evento de solicitud del visor de CloudFront Functions
  - Agregar index.html a las URL de solicitud sin un nombre de archivo en un evento de solicitud del visor de CloudFront Functions
  - Normalizar los parámetros de la cadena de consulta en una solicitud de visor de CloudFront Functions
  - Redirigir a una nueva URL en un evento de solicitud de visor de CloudFront Functions
  - Reescribir el URI de una solicitud en función de la configuración de KeyValueStore para un evento de solicitud de un visor de CloudFront Functions
  - Dirección de las solicitudes a un origen más cercano al espectador en un evento de solicitud de espectador de CloudFront Functions
  - Uso de pares clave-valor en una solicitud de visor de CloudFront Functions
  - Validar un token simple en una solicitud de visor de CloudFront Functions

Ejemplos básicos de CloudFront mediante los AWS SDK

Los siguientes ejemplos de código muestran cómo utilizar los aspectos básicos de Amazon CloudFront con los AWS SDK.

Ejemplos

- Acciones para CloudFront usando SDK de AWS
  - Uso de CreateDistribution con un AWS SDK o una CLI
  - Uso de CreateFunction con un SDK de AWS

- Utilizar CreateInvalidation con una CLI
- Uso de CreateKeyGroup con un SDK de AWS
- Uso de CreatePublicKey con un SDK de AWS o la CLI
- Uso de DeleteDistribution con un SDK de AWS o la CLI
- Utilizar GetCloudFrontOriginAccessIdentity con una CLI
- Utilizar GetCloudFrontOriginAccessIdentityConfig con una CLI
- Utilizar GetDistribution con una CLI
- Uso de GetDistributionConfig con un SDK de AWS o la CLI
- Utilizar ListCloudFrontOriginAccessIdentities con una CLI
- Uso de ListDistributions con un SDK de AWS o la CLI
- Uso de UpdateDistribution con un SDK de AWS o la CLI

Acciones para CloudFront usando SDK de AWS

Los siguientes ejemplos de código muestran cómo realizar acciones de CloudFront individuales con AWS SDK. En cada ejemplo se incluye un enlace a GitHub, con instrucciones de configuración y ejecución del código.

Estos fragmentos llaman a la API de CloudFront y son partes de código de programas más grandes que deben ejecutarse en contexto. Puede ver las acciones en contexto en Escenarios para CloudFront usando SDK de AWS.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para ver una lista completa, consulte la Referencia de la API de Amazon CloudFront.

Ejemplos

- Uso de CreateDistribution con un AWS SDK o una CLI
- Uso de CreateFunction con un SDK de AWS
- Utilizar CreateInvalidation con una CLI
- Uso de CreateKeyGroup con un SDK de AWS
- Uso de CreatePublicKey con un SDK de AWS o la CLI
- Uso de DeleteDistribution con un SDK de AWS o la CLI
- Utilizar GetCloudFrontOriginAccessIdentity con una CLI
- Utilizar GetCloudFrontOriginAccessIdentityConfig con una CLI

- Utilizar GetDistribution con una CLI
- Uso de GetDistributionConfig con un SDK de AWS o la CLI
- Utilizar ListCloudFrontOriginAccessIdentities con una CLI
- Uso de ListDistributions con un SDK de AWS o la CLI
- Uso de UpdateDistribution con un SDK de AWS o la CLI

Uso de **`CreateDistribution`** con un AWS SDK o una CLI

Los siguientes ejemplos de código muestran cómo utilizar `CreateDistribution`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en los siguientes ejemplos de código:

- Creación de una distribución de varios inquilinos y un inquilino de distribución
- Introducción a CloudFront

CLI

AWS CLI

Ejemplo 1: para crear una distribución de CloudFront

En el siguiente ejemplo de `create-distribution` se crea una distribución para un bucket de S3 denominado `amzn-s3-demo-bucket` y también se especifica `index.html` como el objeto raíz predeterminado mediante argumentos de línea de comandos.

```
aws cloudfront create-distribution \
    --origin-domain-name amzn-s3-demo-bucket.s3.amazonaws.com \
    --default-root-object index.html
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EMLARXS9EXAMPLE",
    "ETag": "E9LHASXEXAMPLE",
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
```

```
        "Status": "InProgress",
        "LastModifiedTime": "2019-11-22T00:55:15.705Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
```

```
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
```

```
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

Ejemplo 2: creación de una distribución de CloudFront mediante un archivo JSON

En el siguiente ejemplo de `create-distribution` se crea una distribución para un bucket de S3 denominado `amzn-s3-demo-bucket` y también se especifica `index.html` como objeto raíz predeterminado mediante un archivo JSON.

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

Contenido de `dist-config.json`:

```
{
    "CallerReference": "cli-example",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
```

```
                "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
```

```
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": true,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
```

```
}
```

Consulte el ejemplo 1 para ver una salida de muestra.

Ejemplo 3: creación de una distribución de varios inquilinos de CloudFront con un certificado

En el siguiente ejemplo de `create-distribution` se crea una distribución de CloudFront con compatibilidad para varios inquilinos y se especifica un certificado TLS.

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

Contenido de `dist-config.json`:

```
{
    "CallerReference": "cli-example-with-cert",
    "Comment": "CLI example distribution",
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "DomainName": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "OriginPath": "/{{tenantName}}",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
        "ViewerProtocolPolicy": "allow-all",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["HEAD", "GET"],
            "CachedMethods": {
                "Quantity": 2,
```

```
                "Items": ["HEAD", "GET"]
            }
        }
    },
    "Enabled": true,
    "ViewerCertificate": {
        "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/191306a1-db01-49ca-90ef-fc414ee5dabc",
        "SSLSupportMethod": "sni-only"
    },
    "HttpVersion": "http2",
    "ConnectionMode": "tenant-only",
    "TenantConfig": {
        "ParameterDefinitions": [
            {
                "Name": "tenantName",
                "Definition": {
                    "StringSchema": {
                        "Comment": "tenantName parameter",
                        "DefaultValue": "root",
                        "Required": false
                    }
                }
            }
        ]
    }
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution/
E1HVIAU7UABC",
    "ETag": "E20LT7R1BABC",
    "Distribution": {
        "Id": "E1HVIAU7U12ABC",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/E1HVIAU7U12ABC",
        "Status": "InProgress",
        "LastModifiedTime": "2025-07-10T20:33:31.117000+00:00",
        "InProgressInvalidationBatches": 0,
        "DomainName": "example.com",
        "ActiveTrustedSigners": {
            "Enabled": false,
```

```
            "Quantity": 0
        },
        "ActiveTrustedKeyGroups": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example-with-cert",
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                        "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                        "OriginPath": "/{{tenantName}}",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
                        "ConnectionTimeout": 10,
                        "OriginShield": {
                            "Enabled": false
                        },
                        "OriginAccessControlId": ""
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                "TrustedKeyGroups": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "AllowedMethods": {
```

```
                    "Quantity": 2,
                    "Items": ["HEAD", "GET"],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": ["HEAD", "GET"]
                    }
                },
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": "",
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
                "GrpcConfig": {
                    "Enabled": false
                }
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "CLI example distribution",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": false,
                "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/1954f095-11b6-4daf-9952-0c308a00abc",
                "SSLSupportMethod": "sni-only",
                "MinimumProtocolVersion": "TLSv1.2_2021",
                "Certificate": "arn:aws:acm:us-
east-1:123456789012:certificate/1954f095-11b6-4daf-9952-0c308a00abc",
                "CertificateSource": "acm"
            },
```

```
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "TenantConfig": {
                "ParameterDefinitions": [
                    {
                        "Name": "tenantName",
                        "Definition": {
                            "StringSchema": {
                                "Comment": "tenantName parameter",
                                "DefaultValue": "root",
                                "Required": false
                            }
                        }
                    }
                ]
            },
            "ConnectionMode": "tenant-only"
        }
    }
}
```

Para obtener más información, consulte Trabajo con distribuciones en la Guía para desarrolladores de Amazon CloudFront.

Ejemplo 4: creación de una distribución de varios inquilinos de CloudFront sin un certificado

En el siguiente ejemplo de `create-distribution` se crea una distribución de CloudFront con compatibilidad para varios inquilinos, pero sin un certificado TLS.

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

Contenido de `dist-config.json`:

```
{
    "CallerReference": "cli-example",
    "Comment": "CLI example distribution",
```

```
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "DomainName": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "OriginPath": "/{{tenantName}}",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
        "ViewerProtocolPolicy": "allow-all",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        }
    },
    "Enabled": true,
    "HttpVersion": "http2",
    "ConnectionMode": "tenant-only",
    "TenantConfig": {
        "ParameterDefinitions": [
            {
                "Name": "tenantName",
                "Definition": {
```

```
                    "StringSchema": {
                        "Comment": "tenantName parameter",
                        "DefaultValue": "root",
                        "Required": false
                    }
                }
            }
        ]
    }
}
```

Salida:

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution/
E2GJ5J9QN12ABC",
    "ETag": "E37YLVVQIABC",
    "Distribution": {
        "Id": "E2GJ5J9QNABC",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/E2GJ5J9QN12ABC",
        "Status": "InProgress",
        "LastModifiedTime": "2025-07-10T20:35:20.565000+00:00",
        "InProgressInvalidationBatches": 0,
        "DomainName": "example.com",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ActiveTrustedKeyGroups": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example-no-cert",
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                        "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                        "OriginPath": "/{{tenantName}}",
```

```
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
                        "ConnectionTimeout": 10,
                        "OriginShield": {
                            "Enabled": false
                        },
                        "OriginAccessControlId": ""
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                "TrustedKeyGroups": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
```

```
                "FunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": "",
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
                "GrpcConfig": {
                    "Enabled": false
                }
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "CLI example distribution",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "SSLSupportMethod": "sni-only",
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "TenantConfig": {
                "ParameterDefinitions": [
                    {
                        "Name": "tenantName",
                        "Definition": {
                            "StringSchema": {
                                "Comment": "tenantName parameter",
```

```
                                "DefaultValue": "root",
                                "Required": false
                            }
                        }
                    }
                ]
            },
            "ConnectionMode": "tenant-only"
        }
    }
}
```

Para obtener más información, consulte Configuración de distribuciones en la Guía para desarrolladores de Amazon CloudFront.

- Para obtener información sobre la API, consulte CreateDistribution en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

El siguiente ejemplo utiliza un bucket de Amazon Simple Storage Service (Amazon S3) como un origen de contenido.

Tras crear la distribución, el código crea un CloudFrontWaiter para esperar a que se implemente la distribución antes de devolverla.

```
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;
        }
}
```

- Para obtener información sobre la API, consulte CreateDistribution en la Referencia de la API de AWS SDK for Java 2.x.

PowerShell

Herramientas para PowerShell V4

Ejemplo 1: Crea una distribución básica de CloudFront, configurada con registro y almacenamiento en caché.

```
$origin = New-Object Amazon.CloudFront.Model.Origin
$origin.DomainName = "amzn-s3-demo-bucket.s3.amazonaws.com"
$origin.Id = "UniqueOrigin1"
$origin.S3OriginConfig = New-Object Amazon.CloudFront.Model.S3OriginConfig
```

```
$origin.S3OriginConfig.OriginAccessIdentity = ""
New-CFDistribution `
      -DistributionConfig_Enabled $true `
      -DistributionConfig_Comment "Test distribution" `
      -Origins_Item $origin `
      -Origins_Quantity 1 `
      -Logging_Enabled $true `
      -Logging_IncludeCookie $true `
      -Logging_Bucket amzn-s3-demo-logging-bucket.s3.amazonaws.com `
      -Logging_Prefix "help/" `
      -DistributionConfig_CallerReference Client1 `
      -DistributionConfig_DefaultRootObject index.html `
      -DefaultCacheBehavior_TargetOriginId $origin.Id `
      -ForwardedValues_QueryString $true `
      -Cookies_Forward all `
      -WhitelistedNames_Quantity 0 `
      -TrustedSigners_Enabled $false `
      -TrustedSigners_Quantity 0 `
      -DefaultCacheBehavior_ViewerProtocolPolicy allow-all `
      -DefaultCacheBehavior_MinTTL 1000 `
      -DistributionConfig_PriceClass "PriceClass_All" `
      -CacheBehaviors_Quantity 0 `
      -Aliases_Quantity 0
```

- Para obtener información sobre la API, consulte CreateDistribution en la Referencia de Cmdlet de Herramientas de AWS para PowerShell (V4).

Herramientas para PowerShell V5

Ejemplo 1: Crea una distribución básica de CloudFront, configurada con registro y almacenamiento en caché.

```
$origin = New-Object Amazon.CloudFront.Model.Origin
$origin.DomainName = "amzn-s3-demo-bucket.s3.amazonaws.com"
$origin.Id = "UniqueOrigin1"
$origin.S3OriginConfig = New-Object Amazon.CloudFront.Model.S3OriginConfig
$origin.S3OriginConfig.OriginAccessIdentity = ""
New-CFDistribution `
      -DistributionConfig_Enabled $true `
      -DistributionConfig_Comment "Test distribution" `
      -Origins_Item $origin `
      -Origins_Quantity 1 `
      -Logging_Enabled $true `
      -Logging_IncludeCookie $true `
```

```
        -Logging_Bucket amzn-s3-demo-logging-bucket.s3.amazonaws.com `
        -Logging_Prefix "help/" `
        -DistributionConfig_CallerReference Client1 `
        -DistributionConfig_DefaultRootObject index.html `
        -DefaultCacheBehavior_TargetOriginId $origin.Id `
        -ForwardedValues_QueryString $true `
        -Cookies_Forward all `
        -WhitelistedNames_Quantity 0 `
        -TrustedSigners_Enabled $false `
        -TrustedSigners_Quantity 0 `
        -DefaultCacheBehavior_ViewerProtocolPolicy allow-all `
        -DefaultCacheBehavior_MinTTL 1000 `
        -DistributionConfig_PriceClass "PriceClass_All" `
        -CacheBehaviors_Quantity 0 `
        -Aliases_Quantity 0
```

- Para obtener detalles de la API, consulte CreateDistribution en la Referencia de cmdlets de Herramientas de AWS para PowerShell (V5).

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`CreateFunction`** con un SDK de AWS

En el siguiente ejemplo de código, se muestra cómo usar `CreateFunction`.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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 "";
    }
}
```

- Para obtener información sobre la API, consulte CreateFunction en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`CreateInvalidation`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `CreateInvalidation`.

CLI

AWS CLI

Creación de una invalidación para una distribución de CloudFront

En el siguiente ejemplo de `create-invalidation` se crea una invalidación para los archivos indicados en la distribución de CloudFront especificada:

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --paths "/example-path/example-file.jpg" "/example-path/example-file2.png"
```

Salida:

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

En el ejemplo anterior, la CLI de AWS generó automáticamente un `CallerReference` aleatorio. Para especificar su propia `CallerReference` o para evitar pasar los parámetros de invalidación como argumentos de la línea de comandos, puede utilizar un archivo JSON.

En el siguiente ejemplo se crea una invalidación para dos archivos y se proporcionan los parámetros de invalidación en un archivo JSON denominado `inv-batch.json`:

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --invalidation-batch file://inv-batch.json
```

Contenido de `inv-batch.json`:

```
{
    "Paths": {
        "Quantity": 2,
        "Items": [
            "/example-path/example-file.jpg",
            "/example-path/example-file2.png"
        ]
    },
    "CallerReference": "cli-example"
}
```

Salida:

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

- Para obtener información sobre la API, consulte CreateInvalidation en la Referencia de comandos de la AWS CLI.

PowerShell

Herramientas para PowerShell V4

Ejemplo 1: En este ejemplo se crea una nueva invalidación en una distribución con un ID de EXAMPLENSTXAXE. CallerReference es un identificador único elegido por el usuario; en este caso, se utiliza una marca temporal que representa el 15 de mayo de 2019 a las 9:00 h. La variable $Paths almacena tres rutas a archivos multimedia y de imagen que el usuario no desea que formen parte de la memoria caché de la distribución. El valor del parámetro -Paths_Quantity es el número total de rutas especificadas en el parámetro -Paths_Item.

```
$Paths = "/images/*.gif", "/images/image1.jpg", "/videos/*.mp4"
New-CFInvalidation -DistributionId "EXAMPLENSTXAXE" -
InvalidationBatch_CallerReference 20190515090000 -Paths_Item $Paths -
Paths_Quantity 3
```

Salida:

```
Invalidation                        Location

------------                        --------

Amazon.CloudFront.Model.Invalidation https://cloudfront.amazonaws.com/2018-11-05/
distribution/EXAMPLENSTXAXE/invalidation/EXAMPLE8NOK9H
```

- Para obtener información sobre la API, consulte CreateDistribution en la Referencia de Cmdlet de Herramientas de AWS para PowerShell (V4).

Herramientas para PowerShell V5

Ejemplo 1: En este ejemplo se crea una nueva invalidación en una distribución con un ID de EXAMPLENSTXAXE. CallerReference es un identificador único elegido por el usuario; en este caso, se utiliza una marca temporal que representa el 15 de mayo de 2019 a las 9:00 h. La variable $Paths almacena tres rutas a archivos multimedia y de imagen que el usuario no desea que formen parte de la memoria caché de la distribución. El valor del parámetro -Paths_Quantity es el número total de rutas especificadas en el parámetro -Paths_Item.

```
$Paths = "/images/*.gif", "/images/image1.jpg", "/videos/*.mp4"
New-CFInvalidation -DistributionId "EXAMPLENSTXAXE" -
InvalidationBatch_CallerReference 20190515090000 -Paths_Item $Paths -
Paths_Quantity 3
```

Salida:

```
Invalidation                        Location

------------                        --------

Amazon.CloudFront.Model.Invalidation https://cloudfront.amazonaws.com/2018-11-05/
distribution/EXAMPLENSTXAXE/invalidation/EXAMPLE8NOK9H
```

- Para obtener detalles de la API, consulte CreateInvalidation en Referencia de cmdlets de Herramientas de AWS para PowerShell (V5).

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`CreateKeyGroup`** con un SDK de AWS

En el siguiente ejemplo de código, se muestra cómo usar `CreateKeyGroup`.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Un grupo de claves requiere al menos una clave pública que se utilice para verificar las URL o cookies firmadas.

```
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;
    }
}
```

- Para obtener información sobre la API, consulte CreateKeyGroup en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`CreatePublicKey`** con un SDK de AWS o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `CreatePublicKey`.

CLI

AWS CLI

Para crear una clave pública de CloudFront

En el siguiente ejemplo se crea una clave pública de CloudFront proporcionando los parámetros en un archivo JSON denominado `pub-key-config.json`. Para poder usar este comando, debe tener una clave pública codificada en PEM. Para obtener más información, consulte Crear un par de claves RSA en la Guía para desarrolladores de Amazon CloudFront.

```
aws cloudfront create-public-key \
    --public-key-config file://pub-key-config.json
```

El archivo `pub-key-config.json` es un documento JSON en la carpeta actual que contiene lo siguiente. Tenga en cuenta que la clave pública está codificada con el 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"
}
```

Salida:

```
{
    "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"
        }
```

```
    }
}
```

- Para obtener información sobre la API, consulte CreatePublicKey en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

El siguiente ejemplo de código lee una clave pública y la carga en 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);
        }
    }
}
```

- Para obtener información sobre la API, consulte CreatePublicKey en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DeleteDistribution`** con un SDK de AWS o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DeleteDistribution`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a CloudFront

CLI

AWS CLI

Eliminación de una distribución de CloudFront

En el siguiente ejemplo se elimina la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`. Antes de eliminar una distribución, debe deshabilitarla. Para deshabilitar una distribución, utilice el comando update-distribution. Para obtener más información, consulte los ejemplos de update-distribution.

Cuando una distribución está deshabilitada, puede eliminarla. Para eliminar una distribución, debe usar la opción `--if-match` para proporcionar la `ETag` de la distribución. Para obtener la `ETag`, utilice el comando get-distribution o get-distribution-config.

```
aws cloudfront delete-distribution \
    --id EDFDVBD6EXAMPLE \
    --if-match E2QWRUHEXAMPLE
```

Cuando tenga éxito, este comando no tiene salida.

- Para obtener información sobre la API, consulte DeleteDistribution en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

El siguiente ejemplo de código actualiza una distribución a deshabilitada, utiliza un esperador que espera a que se implemente el cambio y, a continuación, elimina la distribución.

```
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);
                }
        }
}
```

- Para obtener detalles sobre la API, consulte DeleteDistribution en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`GetCloudFrontOriginAccessIdentity`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetCloudFrontOriginAccessIdentity`.

CLI

AWS CLI

Obtención de la identidad de acceso de origen de CloudFront

En el siguiente ejemplo se obtiene la identidad de acceso de origen (OAI) de CloudFront con el ID `E74FTE3AEXAMPLE`, incluida su `ETag` y el ID canónico de S3 asociado. El ID de OAI se devuelve en la salida de los comandos create-cloud-front-origin-access-identity y list-cloud-front-origin-access-identities.

```
aws cloudfront get-cloud-front-origin-access-identity --id E74FTE3AEXAMPLE
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentity": {
        "Id": "E74FTE3AEXAMPLE",
        "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
        "CloudFrontOriginAccessIdentityConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example OAI"
        }
    }
}
```

- Para obtener información sobre la API, consulte GetCloudFrontOriginAccessIdentity en la Referencia de comandos de la AWS CLI.

PowerShell

Herramientas para PowerShell V4

Ejemplo 1: Este ejemplo devuelve una identidad de acceso de origen específica de Amazon CloudFront, especificada mediante el parámetro -Id. Aunque el parámetro -Id no es obligatorio, si no lo especifica, no se devolverá ningún resultado.

```
Get-CFCloudFrontOriginAccessIdentity -Id E3XXXXXXXXXXRT
```

Salida:

```
      CloudFrontOriginAccessIdentityConfig    Id
     S3CanonicalUserId
```

```
     -----------------------------------    --
    -----------------
     Amazon.CloudFront.Model.CloudFrontOr... E3XXXXXXXXXXRT
    4b6e...
```

- Para obtener información sobre la API, consulte GetCloudFrontOriginAccessIdentity en la Referencia de Cmdlet de Herramientas de AWS para PowerShell (V4).

Herramientas para PowerShell V5

Ejemplo 1: Este ejemplo devuelve una identidad de acceso de origen específica de Amazon CloudFront, especificada mediante el parámetro -Id. Aunque el parámetro -Id no es obligatorio, si no lo especifica, no se devolverá ningún resultado.

```
Get-CFCloudFrontOriginAccessIdentity -Id E3XXXXXXXXXXRT
```

Salida:

```
     CloudFrontOriginAccessIdentityConfig    Id
    S3CanonicalUserId
     -----------------------------------    --
    -----------------
     Amazon.CloudFront.Model.CloudFrontOr... E3XXXXXXXXXXRT
    4b6e...
```

- Para obtener detalles sobre la API, consulte GetCloudFrontOriginAccessIdentity en la Referencia de cmdlets de Herramientas de AWS para PowerShell (V5).

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`GetCloudFrontOriginAccessIdentityConfig`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetCloudFrontOriginAccessIdentityConfig`.

CLI

AWS CLI

Obtención de una configuración de identidad de acceso de origen de CloudFront

En el siguiente ejemplo se obtienen metadatos sobre la identidad de acceso de origen (OAI) con el ID `E74FTE3AEXAMPLE`, incluida su `ETag`. El ID de OAI se devuelve en la salida de los comandos create-cloud-front-origin-access-identity y list-cloud-front-origin-access-identities.

```
aws cloudfront get-cloud-front-origin-access-identity-config --id E74FTE3AEXAMPLE
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentityConfig": {
        "CallerReference": "cli-example",
        "Comment": "Example OAI"
    }
}
```

- Para obtener información sobre la API, consulte GetCloudFrontOriginAccessIdentityConfig en la Referencia de comandos de la AWS CLI.

PowerShell

Herramientas para PowerShell V4

Ejemplo 1: Este ejemplo devuelve información de configuración sobre una única identidad de acceso de origen de Amazon CloudFront, especificada mediante el parámetro -Id. Se producen errores si no se especifica ningún parámetro -Id..

```
Get-CFCloudFrontOriginAccessIdentityConfig -Id E3XXXXXXXXXXRT
```

Salida:

```
      CallerReference                                            Comment
      ---------------                                            -------
      mycallerreference: 2/1/2011 1:16:32 PM                     Caller
 reference: 2/1/2011 1:16:32 PM
```

- Para obtener información sobre la API, consulte GetCloudFrontOriginAccessIdentityConfig en la Referencia de Cmdlet de Herramientas de AWS para PowerShell (V4).

Herramientas para PowerShell V5

Ejemplo 1: Este ejemplo devuelve información de configuración sobre una única identidad de acceso de origen de Amazon CloudFront, especificada mediante el parámetro -Id. Se producen errores si no se especifica ningún parámetro -Id..

```
Get-CFCloudFrontOriginAccessIdentityConfig -Id E3XXXXXXXXXXRT
```

Salida:

```
     CallerReference                                            Comment
     ---------------                                            -------
     mycallerreference: 2/1/2011 1:16:32 PM                     Caller
reference: 2/1/2011 1:16:32 PM
```

- Para obtener detalles de la API, consulte GetCloudFrontOriginAccessIdentityConfig en la Referencia de cmdlets de Herramientas de AWS para PowerShell (V5).

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`GetDistribution`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetDistribution`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a CloudFront

CLI

AWS CLI

Obtención de una distribución de CloudFront

En el siguiente ejemplo de `get-distribution`, se obtiene la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`, incluida su `ETag`. El ID de distribución se devuelve en los comandos create-distribution y list-distributions.

```
aws cloudfront get-distribution \
    --id EDFDVBD6EXAMPLE
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "Distribution": {
        "Id": "EDFDVBD6EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE",
        "Status": "Deployed",
        "LastModifiedTime": "2019-12-04T23:35:41.433Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
```

```
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
```

```
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Para obtener información sobre la API, consulte GetDistribution en la Referencia de comandos de la AWS CLI.

PowerShell

Herramientas para PowerShell V4

Ejemplo 1: Recupera la información de una distribución específica.

```
Get-CFDistribution -Id EXAMPLE0000ID
```

- Para obtener información sobre la API, consulte GetDistribution en la Referencia de cmdlet de Herramientas de AWS para PowerShell (V4).

Herramientas para PowerShell V5

Ejemplo 1: Recupera la información de una distribución específica.

```
Get-CFDistribution -Id EXAMPLE0000ID
```

- Para obtener detalles de la API, consulte GetDistribution en la Referencia de cmdlets de Herramientas de AWS para PowerShell (V5).

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`GetDistributionConfig`** con un SDK de AWS o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `GetDistributionConfig`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a CloudFront

CLI

AWS CLI

Obtención de la configuración de distribución de CloudFront

En el siguiente ejemplo se obtienen metadatos sobre la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`, incluida su `ETag`. El ID de distribución se devuelve en los comandos create-distribution y list-distributions.

```
aws cloudfront get-distribution-config \
    --id EDFDVBD6EXAMPLE
```

Salida:

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "DistributionConfig": {
        "CallerReference": "cli-example",
        "Aliases": {
            "Quantity": 0
        },
        "DefaultRootObject": "index.html",
        "Origins": {
            "Quantity": 1,
            "Items": [
                {
                    "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                    "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                    "OriginPath": "",
                    "CustomHeaders": {
                        "Quantity": 0
                    },
                    "S3OriginConfig": {
                        "OriginAccessIdentity": ""
                    }
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 0
                },
                "QueryStringCacheKeys": {
                    "Quantity": 0
                }
            },
            "TrustedSigners": {
```

```
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "SmoothStreaming": false,
            "DefaultTTL": 86400,
            "MaxTTL": 31536000,
            "Compress": false,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": ""
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
        "PriceClass": "PriceClass_All",
        "Enabled": true,
        "ViewerCertificate": {
```

```
            "CloudFrontDefaultCertificate": true,
            "MinimumProtocolVersion": "TLSv1",
            "CertificateSource": "cloudfront"
        },
        "Restrictions": {
            "GeoRestriction": {
                "RestrictionType": "none",
                "Quantity": 0
            }
        },
        "WebACLId": "",
        "HttpVersion": "http2",
        "IsIPV6Enabled": true
    }
}
```

- Para obtener información sobre la API, consulte GetDistributionConfig en la Referencia de comandos de la AWS CLI.

PowerShell

Herramientas para PowerShell V4

Ejemplo 1: Recupera la configuración de una distribución específica.

```
Get-CFDistributionConfig -Id EXAMPLE0000ID
```

- Para obtener información sobre la API, consulte GetDistributionConfig en la Referencia de Cmdlets de Herramientas de AWS para PowerShell (V4).

Herramientas para PowerShell V5

Ejemplo 1: Recupera la configuración de una distribución específica.

```
Get-CFDistributionConfig -Id EXAMPLE0000ID
```

- Para obtener detalles de la API, consulte GetDistributionConfig en la Referencia de cmdlets de Herramientas de AWS para PowerShell (V5).

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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!")
```

- Para obtener información sobre la API, consulte GetDistributionConfig en la Referencia de la API de AWS SDK para Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **`ListCloudFrontOriginAccessIdentities`** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `ListCloudFrontOriginAccessIdentities`.

CLI

AWS CLI

Enumeración de las identidades de acceso de origen de CloudFront

En el siguiente ejemplo se obtiene una lista de las identidades de acceso de origen (OAI) de CloudFront de la cuenta de AWS:

```
aws cloudfront list-cloud-front-origin-access-identities
```

Salida:

```
{
    "CloudFrontOriginAccessIdentityList": {
        "Items": [
            {
                "Id": "E74FTE3AEXAMPLE",
                "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
                "Comment": "Example OAI"
            },
```

```
            {
                "Id": "EH1HDMBEXAMPLE",
                "S3CanonicalUserId":
 "1489f6f2e6faacaae7ff64c4c3e6956c24f78788abfc1718c3527c263bf7a17EXAMPLE",
                "Comment": "Test OAI"
            },
            {
                "Id": "E2X2C9TEXAMPLE",
                "S3CanonicalUserId":
 "cbfeebb915a64749f9be546a45b3fcfd3a31c779673c13c4dd460911ae402c2EXAMPLE",
                "Comment": "Example OAI #2"
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte ListCloudFrontOriginAccessIdentities en la Referencia de comandos de la AWS CLI.

PowerShell

Herramientas para PowerShell V4

Ejemplo 1: Este ejemplo devuelve una lista de identidades de acceso de origen de Amazon CloudFront. Como el parámetro -MaxItem especifica un valor de 2, los resultados incluyen dos identidades.

```
Get-CFCloudFrontOriginAccessIdentityList -MaxItem 2
```

Salida:

```
IsTruncated : True
Items       : {E326XXXXXXXXXT, E1YWXXXXXXX9B}
Marker      :
MaxItems    : 2
NextMarker  : E1YXXXXXXXXX9B
Quantity    : 2
```

- Para obtener información sobre la API, consulte ListCloudFrontOriginAccessIdentities en la Referencia de Cmdlet de Herramientas de AWS para PowerShell (V4).

Herramientas para PowerShell V5

Ejemplo 1: Este ejemplo devuelve una lista de identidades de acceso de origen de Amazon CloudFront. Como el parámetro -MaxItem especifica un valor de 2, los resultados incluyen dos identidades.

```
Get-CFCloudFrontOriginAccessIdentityList -MaxItem 2
```

Salida:

```
IsTruncated : True
Items       : {E326XXXXXXXXXT, E1YWXXXXXXX9B}
Marker      :
MaxItems    : 2
NextMarker  : E1YXXXXXXXXX9B
Quantity    : 2
```

- Para obtener detalles de la API, consulte ListCloudFrontOriginAccessIdentities en la Referencia de cmdlets de Herramientas de AWS para PowerShell (V5).

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`ListDistributions`** con un SDK de AWS o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `ListDistributions`.

CLI

AWS CLI

Obtención de una lista de las distribuciones de CloudFront

En el siguiente ejemplo, se obtiene una lista de las distribuciones de CloudFront de la cuenta de AWS.

```
aws cloudfront list-distributions
```

Salida:

```
{
    "DistributionList": {
        "Items": [
            {
                "Id": "E23YS8OEXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
E23YS8OEXAMPLE",
                "Status": "Deployed",
                "LastModifiedTime": "2024-08-05T18:23:40.375000+00:00",
                "DomainName": "abcdefgh12ijk.cloudfront.net",
                "Aliases": {
                    "Quantity": 0
                },
                "Origins": {
                    "Quantity": 1,
                    "Items": [
                        {
                            "Id": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                            "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                            "OriginPath": "",
                            "CustomHeaders": {
                                "Quantity": 0
                            },
                            "S3OriginConfig": {
                                "OriginAccessIdentity": ""
                            },
                            "ConnectionAttempts": 3,
                            "ConnectionTimeout": 10,
                            "OriginShield": {
                                "Enabled": false
                            },
                            "OriginAccessControlId": "EIAP8PEXAMPLE"
                        }
                    ]
                },
                "OriginGroups": {
                    "Quantity": 0
                },
                "DefaultCacheBehavior": {
                    "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
```

```
                    "TrustedSigners": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "TrustedKeyGroups": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "ViewerProtocolPolicy": "allow-all",
                    "AllowedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ],
                        "CachedMethods": {
                            "Quantity": 2,
                            "Items": [
                                "HEAD",
                                "GET"
                            ]
                        }
                    },
                    "SmoothStreaming": false,
                    "Compress": true,
                    "LambdaFunctionAssociations": {
                        "Quantity": 0
                    },
                    "FunctionAssociations": {
                        "Quantity": 0
                    },
                    "FieldLevelEncryptionId": "",
                    "CachePolicyId": "658327ea-f89d-4fab-a63d-7e886EXAMPLE"
                },
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "CustomErrorResponses": {
                    "Quantity": 0
                },
                "Comment": "",
                "PriceClass": "PriceClass_All",
                "Enabled": true,
                "ViewerCertificate": {
```

```
                    "CloudFrontDefaultCertificate": true,
                    "SSLSupportMethod": "vip",
                    "MinimumProtocolVersion": "TLSv1",
                    "CertificateSource": "cloudfront"
                },
                "Restrictions": {
                    "GeoRestriction": {
                        "RestrictionType": "none",
                        "Quantity": 0
                    }
                },
                "WebACLId": "",
                "HttpVersion": "HTTP2",
                "IsIPV6Enabled": true,
                "Staging": false
            }
        ]
    }
}
```

- Para obtener información sobre la API, consulte ListDistributions en la Referencia de comandos de la AWS CLI.

PowerShell

Herramientas para PowerShell V4

Ejemplo 1: Devuelve distribuciones.

```
Get-CFDistributionList
```

- Para obtener información sobre la API, consulte ListDistributions en la Referencia de Cmdlet de Herramientas de AWS para PowerShell (V4).

Herramientas para PowerShell V5

Ejemplo 1: Devuelve distribuciones.

```
Get-CFDistributionList
```

- Para obtener detalles de la API, consulte ListDistributions en la Referencia de cmdlets de Herramientas de AWS para PowerShell (V5).

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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.")
```

- Para obtener información sobre la API, consulte ListDistributions en la Referencia de la API de AWS SDK para Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   TRY.
       oo_result = lo_fnt->listdistributions( ). " oo_result is returned for
testing purposes. "
       MESSAGE 'Retrieved list of CloudFront distributions.' TYPE 'I'.
     CATCH /aws1/cx_fntinvalidargument.
       MESSAGE 'Invalid argument provided.' TYPE 'E'.
   ENDTRY.
```

- Para obtener detalles sobre la API, consulte ListDistributions en la Referencia de la API de AWS SDK para SAP ABAP.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`UpdateDistribution`** con un SDK de AWS o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `UpdateDistribution`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a CloudFront

CLI

AWS CLI

Ejemplo 1: actualización de un objeto raíz predeterminado de una distribución de CloudFront

En el siguiente ejemplo, se actualiza el objeto raíz predeterminado a `index.html` para la distribución de CloudFront con el ID `EDFDVBD6EXAMPLE`.

```
aws cloudfront update-distribution \
    --id EDFDVBD6EXAMPLE \
    --default-root-object index.html
```

Salida:

```
{
    "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
        }
    }
}
```

Ejemplo 2: actualización de una distribución de CloudFront

En el siguiente ejemplo se deshabilita la distribución de CloudFront con el ID de `EMLARXS9EXAMPLE` al proporcionar la configuración de distribución en un archivo JSON denominado `dist-config-disable.json`. Para actualizar una distribución, debe usar la opción `--if-match` para proporcionar la `ETag` de la distribución. Para obtener la `ETag`, utilice el comando get-distribution o get-distribution-config. Tenga en cuenta que el campo `Enabled` se ha establecido en `false` en el archivo JSON.

Una vez que utilice el siguiente ejemplo para deshabilitar una distribución, puede utilizar el comando delete-distribution para eliminarla.

```
aws cloudfront update-distribution \
    --id EMLARXS9EXAMPLE \
    --if-match E2QWRUHEXAMPLE \
    --distribution-config file://dist-config-disable.json
```

Contenido de `dist-config-disable.json`:

```
{
    "CallerReference": "cli-1574382155-496510",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-1574382155-273939",
```

```
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
```

```
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": false,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
```

```
}
```

Salida:

```
{
    "ETag": "E9LHASXEXAMPLE",
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-12-06T18:32:35.553Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-1574382155-496510",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
```

```
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
```

```
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": false,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Para obtener información acerca de la API, consulte UpdateDistribution en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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);
        }
    }
}
```

- Para obtener información sobre la API, consulte UpdateDistribution en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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!")
```

- Para obtener información sobre la API, consulte UpdateDistribution en la Referencia de la API de AWS SDK para Python (Boto3).

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    TRY.
        " Get the current distribution configuration and ETag "
        DATA(lo_distribution_config_result) = lo_fnt-
>getdistributionconfig( iv_id = iv_distribution_id ).
        DATA(lo_old_config) = lo_distribution_config_result-
>get_distributionconfig( ).
        DATA(lv_etag) = lo_distribution_config_result->get_etag( ).

        " Create a new distribution config with the updated comment "
        " Since the config object is immutable, we need to create a new one with
 all existing values "
        DATA(lo_new_config) = NEW /aws1/cl_fntdistributionconfig(
          iv_callerreference = lo_old_config->get_callerreference( )
          io_aliases = lo_old_config->get_aliases( )
          iv_defaultrootobject = lo_old_config->get_defaultrootobject( )
          io_origins = lo_old_config->get_origins( )
          io_origingroups = lo_old_config->get_origingroups( )
          io_defaultcachebehavior = lo_old_config->get_defaultcachebehavior( )
          io_cachebehaviors = lo_old_config->get_cachebehaviors( )
          io_customerrorresponses = lo_old_config->get_customerrorresponses( )
          iv_comment = iv_comment
          io_logging = lo_old_config->get_logging( )
          iv_priceclass = lo_old_config->get_priceclass( )
          iv_enabled = lo_old_config->get_enabled( )
          io_viewercertificate = lo_old_config->get_viewercertificate( )
          io_restrictions = lo_old_config->get_restrictions( )
          iv_webaclid = lo_old_config->get_webaclid( )
          iv_httpversion = lo_old_config->get_httpversion( )
          iv_isipv6enabled = lo_old_config->get_isipv6enabled( ) ).

        " Update the distribution with the modified configuration "
        lo_fnt->updatedistribution(
          io_distributionconfig = lo_new_config
          iv_id = iv_distribution_id
          iv_ifmatch = lv_etag ).
        MESSAGE 'CloudFront distribution updated successfully.' TYPE 'I'.
      CATCH /aws1/cx_fntnosuchdistribution.
        MESSAGE 'Distribution does not exist.' TYPE 'E'.
      CATCH /aws1/cx_fntpreconditionfailed.
        MESSAGE 'Precondition failed - ETag mismatch.' TYPE 'E'.
      CATCH /aws1/cx_fntinvalidifmatchvrs.
        MESSAGE 'Invalid If-Match version.' TYPE 'E'.
    ENDTRY.
```

- Para obtener detalles sobre la API, consulte UpdateDistribution en la Referencia de la API de AWS SDK para SAP ABAP.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Escenarios para CloudFront usando SDK de AWS

En los siguientes ejemplos de código se muestra cómo implementar escenarios habituales en CloudFront con AWS SDK. Estos escenarios muestran cómo llevar a cabo tareas específicas a través de llamadas a varias funciones en CloudFront o en combinación con otros Servicios de AWS. En cada escenario se incluye un enlace al código fuente completo, con instrucciones de configuración y ejecución del código.

Los escenarios requieren un nivel intermedio de experiencia para entender las acciones de servicio en su contexto.

Ejemplos

- Creación de un SDK de recursos para administradores de AWS SaaS
- Eliminar los recursos de firma de CloudFront usando un SDK de AWS
- Introducción a una distribución de CloudFront básica con la CLI
- Crear URL y cookies firmadas usando un SDK de AWS

Creación de un SDK de recursos para administradores de AWS SaaS

El siguiente ejemplo de código muestra cómo crear una distribución de varios inquilinos y un inquilino de distribución con varias configuraciones.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

El siguiente ejemplo demuestra cómo crear una distribución de varios inquilino con parámetros y un certificado comodín.

```
import software.amazon.awssdk.core.internal.waiters.ResponseOrException;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.ConnectionMode;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.Distribution;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.HttpVersion;
import software.amazon.awssdk.services.cloudfront.model.Method;
import software.amazon.awssdk.services.cloudfront.model.SSLSupportMethod;
import software.amazon.awssdk.services.cloudfront.model.ViewerProtocolPolicy;
import software.amazon.awssdk.services.cloudfront.waiters.CloudFrontWaiter;
import software.amazon.awssdk.services.s3.S3Client;

import java.time.Instant;

public class CreateMultiTenantDistribution {
    public static Distribution
 CreateMultiTenantDistributionWithCert(CloudFrontClient cloudFrontClient,
                                                                  S3Client
 s3Client,
                                                                  final String
 bucketName,
                                                                  final String
 certificateArn) {
        // fetch the origin info if necessary
        final String region = s3Client.headBucket(b ->
 b.bucket(bucketName)).sdkHttpResponse().headers()
```

```
                .get("x-amz-bucket-region").get(0);
        final String originDomain = bucketName + ".s3." + region +
 ".amazonaws.com";
        String originId = originDomain; // Use the originDomain value for the
 originId.

        CreateDistributionResponse createDistResponse =
 cloudFrontClient.createDistribution(builder -> builder
                .distributionConfig(b1 -> b1
                        .httpVersion(HttpVersion.HTTP2)
                        .enabled(true)
                        .comment("Template Distribution with cert built with
 java")
                        .connectionMode(ConnectionMode.TENANT_ONLY)
                        .callerReference(Instant.now().toString())
                        .viewerCertificate(certBuilder -> certBuilder
                                .acmCertificateArn(certificateArn)
                                .sslSupportMethod(SSLSupportMethod.SNI_ONLY))
                        .origins(b2 -> b2
                                .quantity(1)
                                .items(b3 -> b3
                                        .domainName(originDomain)
                                        .id(originId)
                                        .originPath("/{{tenantName}}")
                                        .s3OriginConfig(builder4 -> builder4
                                                .originAccessIdentity(
                                                        "")))
                        .tenantConfig(b5 -> b5
                                .parameterDefinitions(b6 -> b6
                                        .name("tenantName")
                                        .definition(b7 -> b7
                                                .stringSchema(b8 -> b8
                                                        .comment("tenantName
 value")
                                                        .defaultValue("root")
                                                        .required(false)))))
                        .defaultCacheBehavior(b2 -> b2

 .viewerProtocolPolicy(ViewerProtocolPolicy.ALLOW_ALL)
                                .targetOriginId(originId)
                                .cachePolicyId("658327ea-f89d-4fab-
a63d-7e88639e58f6") // CachingOptimized Policy
                                .allowedMethods(b4 -> b4
                                        .quantity(2)
```

```
                                        .items(Method.HEAD, Method.GET)))
               ));

       final Distribution distribution = createDistResponse.distribution();
       try (CloudFrontWaiter cfWaiter =
CloudFrontWaiter.builder().client(cloudFrontClient).build()) {
           ResponseOrException<GetDistributionResponse> responseOrException =
cfWaiter
                   .waitUntilDistributionDeployed(builder ->
builder.id(distribution.id()))
                   .matched();
           responseOrException.response()
                   .orElseThrow(() -> new RuntimeException("Distribution not
created"));
       }
       return distribution;
   }

   public static Distribution
CreateMultiTenantDistributionNoCert(CloudFrontClient cloudFrontClient,
                                                                S3Client s3Client,
                                                                final String
bucketName) {
       // fetch the origin info if necessary
       final String region = s3Client.headBucket(b ->
b.bucket(bucketName)).sdkHttpResponse().headers()
               .get("x-amz-bucket-region").get(0);
       final String originDomain = bucketName + ".s3." + region +
".amazonaws.com";
       String originId = originDomain; // Use the originDomain value for the
originId.

       CreateDistributionResponse createDistResponse =
cloudFrontClient.createDistribution(builder -> builder
               .distributionConfig(b1 -> b1
                       .httpVersion(HttpVersion.HTTP2)
                       .enabled(true)
                       .comment("Template Distribution with cert built with
java")
                       .connectionMode(ConnectionMode.TENANT_ONLY)
                       .callerReference(Instant.now().toString())
                       .origins(b2 -> b2
                               .quantity(1)
                               .items(b3 -> b3
```

```
                                        .domainName(originDomain)
                                        .id(originId)
                                        .originPath("/{{tenantName}}")
                                        .s3OriginConfig(builder4 -> builder4
                                                .originAccessIdentity(
                                                        "")))
                        .tenantConfig(b5 -> b5
                                .parameterDefinitions(b6 -> b6
                                        .name("tenantName")
                                        .definition(b7 -> b7
                                                .stringSchema(b8 -> b8
                                                        .comment("tenantName
 value")
                                                        .defaultValue("root")
                                                        .required(false)))))
                        .defaultCacheBehavior(b2 -> b2

 .viewerProtocolPolicy(ViewerProtocolPolicy.ALLOW_ALL)
                                .targetOriginId(originId)
                                .cachePolicyId("658327ea-f89d-4fab-
a63d-7e88639e58f6") // CachingOptimized Policy
                                .allowedMethods(b4 -> b4
                                        .quantity(2)
                                        .items(Method.HEAD, Method.GET)))
                ));

        final Distribution distribution = createDistResponse.distribution();
        try (CloudFrontWaiter cfWaiter =
 CloudFrontWaiter.builder().client(cloudFrontClient).build()) {
            ResponseOrException<GetDistributionResponse> responseOrException =
 cfWaiter
                    .waitUntilDistributionDeployed(builder ->
 builder.id(distribution.id()))
                    .matched();
            responseOrException.response()
                    .orElseThrow(() -> new RuntimeException("Distribution not
 created"));
        }
        return distribution;
    }
}
```

El siguiente ejemplo demuestra cómo crear un inquilino de distribución asociado con esa plantilla, incluida la utilización del parámetro que hemos declarado anteriormente. Tenga en cuenta que no es necesario agregar información del certificado aquí, ya que nuestro dominio ya está cubierto por la plantilla principal.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantNoCert(CloudFrontClient cloudFrontClient,
                                                                    Route53Client
 route53Client,
                                                                    String
 distributionId,
                                                                    String
 domain,
                                                                    String
 hostedZoneId) {
        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .enabled(false)
                .name("no-cert-tenant")
        );
```

```
        final DistributionTenant distributionTenant =
 createResponse.distributionTenant();

        // Then update the Route53 hosted zone to point your domain at the
 distribution tenant
        // We fetch the RoutingEndpoint to point to via the default connection
 group that was created for your tenant
        final GetConnectionGroupResponse fetchedConnectionGroup =
 cloudFrontClient.getConnectionGroup(builder -> builder
                .identifier(distributionTenant.connectionGroupId()));

        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
                        .comment("ChangeBatch comment")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type("CNAME")
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

 .value(fetchedConnectionGroup.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
                ));
        return distributionTenant;
    }

}
```

Si el certificado del lector se ha omitido en la plantilla principal, deberá agregar la información del certificado en los inquilinos asociados a ella. El siguiente ejemplo muestra cómo hacerlo mediante un certificado arn de ACM que cubre el dominio necesario para el inquilino.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
```

```
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantWithCert(CloudFrontClient cloudFrontClient,

 Route53Client route53Client,
                                                                        String
 distributionId,
                                                                        String
 domain,
                                                                        String
 hostedZoneId,
                                                                        String
 certificateArn) {
        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))
                .enabled(false)
                .name("tenant-with-cert")
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .customizations(b3 -> b3
                        .certificate(b4 -> b4
                                .arn(certificateArn))) // NOTE: Cert must be in
 Us-East-1 and cover the domain provided in this request

        );

        final DistributionTenant distributionTenant =
 createResponse.distributionTenant();

        // Then update the Route53 hosted zone to point your domain at the
 distribution tenant
```

```
        // We fetch the RoutingEndpoint to point to via the default connection
 group that was created for your tenant
        final GetConnectionGroupResponse fetchedConnectionGroup =
 cloudFrontClient.getConnectionGroup(builder -> builder
                .identifier(distributionTenant.connectionGroupId()));

        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
                        .comment("ChangeBatch comment")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type("CNAME")
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

 .value(fetchedConnectionGroup.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
                ));
        return distributionTenant;
    }

}
```

El siguiente ejemplo demuestra cómo hacerlo con una solicitud de certificado administrado alojado en CloudFront. Esto es ideal si aún no tiene tráfico hacia el dominio. En este caso, creamos un ConnectionGroup para generar un RoutingEndpoint. A continuación, utilizamos ese RoutingEndpoint para crear registros DNS que verifiquen la propiedad del dominio y apunten a CloudFront. CloudFront servirá automáticamente un token para validar la propiedad del dominio y crear un certificado administrado.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
```

```
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantCfHosted(CloudFrontClient cloudFrontClient,

 Route53Client route53Client,
                                                                    String
 distributionId,
                                                                    String
 domain,
                                                                    String
 hostedZoneId) throws InterruptedException {
        CreateConnectionGroupResponse createConnectionGroupResponse =
 cloudFrontClient.createConnectionGroup(builder -> builder
                .ipv6Enabled(true)
                .name("cf-hosted-connection-group")
                .enabled(true));

        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
                        .comment("cf-hosted domain validation record")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type(RRType.CNAME)
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

 .value(createConnectionGroupResponse.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
                ));

        // Give the R53 record time to propagate, if it isn't being returned by
 servers yet, the following call will fail
        Thread.sleep(60000);
```

```
        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))

 .connectionGroupId(createConnectionGroupResponse.connectionGroup().id())
                .enabled(false)
                .name("cf-hosted-tenant")
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .managedCertificateRequest(b3 -> b3
                        .validationTokenHost(ValidationTokenHost.CLOUDFRONT)
                )
        );

        return createResponse.distributionTenant();
    }

}
```

El siguiente ejemplo demuestra cómo hacerlo con una solicitud de certificado autoadministrada. Esto es ideal si tiene tráfico hacia el dominio y no puede tolerar el tiempo de inactividad durante una migración. Al final de este ejemplo, el inquilino se creará con un estado de espera de la validación del dominio y la configuración de DNS. Siga los pasos [aquí](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/managed-cloudfront-certificates.html#complete-domain-ownership) para completar la configuración cuando se haya preparado para migrar el tráfico.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
```

```
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantSelfHosted(CloudFrontClient cloudFrontClient,
                                                                        String
 distributionId,
                                                                        String
 domain) {
        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .enabled(false)
                .name("self-hosted-tenant")
                .managedCertificateRequest(b3 -> b3
                        .validationTokenHost(ValidationTokenHost.SELF_HOSTED)
                        .primaryDomainName(domain)
                )
        );

        return createResponse.distributionTenant();
    }

}
```

- Para obtener detalles sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK for Java 2.x.
  - CreateDistribution
  - CreateDistributionTenant

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Eliminar los recursos de firma de CloudFront usando un SDK de AWS

En el siguiente ejemplo de código, se muestra cómo eliminar los recursos que se utilizan para acceder a contenido restringido de un bucket de Amazon Simple Storage Service (Amazon S3).

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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);
        }
    }
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la referencia de la API de AWS SDK for Java 2.x.
  - DeleteKeyGroup

- DeleteOriginAccessControl
- DeletePublicKey

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Introducción a una distribución de CloudFront básica con la CLI

En el siguiente ejemplo de código, se muestra cómo:

- Creación de un bucket de Amazon S3 para el almacenamiento de contenido
- Carga del contenido de ejemplo en el bucket de S3
- Creación de un control de acceso de origen (OAC) para el acceso seguro a S3
- Creación de una distribución de CloudFront con S3 como origen
- Actualización de la política de bucket de S3 para permitir el acceso de CloudFront
- Espera para la implementación de la distribución y prueba del acceso al contenido
- Limpia de los recursos, incluidos la distribución, el OAC y el bucket de S3

Bash

AWS CLI con script Bash

> **Note**
>
> Hay más en GitHub. Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de Tutoriales para desarrolladores de ejemplo.

```
#!/bin/bash

# CloudFront Getting Started Tutorial Script
# This script creates an S3 bucket, uploads sample content, creates a CloudFront
 distribution with OAC,
# and demonstrates how to access content through CloudFront.
```

```
# Set up logging
LOG_FILE="cloudfront-tutorial.log"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "Starting CloudFront Getting Started Tutorial at $(date)"

# Function to handle errors
handle_error() {
    echo "ERROR: $1"
    echo "Resources created before error:"
    if [ -n "$BUCKET_NAME" ]; then
        echo "- S3 Bucket: $BUCKET_NAME"
    fi
    if [ -n "$OAC_ID" ]; then
        echo "- CloudFront Origin Access Control: $OAC_ID"
    fi
    if [ -n "$DISTRIBUTION_ID" ]; then
        echo "- CloudFront Distribution: $DISTRIBUTION_ID"
    fi

    echo "Attempting to clean up resources..."
    cleanup
    exit 1
}

# Function to clean up resources
cleanup() {
    echo "Cleaning up resources..."

    if [ -n "$DISTRIBUTION_ID" ]; then
        echo "Disabling CloudFront distribution $DISTRIBUTION_ID..."

        # Get the current configuration and ETag
        ETAG=$(aws cloudfront get-distribution-config --id "$DISTRIBUTION_ID" --
query 'ETag' --output text)
        if [ $? -ne 0 ]; then
            echo "Failed to get distribution config. Continuing with cleanup..."
        else
            # Create a modified configuration with Enabled=false
            aws cloudfront get-distribution-config --id "$DISTRIBUTION_ID" | \
            jq '.DistributionConfig.Enabled = false' > temp_disabled_config.json

            # Update the distribution to disable it
            aws cloudfront update-distribution \
```

```
                --id "$DISTRIBUTION_ID" \
                --distribution-config file://<(jq '.DistributionConfig'
 temp_disabled_config.json) \
                --if-match "$ETAG"

            if [ $? -ne 0 ]; then
                echo "Failed to disable distribution. Continuing with cleanup..."
            else
                echo "Waiting for distribution to be disabled (this may take
 several minutes)..."
                aws cloudfront wait distribution-deployed --id "$DISTRIBUTION_ID"

                # Delete the distribution
                ETAG=$(aws cloudfront get-distribution-config --id
 "$DISTRIBUTION_ID" --query 'ETag' --output text)
                aws cloudfront delete-distribution --id "$DISTRIBUTION_ID" --if-
match "$ETAG"
                if [ $? -ne 0 ]; then
                    echo "Failed to delete distribution. You may need to delete
 it manually."
                else
                    echo "CloudFront distribution deleted."
                fi
            fi
        fi
    fi

    if [ -n "$OAC_ID" ]; then
        echo "Deleting Origin Access Control $OAC_ID..."
        OAC_ETAG=$(aws cloudfront get-origin-access-control --id "$OAC_ID" --
query 'ETag' --output text 2>/dev/null)
        if [ $? -ne 0 ]; then
            echo "Failed to get Origin Access Control ETag. You may need to
 delete it manually."
        else
            aws cloudfront delete-origin-access-control --id "$OAC_ID" --if-match
 "$OAC_ETAG"
            if [ $? -ne 0 ]; then
                echo "Failed to delete Origin Access Control. You may need to
 delete it manually."
            else
                echo "Origin Access Control deleted."
            fi
        fi
```

```
    fi

    if [ -n "$BUCKET_NAME" ]; then
        echo "Deleting S3 bucket $BUCKET_NAME and its contents..."
        aws s3 rm "s3://$BUCKET_NAME" --recursive
        if [ $? -ne 0 ]; then
            echo "Failed to remove bucket contents. Continuing with bucket
 deletion..."
        fi

        aws s3 rb "s3://$BUCKET_NAME"
        if [ $? -ne 0 ]; then
            echo "Failed to delete bucket. You may need to delete it manually."
        else
            echo "S3 bucket deleted."
        fi
    fi

    # Clean up temporary files
    rm -f temp_disabled_config.json
    rm -rf temp_content
}

# Generate a random identifier for the bucket name
RANDOM_ID=$(openssl rand -hex 6)
BUCKET_NAME="cloudfront-${RANDOM_ID}"
echo "Using bucket name: $BUCKET_NAME"

# Create a temporary directory for content
TEMP_DIR="temp_content"
mkdir -p "$TEMP_DIR/css"
if [ $? -ne 0 ]; then
    handle_error "Failed to create temporary directory"
fi

# Step 1: Create an S3 bucket
echo "Creating S3 bucket: $BUCKET_NAME"
aws s3 mb "s3://$BUCKET_NAME"
if [ $? -ne 0 ]; then
    handle_error "Failed to create S3 bucket"
fi

# Step 2: Create sample content
echo "Creating sample content..."
```

```
cat > "$TEMP_DIR/index.html" << 'EOF'
<!DOCTYPE html>
<html>
<head>
    <title>Hello World</title>
    <link rel="stylesheet" type="text/css" href="css/styles.css">
</head>
<body>
    <h1>Hello world!</h1>
</body>
</html>
EOF

cat > "$TEMP_DIR/css/styles.css" << 'EOF'
body {
    font-family: Arial, sans-serif;
    margin: 40px;
    background-color: #f5f5f5;
}
h1 {
    color: #333;
    text-align: center;
}
EOF

# Step 3: Upload content to the S3 bucket
echo "Uploading content to S3 bucket..."
aws s3 cp "$TEMP_DIR/" "s3://$BUCKET_NAME/" --recursive
if [ $? -ne 0 ]; then
    handle_error "Failed to upload content to S3 bucket"
fi

# Step 4: Create Origin Access Control
echo "Creating Origin Access Control..."
OAC_RESPONSE=$(aws cloudfront create-origin-access-control \
    --origin-access-control-config Name="oac-for-
$BUCKET_NAME",SigningProtocol=sigv4,SigningBehavior=always,OriginAccessControlOriginType=

if [ $? -ne 0 ]; then
    handle_error "Failed to create Origin Access Control"
fi

OAC_ID=$(echo "$OAC_RESPONSE" | jq -r '.OriginAccessControl.Id')
echo "Created Origin Access Control with ID: $OAC_ID"
```

```
# Step 5: Create CloudFront distribution
echo "Creating CloudFront distribution..."

# Get AWS account ID for bucket policy
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)
if [ $? -ne 0 ]; then
    handle_error "Failed to get AWS account ID"
fi

# Create distribution configuration
cat > distribution-config.json << EOF
{
    "CallerReference": "cli-tutorial-$(date +%s)",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "S3-$BUCKET_NAME",
                "DomainName": "$BUCKET_NAME.s3.amazonaws.com",
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                },
                "OriginAccessControlId": "$OAC_ID"
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "S3-$BUCKET_NAME",
        "ViewerProtocolPolicy": "redirect-to-https",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["GET", "HEAD"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["GET", "HEAD"]
            }
        },
        "DefaultTTL": 86400,
        "MinTTL": 0,
        "MaxTTL": 31536000,
        "Compress": true,
        "ForwardedValues": {
            "QueryString": false,
```

```
            "Cookies": {
                "Forward": "none"
            }
        }
    },
    "Comment": "CloudFront distribution for tutorial",
    "Enabled": true,
    "WebACLId": ""
}
EOF

DIST_RESPONSE=$(aws cloudfront create-distribution --distribution-config file://
distribution-config.json)
if [ $? -ne 0 ]; then
    handle_error "Failed to create CloudFront distribution"
fi

DISTRIBUTION_ID=$(echo "$DIST_RESPONSE" | jq -r '.Distribution.Id')
DOMAIN_NAME=$(echo "$DIST_RESPONSE" | jq -r '.Distribution.DomainName')

echo "Created CloudFront distribution with ID: $DISTRIBUTION_ID"
echo "CloudFront domain name: $DOMAIN_NAME"

# Step 6: Update S3 bucket policy
echo "Updating S3 bucket policy..."
cat > bucket-policy.json << EOF
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::$BUCKET_NAME/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudfront::
$ACCOUNT_ID:distribution/$DISTRIBUTION_ID"
                }
            }
        }
```

```
    ]
}
EOF

aws s3api put-bucket-policy --bucket "$BUCKET_NAME" --policy file://bucket-
policy.json
if [ $? -ne 0 ]; then
    handle_error "Failed to update S3 bucket policy"
fi

# Step 7: Wait for distribution to deploy
echo "Waiting for CloudFront distribution to deploy (this may take 5-10
 minutes)..."
aws cloudfront wait distribution-deployed --id "$DISTRIBUTION_ID"
if [ $? -ne 0 ]; then
    echo "Warning: Distribution deployment wait timed out. The distribution may
 still be deploying."
else
    echo "CloudFront distribution is now deployed."
fi

# Step 8: Display access information
echo ""
echo "===== CloudFront Distribution Setup Complete ======"
echo "You can access your content at: https://$DOMAIN_NAME/index.html"
echo ""
echo "Resources created:"
echo "- S3 Bucket: $BUCKET_NAME"
echo "- CloudFront Origin Access Control: $OAC_ID"
echo "- CloudFront Distribution: $DISTRIBUTION_ID"
echo ""

# Ask user if they want to clean up resources
read -p "Do you want to clean up all resources created by this script? (y/n): "
 CLEANUP_RESPONSE
if [[ "$CLEANUP_RESPONSE" =~ ^[Yy] ]]; then
    cleanup
    echo "All resources have been cleaned up."
else
    echo "Resources will not be cleaned up. You can manually delete them later."
    echo "To access your content, visit: https://$DOMAIN_NAME/index.html"
fi

echo "Tutorial completed at $(date)"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI.
  - CreateDistribution
  - CreateOriginAccessControl
  - DeleteDistribution
  - DeleteOriginAccessControl
  - GetDistribution
  - GetDistributionConfig
  - GetOriginAccessControl
  - UpdateDistribution
  - WaitDistributionDeployed

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Crear URL y cookies firmadas usando un SDK de AWS

En el siguiente ejemplo de código, se muestra cómo crear URL firmadas y cookies que permitan el acceso a recursos restringidos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Use la clase CannedSignerRequest para firmar las URL o las cookies con una política predefinida.

```
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();
    }
}
```

Use la clase CustomSignerRequest para firmar las URL o las cookies con una política personalizada. `activeDate` y `ipRange` son métodos opcionales.

```
import software.amazon.awssdk.services.cloudfront.model.CustomSignerRequest;

import java.net.URL;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.time.Instant;
import java.time.temporal.ChronoUnit;

public class CreateCustomPolicyRequest {
```

```
    public static CustomSignerRequest createRequestForCustomPolicy(String
 distributionDomainName,
            String fileNameToUpload,
            String privateKeyFullPath, String publicKeyId) throws Exception {
        String protocol = "https";
        String resourcePath = "/" + fileNameToUpload;

        String cloudFrontUrl = new URL(protocol, distributionDomainName,
 resourcePath).toString();
        Instant expireDate = Instant.now().plus(7, ChronoUnit.DAYS);
        // URL will be accessible tomorrow using the signed URL.
        Instant activeDate = Instant.now().plus(1, ChronoUnit.DAYS);
        Path path = Paths.get(privateKeyFullPath);

        return CustomSignerRequest.builder()
                .resourceUrl(cloudFrontUrl)
                // .resourceUrlPattern("https://*.example.com/*")  // Optional.
                .privateKey(path)
                .keyPairId(publicKeyId)
                .expirationDate(expireDate)
                .activeDate(activeDate) // Optional.
                // .ipRange("192.168.0.1/24") // Optional.
                .build();
    }
}
```

El siguiente ejemplo es una demostración del uso de la clase CloudFrontUtilities para generar cookies y direcciones URL firmadas. Consulte este ejemplo de código en 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;
   }
```

```
}
```

- Para obtener información sobre la API, consulte CloudFrontUtilities en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de CloudFront Functions para CloudFront

Los siguientes ejemplos de código muestran cómo utilizar CloudFront con los SDK de AWS.

Ejemplos

- Añadir encabezados de seguridad HTTP a un evento de respuesta del visor de CloudFront Functions
- Añadir un encabezado CORS a un evento de respuesta del visor de CloudFront Functions
- Añadir un encabezado de control de caché a un evento de respuesta del visor de CloudFront Functions
- Agregar un encabezado True-Client-IP a un evento de solicitud de visor de CloudFront Functions
- Añadir un encabezado True-Client-IP a un evento de solicitud del visor de CloudFront Functions
- Agregar index.html a las URL de solicitud sin un nombre de archivo en un evento de solicitud del visor de CloudFront Functions
- Normalizar los parámetros de la cadena de consulta en una solicitud de visor de CloudFront Functions
- Redirigir a una nueva URL en un evento de solicitud de visor de CloudFront Functions
- Reescribir el URI de una solicitud en función de la configuración de KeyValueStore para un evento de solicitud de un visor de CloudFront Functions
- Dirección de las solicitudes a un origen más cercano al espectador en un evento de solicitud de espectador de CloudFront Functions
- Uso de pares clave-valor en una solicitud de visor de CloudFront Functions
- Validar un token simple en una solicitud de visor de CloudFront Functions

Añadir encabezados de seguridad HTTP a un evento de respuesta del visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo añadir encabezados de seguridad HTTP a un evento de respuesta del visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
async function handler(event) {
    var response = event.response;
    var headers = response.headers;

    // Set HTTP security headers
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation
    headers['strict-transport-security'] = { value: 'max-age=63072000;
 includeSubdomains; preload'};
    headers['content-security-policy'] = { value: "default-src 'none'; img-src
 'self'; script-src 'self'; style-src 'self'; object-src 'none'; frame-ancestors
 'none'"};
    headers['x-content-type-options'] = { value: 'nosniff'};
    headers['x-frame-options'] = {value: 'DENY'};
    headers['x-xss-protection'] = {value: '1; mode=block'};
    headers['referrer-policy'] = {value: 'same-origin'};

    // Return the response to viewers
    return response;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Añadir un encabezado CORS a un evento de respuesta del visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo añadir un encabezado CORS a un evento de respuesta del visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
async function handler(event)  {
    var request = event.request;
    var response  = event.response;

    // If Access-Control-Allow-Origin CORS header is missing, add it.
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation.
    if (!response.headers['access-control-allow-origin'] &&
 request.headers['origin']) {
        response.headers['access-control-allow-origin'] = {value:
 request.headers['origin'].value};
        console.log("Access-Control-Allow-Origin was missing, adding it now.");
    }

    return response;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Añadir un encabezado de control de caché a un evento de respuesta del visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo añadir un encabezado de control de caché a un evento de respuesta del visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
async function handler(event) {
    var response = event.response;
    var headers = response.headers;

    if (response.statusCode >= 200 && response.statusCode < 400) {
        // Set the cache-control header
        headers['cache-control'] = {value: 'public, max-age=63072000'};
    }

    // Return response to viewers
    return response;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Agregar un encabezado True-Client-IP a un evento de solicitud de visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo añadir un encabezado True-Client-IP a un evento de solicitud del visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
async function handler(event) {
    var request = event.request;
    var clientIP = event.viewer.ip;

    //Add the true-client-ip header to the incoming request
    request.headers['true-client-ip'] = {value: clientIP};

    return request;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Añadir un encabezado True-Client-IP a un evento de solicitud del visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo añadir un encabezado de origen a un evento de solicitud del visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
async function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var host = request.headers.host.value;

   // If origin header is missing, set it equal to the host header.
   if (!headers.origin)
       headers.origin = {value:`https://${host}`};

   return request;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Agregar index.html a las URL de solicitud sin un nombre de archivo en un evento de solicitud del visor de CloudFront Functions

En el siguiente ejemplo se muestra cómo agregar index.html a las URL de solicitud sin un nombre de archivo en un evento de solicitud del visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
async function handler(event) {
    var request = event.request;
    var uri = request.uri;

    // Check whether the URI is missing a file name.
    if (uri.endsWith('/')) {
        request.uri += 'index.html';
    }
    // Check whether the URI is missing a file extension.
    else if (!uri.includes('.')) {
        request.uri += '/index.html';
    }

    return request;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Normalizar los parámetros de la cadena de consulta en una solicitud de visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo normalizar los parámetros de cadena de consulta en una solicitud de visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
function handler(event) {
     var qs=[];
     for (var key in event.request.querystring) {
         if (event.request.querystring[key].multiValue) {
             event.request.querystring[key].multiValue.forEach((mv) =>
 {qs.push(key + "=" + mv.value)});
         } else {
             qs.push(key + "=" + event.request.querystring[key].value);
         }
     };

     event.request.querystring = qs.sort().join('&');


     return event.request;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Redirigir a una nueva URL en un evento de solicitud de visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo redirigir una nueva URL en un evento de solicitud del visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
async function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var host = request.headers.host.value;
    var country = 'DE' // Choose a country code
    var newurl = `https://${host}/de/index.html`; // Change the redirect URL to
 your choice

    if (headers['cloudfront-viewer-country']) {
        var countryCode = headers['cloudfront-viewer-country'].value;
        if (countryCode === country) {
            var response = {
                statusCode: 302,
                statusDescription: 'Found',
                headers:
                    { "location": { "value": newurl } }
                }

            return response;
        }
    }
    return request;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Reescribir el URI de una solicitud en función de la configuración de KeyValueStore para un evento de solicitud de un visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo reescribir el URI de una solicitud en función de la configuración de KeyValueStore para un evento de solicitud de un visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
import cf from 'cloudfront';

// (Optional) Replace KVS_ID with actual KVS ID
const kvsId = "KVS_ID";
// enable stickiness by setting a cookie from origin or using another edge
 function
const stickinessCookieName = "appversion";
// set to true to enable console logging
const loggingEnabled = false;

// function rewrites the request uri based on configuration in KVS
// example config in KVS in key:value format
// "latest": {"a_weightage": .8, "a_url": "v1", "b_url": "v2"}
// given above key and value in KVS the request uri will be rewritten
// for example http(s)://domain/latest/something/else will be rewritten as
 http(s)://domain/v1/something/else or http(s)://domain/v2/something/else
 depending on weightage
// if no configuration is found, then the request is returned as is
async function handler(event) {
    // NOTE: This example function is for a viewer request event trigger.
    // Choose viewer request for event trigger when you associate this function
 with a distribution.
    const request = event.request;
    const pathSegments = request.uri.split('/');
```

```
    const key = pathSegments[1];

    // if empty path segment or if there is valid stickiness cookie
    // then skip call to KVS and let the request continue.
    if (!key || hasValidSticknessCookie(request.cookies[stickinessCookieName],
 key)) {
        return event.request;
    }

    try {
        // get the prefix replacement from KVS
        const replacement = await getPathPrefixByWeightage(key);
        if (!replacement) {
            return event.request;
        }
        //Replace the first path with the replacement
        pathSegments[1] = replacement;
        log(`using prefix ${pathSegments[1]}`)
        const newUri = pathSegments.join('/');
        log(`${request.uri} -> ${newUri}`);
        request.uri = newUri;

        return request;
    } catch (err) {
        // No change to the path if the key is not found or any other error
        log(`request uri: ${request.uri}, error: ${err}`);
    }
    // no change to path - return request
    return event.request;
}

// function to get the prefix from KVS
async function getPathPrefixByWeightage(key) {
    const kvsHandle = cf.kvs(kvsId);
    // get the weightage config from KVS
    const kvsResponse = await kvsHandle.get(key);
    const weightageConfig = JSON.parse(kvsResponse);
    // no configuration - return null
    if (!weightageConfig || !isFinite(weightageConfig.a_weightage)) {
        return null;
    }
    // return the url based on weightage
    // return null if no url is configured
    if (Math.random() <= weightageConfig.a_weightage) {
```

```
        return weightageConfig.a_url ? weightageConfig.a_url: null;
    } else {
        return weightageConfig.b_url ? weightageConfig.b_url : null;
    }
}

// function to check if the stickiness cookie is valid
function hasValidStickinessCookie(stickinessCookie, pathSegment) {
    // if the value exists and it matches pathSegment
    return (stickinessCookie && stickinessCookie.value === pathSegment)
}

function log(message) {
    if (loggingEnabled) {
        console.log(message);
    }
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Dirección de las solicitudes a un origen más cercano al espectador en un evento de solicitud de espectador de CloudFront Functions

En el siguiente ejemplo de código, se muestra cómo dirigir las solicitudes a un origen más cercano al espectador en un evento de solicitud de espectador de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
import cf from 'cloudfront';
```

```
function handler(event) {
    const request = event.request;
    const headers = request.headers;
    const country = headers['cloudfront-viewer-country'] &&
        headers['cloudfront-viewer-country'].value;

    //List of Regions with S3 buckets containing content
    const countryToRegion = {
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
    };

    const DEFAULT_REGION = 'us-east-1';

    const selectedRegion = (country && countryToRegion[country]) ||
 DEFAULT_REGION;

    const domainName =
        `cloudfront-functions-demo-bucket-in-${selectedRegion}.s3.
${selectedRegion}.amazonaws.com`;

    cf.updateRequestOrigin({
        "domainName": domainName,
        "originAccessControlConfig": {
            "enabled": true,
            "region": selectedRegion,
            "signingBehavior": "always",
            "signingProtocol": "sigv4",
            "originType": "s3"
        },
    });

    return request;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de pares clave-valor en una solicitud de visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo usar pares clave-valor en una solicitud de visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
import cf from 'cloudfront';

// This fails if there is no key value store associated with the function
const kvsHandle = cf.kvs();

// Remember to associate the KVS with your function before referencing KVS in
 your code.
// https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/kvs-with-
functions-associate.html
async function handler(event) {
    const request = event.request;
    // Use the first segment of the pathname as key
    // For example http(s)://domain/<key>/something/else
    const pathSegments = request.uri.split('/')
    const key = pathSegments[1]
    try {
        // Replace the first path of the pathname with the value of the key
        // For example http(s)://domain/<value>/something/else
        pathSegments[1] = await kvsHandle.get(key);
        const newUri = pathSegments.join('/');
        console.log(`${request.uri} -> ${newUri}`)
        request.uri = newUri;
    } catch (err) {
```

```
        // No change to the pathname if the key is not found
        console.log(`${request.uri} | ${err}`);
    }
    return request;
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Validar un token simple en una solicitud de visor de CloudFront Functions

En el siguiente ejemplo de código se muestra cómo validar un token simple en una solicitud de visor de CloudFront Functions.

JavaScript

Tiempo de ejecución 2.0 de JavaScript para CloudFront Functions

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de Ejemplos de código de CloudFront Functions.

```
import crypto from 'crypto';
import cf from 'cloudfront';

//Response when JWT is not valid.
const response401 = {
    statusCode: 401,
    statusDescription: 'Unauthorized'
};

// Remember to associate the KVS with your function before calling the const
 kvsKey = 'jwt.secret'.
// https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/kvs-with-
functions-associate.html
const kvsKey = 'jwt.secret';
// set to true to enable console logging
```

```
const loggingEnabled = false;


function jwt_decode(token, key, noVerify, algorithm) {
    // check token
    if (!token) {
        throw new Error('No token supplied');
    }
    // check segments
    const segments = token.split('.');
    if (segments.length !== 3) {
        throw new Error('Not enough or too many segments');
    }

    // All segment should be base64
    const headerSeg = segments[0];
    const payloadSeg = segments[1];
    const signatureSeg = segments[2];

    // base64 decode and parse JSON
    const payload = JSON.parse(_base64urlDecode(payloadSeg));

    if (!noVerify) {
        const signingMethod = 'sha256';
        const signingType = 'hmac';

        // Verify signature. `sign` will return base64 string.
        const signingInput = [headerSeg, payloadSeg].join('.');

        if (!_verify(signingInput, key, signingMethod, signingType,
 signatureSeg)) {
            throw new Error('Signature verification failed');
        }

        // Support for nbf and exp claims.
        // According to the RFC, they should be in seconds.
        if (payload.nbf && Date.now() < payload.nbf*1000) {
            throw new Error('Token not yet active');
        }

        if (payload.exp && Date.now() > payload.exp*1000) {
            throw new Error('Token expired');
        }
    }
```

```
    return payload;
}

//Function to ensure a constant time comparison to prevent
//timing side channels.
function _constantTimeEquals(a, b) {
    if (a.length != b.length) {
        return false;
    }

    let xor = 0;
    for (let i = 0; i < a.length; i++) {
    xor |= (a.charCodeAt(i) ^ b.charCodeAt(i));
    }

    return 0 === xor;
}

function _verify(input, key, method, type, signature) {
    if(type === "hmac") {
        return _constantTimeEquals(signature, _sign(input, key, method));
    }
    else {
        throw new Error('Algorithm type not recognized');
    }
}

function _sign(input, key, method) {
    return crypto.createHmac(method, key).update(input).digest('base64url');
}

function _base64urlDecode(str) {
    return Buffer.from(str, 'base64url')
}

async function handler(event) {
    let request = event.request;

    //Secret key used to verify JWT token.
    //Update with your own key.
    const secret_key = await getSecret()

    if(!secret_key) {
```

```
        return response401;
    }

    // If no JWT token, then generate HTTP redirect 401 response.
    if(!request.querystring.jwt) {
        log("Error: No JWT in the querystring");
        return response401;
    }

    const jwtToken = request.querystring.jwt.value;

    try{
        jwt_decode(jwtToken, secret_key);
    }
    catch(e) {
        log(e);
        return response401;
    }

    //Remove the JWT from the query string if valid and return.
    delete request.querystring.jwt;
    log("Valid JWT token");
    return request;
}

// get secret from key value store
async function getSecret() {
    // initialize cloudfront kv store and get the key value
    try {
        const kvsHandle = cf.kvs();
        return await kvsHandle.get(kvsKey);
    } catch (err) {
        log(`Error reading value for key: ${kvsKey}, error: ${err}`);
        return null;
    }

}

function log(message) {
    if (loggingEnabled) {
        console.log(message);
    }
}
```

Para obtener una lista completa de las guías para desarrolladores de AWS SDK y ejemplos de código, consulte Uso de CloudFront con AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Historial de documentos

En la siguiente tabla, se describen los cambios importantes realizados en la documentación de CloudFront. Para recibir notificaciones sobre las actualizaciones, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
Se ha agregado TLS mutua (espectador)	CloudFront admite TLS mutua (espectador).	24 de noviembre de 2025
Se ha agregado un campo de registro para los registros de acceso	Se ha agregado el campo `connection-id` para los registros de acceso (registros estándar) y los registros de acceso en tiempo real.	24 de noviembre de 2025
Se han agregado registros de conexión	Se han agregado los registros de conexión como una nueva característica de registro para el TLS mutua (espectador).	24 de noviembre de 2025
Se han agregado funciones de conexión	CloudFront admite funciones de conexión para TLS mutua (espectador).	24 de noviembre de 2025
Agregación de compatibilidad para la incorporación de la propia IP a CloudFront mediante IPAM	CloudFront permite incorporar las propias direcciones IPv4 a través del BYOIP de IPAM para servicios globales.	24 de noviembre de 2025
AWS Actualización de política administrada por	Las políticas de IAM `CloudFrontReadOnlyAccess` y `CloudFrontFullAccess` ahora apoyan las acciones `ec2:DescribeIpamPo`	24 de noviembre de 2025

	`ols` y `ec2:GetIpamPoolCidrs`.	
Actualizaciones de CloudFront Functions	Esta versión agrega parámetros para los métodos auxiliares de modificación de origen en CloudFront Functions. Puede utilizar los parámetros `hostHeader`, `sni`, `allowedCertificateNames` y `originOverrides`.	20 de noviembre de 2025
Actualizaciones de CloudFront Functions	Se ha agregado compatibilidad con los tókenes web CBOR (CWT) para las CloudFront Functions.	20 de noviembre de 2025
Actualizaciones de CloudFront Functions	Se han agregado métodos de ayuda generales para CloudFront Functions.	20 de noviembre de 2025
Actualización de la política administrada de AWS	Se ha actualizado `CloudFrontFullAccess` para permitir crear un recurso de ACL web de AWS WAF y crear, actualizar, eliminar y leer el acceso a AWS Pricing Plan Manager.	18 de noviembre de 2025
Actualización de la política administrada de AWS	Se ha actualizado `CloudFrontReadOnlyAccess` para permitir el acceso de solo lectura al AWS Pricing Plan Manager.	18 de noviembre de 2025

Actualización de la política administrada de AWS	Se ha actualizado `CloudFrontFullAccess` para permitir crear un recurso de ACL web de AWS WAF y crear, actualizar, eliminar y leer el acceso a AWS Pricing Plan Manager.	18 de noviembre de 2025
Actualización de la política administrada de AWS	Se ha actualizado `CloudFrontReadOnlyAccess` para permitir el acceso de solo lectura al AWS Pricing Plan Manager.	18 de noviembre de 2025
CloudFront admite planes de precios de tarifa fija	Ahora puede suscribir las distribuciones a un plan de precios de tarifa fija de CloudFront.	18 de noviembre de 2025
Direcciones IP estáticas de anycast	Ahora puede elegir solo entre direcciones IPv4 o direcciones IPv4 e IPv6 (doble pila).	5 de noviembre de 2025
Compatibilidad agregada para compartir orígenes de la VPC en Cuentas de AWS	Puede crear un recurso compartido y agregarle orígenes de VPC. Esto le permite mantener los orígenes de VPC y las distribuciones de CloudFront en Cuentas de AWS independientes, lo que permite a la organización mantener los requisitos de varias cuentas. Otras Cuentas de AWS pueden asociar los orígenes de la VPC compartidos a las distribuciones de CloudFront.	5 de noviembre de 2025

Se ha agregado una política de seguridad para los espectadores	Se ha agregado la política de seguridad TLSv1.2_2025. • Protocolos y cifrados admitidos entre lectores y CloudFront • Política de seguridad (versión mínima de SSL/TLS)	10 de octubre de 2025
Se han agregado algoritmos de intercambio de claves poscuánticos (PQ	Se han agregado dos nuevos algoritmos de intercambio de claves PQ a las políticas TLS de CloudFront.	4 de septiembre de 2025
Solicitudes de origen de IPv	Cuando utiliza un origen personalizado (excepto los orígenes de Amazon S3 y VPC), puede personalizar la configuración de origen de la distribución para elegir la forma en que CloudFront se conecta al origen mediante direcciones IPv4 o IPv6.	3 de septiembre de 2025
Se ha agregado una nueva política de solicitud de origen administrada	Se ha agregado una nueva política de solicitud de origen administrada `HostHeaderOnly` .	29 de agosto de 2025

Los puntos de conexión públicos de CloudFront ahora admiten IPv6	Consulte los puntos de conexión y las cuotas de Amazon CloudFront en Referencia general de AWS y Servicios de AWS que admiten IPv6 en la Guía del usuario de la VPC de Amazon.	21 de agosto de 2025
Se ha agregado una política de seguridad para los espectadores	Se ha agregado TLSv1.3_2025, una nueva política de seguridad solo de TLS 1.3.	7 de agosto de 2025
Se han agregado nuevas opciones de configuración del tiempo de espera de origen	Se ha agregado el tiempo de espera de finalización de respuesta para todos los orígenes y se ha agregado el tiempo de espera de respuesta (tiempo de espera de lectura de origen) para los orígenes de S3.	30 de julio de 2025
Se ha agregado la configuración de distribución estándar preconfigurada	Se ha agregado la configuración preconfigurada para distribuciones estándar.	17 de junio de 2025
Se ha agregado un nuevo flujo de trabajo de la consola para la configuración de dominios de distribución estándar	Se ha agregado un nuevo flujo de trabajo de la consola para la configuración de dominios de distribución estándar.	17 de junio de 2025
Se han agregado parámetros de ejemplo	Se han agregado ejemplos para utilizar parámetros con nombres de dominio y rutas de origen en inquilinos de distribución.	17 de junio de 2025

Compatibilidad con CloudFront Functions para CloudFront SaaS Manager	Se han agregado las funciones auxiliares y el campo `endpoint` para el objeto `context`.	2 de mayo de 2025
Actualizaciones del registro estándar (v2)	Se ha agregado la variable de partición `{distributionid}` para permitir el envío de registros de acceso a AWS Glue.	1 de mayo de 2025
Actualizaciones de las políticas administradas de CloudFront	Se han agregado permisos de ACM a las políticas administradas `CloudFrontReadOnlyAccess` y `CloudFrontFullAccess`.	28 de abril de 2025
Compatibilidad con distribuciones de varios inquilinos e inquilinos de distribución	Puede crear una distribución de varios inquilinos para establecer una configuración de distribución común en función del tipo de origen. A continuación, puede reutilizar la distribución de varios inquilinos para crear varios inquilinos de distribución que compartan esa configuración. A continuación, puede personalizar inquilinos de distribución específicos a medida que agrega sitios web o aplicaciones adicionales.	28 de abril de 2025

Actualizaciones para funciones de Lambda@Edge	Las funciones de Lambda@Edge admiten ahora controles de registro avanzados y la personalización del nombre del grupo de registro de CloudWatch.	7 de abril de 2025
Direcciones IP estáticas de anycast	Puede utilizar IPs estáticas de anycast para habilitar el enrutamiento de dominios apex directamente a las distribuciones de CloudFront.	4 de abril de 2025
Métodos auxiliares adicionales agregados para la modificación del origen	Se han agregado los métodos auxiliares `selectRequestOriginById()` y `createRequestOriginGroup()` de CloudFront Functions.	2 de abril de 2025
Actualizaciones del registro estándar (v2)	Se ha agregado la variable de la partición `{accountid}` y las rutas de sufijo de ejemplo para la entrega del registro de acceso a Amazon S3.	14 de febrero de 2025
Se han agregado campos de registro de acceso en tiempo real adicionales para el registro estándar (v2)	Puede especificar los campos de registro de acceso en tiempo real `c-country` y `cache-behavior-path-pattern` al habilitar el registro estándar (v2).	31 de enero de 2025
Lambda@Edge admite la versión más reciente del tiempo de ejecución	Lambda@Edge ahora admite funciones de Lambda con los tiempos de ejecución de Node.js 22.	22 de noviembre de 2024

Compatibilidad de la resiliencia basada en la calidad multimedia con CloudFront	Puede utilizar la característica de la resiliencia basada en la calidad multimedia (MQAR) para que CloudFront elija automáticamente el origen en un grupo de origen con la puntuación de calidad multimedia más alta.	21 de noviembre de 2024
Método auxiliar para la modificación del origen	Se agregó un nuevo método auxiliar de CloudFront Functions para modificar el origen.	21 de noviembre de 2024
Orígenes de la VPC	Utilice Orígenes de la VPC de CloudFront para restringir el acceso a un equilibrador de carga de aplicación, un equilibrador de carga de red o una instancia de EC2.	20 de noviembre de 2024
Actualizaciones a políticas administradas	Se actualizó la política administrada de `CloudFrontFullAccess` .	20 de noviembre de 2024
Direcciones IP estáticas de anycast	Puede solicitar direcciones IP estáticas de anycast a CloudFront para usarlas con sus distribuciones.	20 de noviembre de 2024
Se agregó compatibilidad para el registro estándar	CloudFront es compatible con el registro estándar (v2) y el envío de registros a los Registros de Amazon CloudWatch, Amazon Data Firehose y Amazon Simple Storage Service (Amazon S3).	20 de noviembre de 2024

Se agregó compatibilidad con gRPC	CloudFront ahora admite las solicitudes de gRPC para su distribución.	20 de noviembre de 2024
Se agregó una nueva política administrada para Orígenes de la VPC	Se agregó la nueva política administrada `AWSCloudFrontVPCOriginServiceRolePolicy` .	20 de noviembre de 2024
Lambda@Edge admite la versión más reciente del tiempo de ejecución	Lambda@Edge ahora es compatible con las funciones de Lambda con tiempo de ejecución de Python 3.13.	13 de noviembre de 2024
Evaluación con reglas de AWS Config	Evalúe las configuraciones de CloudFront con reglas de AWS Config.	20 de septiembre de 2024
Se ha agregado más contenido de solución de problemas	Se ha agregado más contenido de solución de problemas para los códigos de estado de respuesta de error HTTP 4xx y 5xx.	26 de agosto de 2024
Nuevas políticas de caché administradas añadidas	Nuevas políticas de caché administradas añadidas `UseOriginCacheControlHeaders` y `UseOriginCacheControlHeaders-QueryStrings` .	24 de mayo de 2024
Se agregó compatibilidad con control de acceso de origen	Ahora puede crear un control de acceso de origen (OAC) para AWS Elemental MediaPackage V2 y una URL de función de AWS Lambda.	11 de abril de 2024

Campos de registro de acceso en tiempo real para CMCD	Se han agregado 18 campos de datos comunes de clientes multimedia (CMCD) para registros en tiempo real.	9 de abril de 2024
Introducción a una distribución de CloudFront básica	Tutorial actualizado para una distribución estándar que utiliza un origen de Amazon S3 con control de acceso de origen (OAC).	18 de marzo de 2024
Ejemplos de código para CloudFront mediante AWS SDK	Se agregaron ejemplos de código que muestran cómo utilizar CloudFront con un kit de desarrollo de software (SDK) de AWS. Los ejemplos están divididos en extractos de código que muestran cómo llamar a funciones de servicio individuales y ejemplos que muestran cómo hacer una tarea específica llamando a múltiples funciones dentro del mismo servicio.	16 de febrero de 2024
AWS Política administrada por	Las políticas `CloudFrontReadOnlyAccess` y `CloudFrontFullAccess` de IAM ahora admiten las operaciones `KeyValueStore`.	19 de diciembre de 2023
Tiempo de ejecución 2.0 de JavaScript 2.0	Características agregadas del tiempo de ejecución 2.0 de JavaScript para CloudFront Functions.	21 de noviembre de 2023

CloudFront KeyValueStore	Amazon CloudFront ahora admite CloudFront KeyValueStore. Esta característica es un almacén de datos clave-valor seguro, global y de baja latencia que permite el acceso de lectura en CloudFront Functions. Puede habilitar la lógica personalizable avanzada en las ubicaciones periféricas de CloudFront.	21 de noviembre de 2023
Lambda@Edge admite la versión más reciente del tiempo de ejecución	Ahora, Lambda@Edge admite funciones de Lambda con los tiempos de ejecución de Node.js 20.	15 de noviembre de 2023
Panel de seguridad	CloudFront crea un panel de seguridad cuando crea una distribución. Habilite AWS WAF, administre las restricciones geográficas y consulte los datos de alto nivel de las solicitudes, los bots y los registros.	8 de noviembre de 2023
Ordenar cadenas de consulta en funciones	CloudFront ahora admite la clasificación de cadenas de consulta mediante CloudFront Functions.	3 de octubre de 2023
AWS WAF Recomendaciones de seguridad de	Amazon CloudFront ahora muestra recomendaciones de seguridad de AWS WAF en la consola de CloudFront.	26 de septiembre de 2023

Compatibilidad con la distribución de contenido de la caché obsoleto (caducado	CloudFront admite las directivas de control de la caché `Stale-While-Revalidate` y `Stale-If-Error` .	15 de mayo de 2023
Habilitar las protecciones de AWS WAF con un solo clic	Un método simplificado para agregar protecciones de seguridad de AWS WAF a las distribuciones de CloudFront.	10 de mayo de 2023
Habilitar las ACL para los nuevos buckets de S3 utilizados para los registros estándar	Se ha agregado una nota y enlaces para abordar la configuración de ACL predeterminada para los nuevos buckets de S3.	11 de abril de 2023
Crear un origen mediante Amazon S3 Object Lambda	Puede utilizar un alias de punto de acceso de Amazon S3 Object Lambda como origen de la distribución.	31 de marzo de 2023
Personalizar el estado y el cuerpo HTTP con CloudFront Functions	Puede utilizar CloudFront Functions para actualizar el código de estado de la respuesta del lector y sustituir o eliminar el cuerpo de la respuesta.	29 de marzo de 2023
Se han agregado opciones comodín de encabezados de CORS para puertos	Ahora puede incluir configuraciones comodín para puertos en encabezados de control de acceso de CORS.	20 de marzo de 2023

Se ha agregado un nuevo enlace para la Guía del usuario de AWS Security Hub CSPM	Se ha actualizado el idioma y se ha agregado un enlace a los controles reorganizados de Amazon CloudFront en la Guía del usuario de AWS Security Hub CSPM.	9 de marzo de 2023
CloudFront ahora admite listas de bloqueo (“todas excepto”) en las políticas de solicitud de origen	Utilice las listas de bloqueo en las políticas de solicitud de origen para incluir todas las cadenas de consulta, los encabezados HTTP o las cookies, excepto las especific adas, en las solicitudes que CloudFront envía al origen.	22 de febrero de 2023
CloudFront agrega una nueva política de solicitud de origen administrada para reenviar todos los encabezados del lector, excepto el encabezado del host	Utilice la nueva política de solicitud de origen administr ada de CloudFront para incluir todos los encabezados de la solicitud del lector, excepto para el encabezado `Host`, en las solicitudes que CloudFront envía al origen.	22 de febrero de 2023
Restricciones actualizadas en Lambda@Edge	Lambda@Edge admite las configuraciones de administr ación del tiempo de ejecución de Lambda establecidas en Auto.	16 de febrero de 2023
Se ha actualizado la guía de IAM para CloudFront	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulta prácticas recomenda das de seguridad en IAM.	15 de febrero de 2023

Seguridad de un control de acceso de origen	Ahora puede proteger los orígenes de MediaStore al permitir el acceso solo a las distribuciones de CloudFront designadas.	9 de febrero de 2023
Nuevos encabezados para determinar la estructura de los encabezados del lector	Ahora puede añadir el orden y el número de los encabezados para ayudar a identificar al lector en función de los encabezados que envía.	13 de enero de 2023
Lambda@Edge admite la versión más reciente del tiempo de ejecución	Ahora, Lambda@Edge admite funciones de Lambda con los tiempos de ejecución de Node.js 18.	12 de enero de 2023
Eliminar los encabezados de respuesta mediante una política de encabezados de respuesta	Ahora puede usar una política de encabezados de respuesta de CloudFront para eliminar del origen los encabezados que CloudFront ha recibido en la respuesta. Los encabezados especificados no se incluyen en la respuesta que CloudFront envía a los lectores.	3 de enero de 2023
Implementación continua para probar de forma segura los cambios de configuración	Ahora puede implementar cambios en la configuración de su CDN realizando pruebas con un subconjunto del tráfico de producción.	18 de noviembre de 2022

Versión del encabezado `CloudFront-Viewer-JA3-Fingerprint`	Ahora puede utilizar la huella digital JA3 para ayudar a determinar si la solicitud proviene de un cliente conocido.	16 de noviembre de 2022
Se han añadido opciones comodín para los encabezados de CORS	Ahora puede usar varias configuraciones comodín en algunos encabezados de control de acceso de CORS.	11 de noviembre de 2022
Métricas adicionales para las distribuciones de CloudFront	Compatibilidad con `MonitoringSubscription` en la API de CloudFront y CloudFormation.	3 de octubre de 2022
Seguridad mejorada con control de acceso de origen	Ahora puede proteger los orígenes de Amazon S3 al permitir el acceso únicamente a las distribuciones de CloudFront designadas.	24 de agosto de 2022
Soporte HTTP/3 para distribuciones de CloudFront	Ahora puede elegir HTTP/3 para su distribución de CloudFront.	15 de agosto de 2022
Añadir detalles del protocolo de enlace al encabezado de CloudFront-Viewer-TLS	Ahora puede ver información sobre el protocolo de enlace SSL/TLS utilizado.	27 de junio de 2022
Nueva métrica en el encabezado Server-Timing	Se ha añadido la nueva métrica `cdn-downstream-fbl` a los encabezados `Server-Timing` .	13 de junio de 2022

Nuevo encabezado para obtener información sobre la versión y el cifrado de TLS	Ahora puede utilizar el encabezado `CloudFront-Viewer-TLS` para obtener información sobre la versión de TLS (o SSL) y el cifrado que se ha utilizado para la conexión entre el visor y CloudFront.	23 de mayo de 2022
Nueva métrica FunctionThrottles para CloudFront Functions	Con Amazon CloudWatch, ahora puede supervisar el número de veces que se ha limitado una CloudFront Function en un periodo de tiempo determinado.	4 de mayo de 2022
CloudFront admite URL de funciones de Lambda	Si crea una aplicación web sin servidor mediante funciones de Lambda con URL de función, ahora puede agregar CloudFront para obtener una serie de beneficios.	6 de abril de 2022
Encabezado Server-Timing en las respuestas HTTP	Ahora puede habilitar el encabezado `Server-Timing` en las respuestas HTTP enviadas desde CloudFront para ver las métricas que pueden ayudarle a obtener información sobre el comportamiento y el rendimiento de CloudFront.	30 de marzo de 2022

Utilice la lista de prefijos administrados por AWS para limitar el tráfico entrante	Ahora puede limitar el tráfico HTTP y HTTPS entrante a sus orígenes desde solo las direcciones IP que pertenecen a los servidores orientados al origen de CloudFront.	7 de febrero de 2022
Nueva característica	Amazon CloudFront agrega compatibilidad con políticas de encabezados de respuesta , que permiten especificar los encabezados HTTP que CloudFront agrega a las respuestas HTTP que envía a los lectores (navegadores web u otros clientes). Puede especificar los encabezad os deseados (y sus valores) sin realizar ningún cambio en el origen ni escribir ningún código. Para obtener más información, consulte Añadir o eliminar encabezados HTTP a las respuestas de CloudFront.	2 de noviembre de 2021
Nuevo encabezado de solicitud `CloudFront-Viewer-Address`	CloudFront agrega compatibi lidad con un nuevo encabezad o, `CloudFront-Viewer-Address` , que contiene la dirección IP del lector que ha enviado la solicitud HTTP a CloudFront. Para obtener más información, consulte Agregar encabezados de solicitudes de CloudFront.	25 de octubre de 2021

Lambda@Edge es compatible con la nueva versión de tiempo de ejecución	Lambda@Edge ahora es compatible con las funciones Lambda con tiempo de ejecución de Python 3.9. Para obtener información, consulte Tiempos de ejecución admitidos.	22 de septiembre de 2021
AWS actualización de política administrada	CloudFront actualizó la política CloudFrontReadOnlyAccess. Para obtener más información, consulte Actualizaciones de CloudFront a las políticas administradas de AWS.	8 de septiembre de 2021
Nueva característica	CloudFront ahora es compatible con los certificados ECDSA para conexiones HTTPS orientadas al lector. Para obtener más información, consulte Protocolos y cifrados admitidos entre lectores y CloudFront y Requisitos para la utilización de certificados SSL/TLS con CloudFront.	14 de julio de 2021
Nueva característica	CloudFront ahora admite más formas de mover un nombre de dominio alternativo de una distribución a otra, sin tener que contactar a Soporte. Para obtener más información, consulte Mover un nombre de dominio alternativo a una distribución diferente.	7 de julio de 2021

Nueva política de seguridad	CloudFront ahora admite una nueva política de seguridad , TLSv1.2_2021, con un conjunto más pequeño de algoritmos criptográ ficos compatibles. Para obtener más información, consulte Protocolos y cifrados admitidos entre lectores y CloudFront.	23 de junio de 2021
Nueva característica	Amazon CloudFront ahora admite CloudFront Functions , una característica nativa de CloudFront con la que puede escribir funciones ligeras en JavaScript para personali zaciones de CDN sensibles a la latencia a gran escala. Para obtener más informaci ón, consulte Personalización en el borde con CloudFront Functions.	3 de mayo de 2021
Lambda@Edge admite versiones más recientes del tiempo de ejecución	Lambda@Edge ahora admite funciones de Lambda con los tiempos de ejecución de Node.js 14. Para obtener información, consulte Tiempos de ejecución admitidos.	29 de abril de 2021

Quitar documentación para distribuciones RTMP	Amazon CloudFront dio de baja las distribuciones del protocolo de mensajería en tiempo real (RTMP) el 31 de diciembre de 31, 2020. La documentación para las distribuciones RTMP ahora se elimina de la Guía para desarrolladores de Amazon CloudFront.	10 de febrero de 2021
Nuevas opciones de precios	Amazon CloudFront presenta el paquete de ahorro de seguridad CloudFront, una forma sencilla de ahorrar hasta un 30 % en los cargos de CloudFront en su factura de AWS. Para obtener más información, consulte las preguntas frecuentes acerca del paquete de ahorros.	5 de febrero de 2021
Nuevo tutorial	La Guía para desarrolladores de Amazon CloudFront incluye ahora un tutorial sobre el uso de Amazon CloudFron t para restringir el acceso a Application Load Balancer en Elastic Load Balancing. Para obtener más informaci ón, consulte Restricción del acceso al Equilibrador de carga de aplicación.	18 de diciembre de 2020

Nueva opción para la administración de claves públicas	CloudFront ahora admite la administración de claves públicas para URL y cookies firmadas a través de la consola y la API de CloudFron t, sin necesidad de acceder al usuario raíz de la Cuenta de AWS. Para obtener más información, consulte Especific ación de los signatarios que pueden crear URL firmadas y cookies firmadas.	22 de octubre de 2020
Nueva característica: Origin Shield	CloudFront ahora admite CloudFront Origin Shield, una capa adicional en la infraestr uctura de almacenamiento en caché de CloudFront que ayuda a minimizar la carga del origen, mejorar la disponibi lidad y reducir los costos de explotación. Para obtener más información, consulte Uso de Amazon CloudFront Origin Shield.	20 de octubre de 2020

Nuevo formato de compresión	CloudFront ahora admite la formación de compresión Brotli cuando configura CloudFront para comprimir objetos en ubicaciones de borde de CloudFront. También puede configurar CloudFront para almacenar en caché objetos Brotli mediante un encabezado `Accept-Encoding` normalizado. Para obtener más información, consulte Ofrecer archivos comprimidos y Compatibilidad con la compresión.	14 de septiembre de 2020
Nuevo protocolo TLS	CloudFront ahora es compatible con el protocolo TLS 1.3 para conexiones HTTPS entre lectores y distribuciones de CloudFront. TLS 1.3 está habilitado de forma predeterminada en todas las políticas de seguridad de CloudFront. Para obtener más información, consulte Protocolos y cifrados admitidos entre lectores y CloudFront.	3 de septiembre de 2020

Registros de acceso en tiempo real nuevos	CloudFront ahora admite registros de acceso en tiempo real configurables. Con los registros de acceso en tiempo real, puede obtener informaci ón sobre las solicitudes realizadas a una distribución en tiempo real. Puede usar los registros de acceso en tiempo real para supervisar, analizar y tomar medidas en función del rendimiento de entrega de contenido. Para obtener más información, consulte Registros en tiempo real.	31 de agosto de 2020
Compatibilidad con API para métricas adicionales	CloudFront ahora admite la habilitación de ocho métricas adicionales en tiempo real con la API de CloudFront. Para obtener más informaci ón, consulte Activación de métricas adicionales.	28 de agosto de 2020
Nuevos encabezados HTTP de CloudFront	CloudFront ha agregado encabezados HTTP adicional es para determinar informaci ón sobre el lector como el tipo de dispositivo, la ubicación geográfica, etc. Para obtener más información, consulte Agregar encabezados de solicitudes de CloudFront.	23 de julio de 2020

Nueva característica	CloudFront ahora admite políticas de caché y políticas de solicitud de origen, que proporcionan un control pormenorizado sobre la clave de caché y las solicitudes de origen para las distribuciones de CloudFront. Para obtener más información, consulte Control de la clave de caché y Control de solicitudes de origen.	22 de julio de 2020
Nueva política de seguridad	CloudFront ahora admite una nueva política de seguridad , TLSv1.2_2019, con un conjunto más pequeño de algoritmos criptográ ficos compatibles. Para obtener más información, consulte Protocolos y cifrados admitidos entre lectores y CloudFront.	8 de julio de 2020
Nueva configuración para controlar los tiempos de espera e intentos de origen	CloudFront ha agregado nuevas configuraciones que controlan los tiempos de espera e intentos de origen. Para obtener más informaci ón, consulte Control de los tiempos de espera de origen y los intentos.	5 de junio de 2020

Nueva documentación para comenzar a usar CloudFront mediante la creación de un sitio web estático seguro	Comience a trabajar con CloudFront creando un sitio web estático seguro con Amazon S3, CloudFront, Lambda@Edge, etc., todo ello implementado con CloudFormation. Para obtener más información, consulte Introducción a un sitio web seguro estático.	2 de junio de 2020
Lambda@Edge admite versiones más recientes del tiempo de ejecución	Lambda@Edge ahora admite funciones de Lambda con los tiempos de ejecución de Node.js 12 y Python 3.8. Para obtener información, consulte Tiempos de ejecución admitidos.	27 de febrero de 2020
Nuevas métricas en tiempo real en CloudWatch	Amazon CloudFront ofrece ahora ocho métricas en tiempo real adicionales en Amazon CloudWatch. Para obtener más información, consulte Activación de métricas de distribución adicionales de CloudFront.	19 de diciembre de 2019
Nuevos campos en los registros de acceso	CloudFront agrega siete nuevos campos para obtener acceso a los registros. Para obtener más información, consulte Campos de archivos de registro estándar.	12 de diciembre de 2019

AWS Complemento de WordPress para	Puede utilizar el complemento AWS WordPress para proporcionar a los visitantes al sitio web de WordPress una experiencia de visualización acelerada con CloudFront. (Actualización: a partir del 30 de septiembre de 2022, AWS para el complemento de WordPress está obsoleto).	30 de octubre de 2019
Políticas de permisos de IAM de recursos y basadas en etiquetas	CloudFront ahora admite dos formas adicionales de especificar políticas de permisos de IAM: permisos de políticas basadas en etiquetas y de nivel de recursos. Para obtener más información, consulte Administración del acceso a los recursos.	8 de agosto de 2019
Compatibilidad con el lenguaje de programación Python	Ahora puede utilizar el lenguaje de programación Python para desarrollar funciones en Lambda@Edge, además de Node.js. Para ver funciones de ejemplo que abarcan diversos escenarios, consulte Funciones de ejemplo de Lambda@Edge.	1 de agosto de 2019

Se han actualizado los gráficos de supervisión	Actualizaciones de contenido para describir nuevas formas de monitorizar funciones Lambda asociadas con las distribuciones de CloudFront directamente desde la consola de CloudFront para realizar un seguimiento y depurar errores más fácilmente. Para obtener más información, consulte Monitoreo de CloudFront.	20 de junio de 2019
Contenido de seguridad consolidado	Un nuevo capítulo de seguridad consolida informaci ón acerca de las caracterí sticas de CloudFront en torno a la implementación de la protección de datos, IAM, registro, conformidad, etc. Para obtener más información, consulte Seguridad.	24 de mayo de 2019
Ahora es necesaria la validación de dominios	CloudFront ahora requiere el uso de un certificado SSL para verificar que se tiene permiso para utilizar un nombre de dominio alternativo con una distribución. Para obtener más información, consulte Usar nombres de dominio alternati vos y HTTPS.	9 de abril de 2019

Se ha actualizado el nombre de archivo PDF	El nuevo nombre de archivo de la Guía para desarrolladores de Amazon CloudFront es: AmazonCloudFront_DevGuide. El nombre anterior era: cf-dg.	7 de enero de 2019
Nuevas características	CloudFront ahora admite WebSocket, un protocolo basado en TCP que resulta útil cuando se necesitan conexiones de larga duración entre clientes y servidores. Ahora también puede configurar CloudFront con conmutación por error en el origen en los casos en los que se requiera alta disponibilidad. Para obtener más información, consulte Uso de WebSocket con distribuciones de CloudFront y Optimización de alta disponibilidad con conmutación por error en el origen de CloudFront.	20 de noviembre de 2018

Nueva característica	CloudFront ahora permite utilizar registros de errores detallados con las solicitudes HTTP que ejecutan funciones Lambda. Puede almacenar los registros de CloudWatch y utilizarlos como ayuda para solucionar errores HTTP 5xx cuando la función devuelve una respuesta no válida. Para obtener más informaci ón, consulte Métricas de CloudWatch y CloudWatch Logs para funciones Lambda.	8 de octubre de 2018
Nueva característica	A partir de ahora, puede hacer que Lambda@Edge exponga el cuerpo de una solicitud en los métodos HTTP que permiten la escritura (POST, PUT, DELETE, etc.) para que puede tener acceso a él en la función Lambda. Puede elegir acceso de solo lectura o puede especificar que sustituir á el cuerpo. Para obtener más información, consulte Acceso al cuerpo de una solicitud eligiendo la opción Incluir cuerpo.	14 de agosto de 2018

Nueva característica	CloudFront ahora permite ofrecer contenido comprimido mediante brotli u otros algoritmos de compresión, además o en lugar de gzip. Para obtener más información, consulte Ofrecer archivos comprimidos.	25 de julio de 2018
Reorganización	La Guía para desarrolladores de Amazon CloudFront se ha reorganizado para simplificar la búsqueda de contenido relacionado y mejorar la capacidad de búsqueda y la navegación.	28 de junio de 2018
Nueva característica	Lambda@Edge le permite ahora personalizar aún más la entrega de contenido almacenado en un bucket de Amazon S3, para que pueda acceder a encabezados adicionales permitidos, incluidos los encabezados personalizados, dentro de eventos producidos en el origen. Para obtener más información, consulte estos ejemplos que muestran cómo personalizar el contenido en función de la ubicación del lector y del tipo de dispositivo del lector.	20 de marzo de 2018

Nueva característica	Ahora puede usar Amazon CloudFront para negociar conexiones HTTPS con orígenes mediante el algoritmo de firma digital de curva elíptica (ECDSA). ECDSA utiliza claves más pequeñas que son más rápidas, aunque, tan seguras como el algoritmo de RSA más antiguo. Para obtener más información, consulte Protocolos y cifrados SSL/TLS admitidos para la comunicaciones entre CloudFront y su origen y Acerca de los algoritmos criptográficos RSA y ECDSA.	15 de marzo de 2018
Nueva característica	Lambda@Edge le permite personalizar respuestas de error recibidas desde el origen, ya que le permite ejecutar funciones de Lambda como respuesta a los errores HTTP que Amazon CloudFron t recibe desde el origen. Para obtener más información, consulte los ejemplos que muestran redireccionamientos a otra ubicación y la generació n de respuestas con el código de estado 200 (OK).	21 de diciembre de 2017

Nueva característica	Una nueva capacidad de CloudFront, el cifrado en el nivel de campo, le permite mejorar aún más la seguridad de los datos confidenciales, como números de tarjetas de crédito, o los datos personale s, como números de la seguridad social. Para obtener más información, consulte Uso del cifrado en el nivel de campo para ayudar a proteger la información confidencial.	14 de diciembre de 2017
Historial de revisión archivado	Se archivó el historial de revisión más antiguo.	1 de diciembre de 2017