



Guía del usuario

Amazon Elastic File System



Amazon Elastic File System: Guía del usuario

Copyright © 2024 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 registradas 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 Elastic File System?	1
¿Es la primera vez que usa Amazon EFS?	3
Funcionamiento	4
Información general	4
Cómo funciona Amazon EFS con Amazon EC2	6
Sistemas de archivos regionales de Amazon EFS	6
Sistemas de archivos One Zone de Amazon EFS	7
Cómo funciona Amazon EFS con una AWS Direct Connect VPN AWS gestionada	9
Cómo funciona Amazon EFS con AWS Backup	10
Resumen de implementación	11
Autenticación y control de acceso	13
Coherencia de datos en Amazon EFS	13
Bloqueo de archivos	14
Clases de almacenamiento de EFS	14
Administración del ciclo de vida	14
Replicación	15
Introducción	16
Requisitos previos	16
Cree un sistema de archivos e inicie la instancia EC2	17
Transfiera archivos a su sistema de archivos	18
Requisitos previos	18
Eliminar recursos	19
Descripción de los tipos de sistemas de archivos y las clases de almacenamiento	20
Tipos de sistemas de archivos EFS	20
Zonas de disponibilidad compatibles con los sistemas de archivos de One Zone	21
Clases de almacenamiento de EFS	23
Optimización de costos de almacenamiento	24
Comparación de clases de almacenamiento	24
Precios de clases de almacenamiento	26
Visualización del tamaño de clases de almacenamiento	27
Uso de recursos	29
ID de recursos	30
Idempotencia y token de creación	30
Creación de sistemas de archivos	31

Permisos necesarios para crear sistemas de archivos	31
Opciones de configuración	31
Eliminar sistemas de archivos	44
Administrar destinos de montaje	45
Creación de grupos de seguridad	53
Creación de políticas de sistema de archivos	55
Crear puntos de acceso	58
Eliminar puntos de acceso	61
Etiquetado de recursos	62
Conceptos básicos de etiquetas	62
Restricciones de las etiquetas	63
Uso de etiquetas para el control de acceso	64
Etiquetar los recursos	64
Instalación de las herramientas EFS	66
Acerca del cliente EFS	66
Distribuciones admitidas	68
Instalación automatizada del cliente EFS	69
Qué hace el cliente de Amazon EFS durante la instalación	70
Sistemas operativos compatibles con Systems Manager Distributor	70
Cómo utilizar para instalar o AWS Systems Manager actualizar automáticamente amazon-efs-utils	71
Instalación manual del cliente EFS	73
Instalación del cliente Amazon EFS en instancias Linux de Amazon EC2	73
Instalación del cliente de Amazon EFS en otras distribuciones Linux	74
Instalación del cliente de EFS en instancias de Mac de EC2	75
Instalación y actualización botocore	75
Actualización de stunnel	76
Deshabilitar la comprobación del nombre de host del certificado	78
Habilitación del protocolo OCSP (Online Certificate Status Protocol)	78
Montaje de sistemas de archivos	80
Uso del ayudante de montaje de EFS	81
Funcionamiento	82
Obtención de registros de soporte	84
Requisitos previos	85
Montaje en EC2 Linux	86
Montaje en Mac en EC2	88

Montaje desde una región diferente	90
Montaje de sistemas de archivos One Zone	91
Montaje con autorización de IAM	95
Montaje con puntos de acceso de EFS	96
Montaje con clientes en las instalaciones	97
Cómo montar EFS automáticamente	98
Montaje en varias instancias de EC2	108
Montaje de otra cuenta o VPC	109
Uso de NFS	113
Compatibilidad con NFS	114
Instalación del cliente NFS	115
Opciones de montaje NFS	117
Montaje en Amazon EC2 con un nombre de DNS	120
Montaje con una dirección IP	123
Consideraciones de montaje adicionales	125
Desmontaje de sistemas de archivos	127
Solución de problemas montaje	128
El montaje del sistema de archivos en la instancia de Windows falla	129
Acceso denegado por el servidor	129
Se produce un error de montaje automático y la instancia no responde	129
Se produce un error de montaje de varios sistemas de archivos de Amazon EFS en /etc/ fstab	130
El comando de montaje falla con el mensaje de error "wrong fs type"	131
El comando de montaje falla con el mensaje de error "incorrect mount option"	131
El montaje con un punto de acceso falla	132
El montaje del sistema de archivos falla de inmediato después de la creación del sistema de archivos	132
El montaje del sistema de archivos deja de responder y, a continuación, falla con un error de tiempo de espera agotado	133
El montaje del sistema de archivos con NFS que utiliza el nombre de DNS falla	134
El montaje del sistema de archivos falla y emite el mensaje "nfs not responding (nfs no responde)"	135
El estado de ciclo de vida de destino de montaje está atascado	135
El estado del ciclo de vida objetivo del montaje muestra un error	135
El montaje no responde	136
El cliente montado se desconecta	136

Las operaciones en el sistema de archivos recién montado devuelven el error "bad file handle"	137
Error de desmontaje de un sistema de archivos	137
Transferencia de datos	139
Utilizando AWS DataSync	139
Utilizando AWS Transfer Family	140
Requisitos previos para su uso AWS Transfer Family con Amazon EFS	141
Configuración del sistema de archivos Amazon EFS para que funcione con AWS Transfer Family	141
Gestión de sistemas de archivos	147
Administrar destinos de montaje	147
Creación o eliminación de destinos de montaje en una VPC	149
Cambio de la VPC para el destino de montaje	150
Actualización de la configuración de destinos de montaje	151
Administrar rendimiento	152
Administrar el almacenamiento del sistema de archivos	154
Políticas de ciclo de vida	154
Operaciones del sistema de archivos para la administración del ciclo de vida	155
Administrar políticas del ciclo de vida de un sistema de archivos	156
Administración del acceso a los sistemas de archivos cifrados	159
Realización de acciones administrativas en las claves KMS de Amazon EFS	160
Medición de un sistema de archivos	161
Medición de objetos	161
Tamaño medido del sistema de archivos	162
Medición del rendimiento	164
Gestione los costes del sistema de archivos con AWS Budgets	165
Requisitos previos	166
Creación de un presupuesto de costes mensual para un sistema de archivos de EFS	166
Estado del sistema de archivos	167
Monitoreo de EFS	169
Herramientas de monitoreo	170
Herramientas automatizadas	170
Herramientas de monitoreo manuales	171
Monitorear las métricas con CloudWatch	171
CloudWatch métricas	172
¿Cómo utilizo las métricas de Amazon EFS?	178

Uso de cálculos de métricas con Amazon EFS	180
Supervisión del estado exitoso o fallido del intento de montaje	185
Acceder a CloudWatch las métricas	187
Creación de alarmas	189
Registro de llamadas a la API de AWS CloudTrail con	191
Información de Amazon EFS en CloudTrail	191
Descripción de las entradas de archivos de registro de Amazon EFS	192
Entradas de archivos de registro de Amazon EFS para sistemas de encrypted-at-rest archivos	200
Rendimiento	201
Resumen de rendimiento	201
Clases de almacenamiento	203
Modos de rendimiento	204
Modos de rendimiento	205
Elección de un modo de rendimiento	205
Rendimiento elástico	206
Rendimiento aprovisionado	206
Restricciones a la hora de cambiar el rendimiento y cambiar la cantidad aprovisionada	209
Consejos de rendimiento	210
Tamaño medio de E/S	210
Optimizar las cargas de trabajo que exigen un alto rendimiento e IOPS	210
Conexiones simultáneas	210
Modelo de solicitud	211
Configuración de montaje del cliente NFS	211
Optimización del rendimiento de los archivos pequeños	212
Optimización del rendimiento de directorio	212
Optimización del tamaño de read_ahead_kb de NFS	213
Solución de problemas de rendimiento	214
No se puede crear un sistema de archivos de EFS	215
Acceso denegado a los archivos permitidos en el sistema de archivos NFS	215
Errores al acceder a la consola de Amazon EFS	216
La instancia de Amazon EC2 deja de responder	216
La aplicación deja de responder al escribir grandes cantidades de datos	216
Rendimiento bajo al abrir muchos archivos en paralelo	217
La configuración de NFS personalizada provoca retrasos de escritura	218
La creación de copias de seguridad con Oracle Recovery Manager es lenta	218

Solución de problemas de AMI y de kernel	219
No se puede cambiar la propiedad	219
El sistema de archivos sigue realizando operaciones repetidamente debido a un error del cliente	220
Cliente con interbloqueo	220
La enumeración de archivos en un directorio grande tarda mucho tiempo	220
Copia de seguridad de sistemas de archivos	222
Copias de seguridad incrementales	222
Coherencia de la copia de seguridad	223
Rendimiento de Backup	223
Intervalo de conclusión de la copia de seguridad	223
Clases de almacenamiento de EFS	224
Permisos de IAM para crear y restaurar copias de seguridad	224
Copias de seguridad bajo demanda	224
Copias de seguridad simultáneas	225
Copias de seguridad automáticas	225
Activación o desactivación de las copias de seguridad automáticas de sistemas de archivos existentes	226
Configurar manualmente las copias de seguridad	227
Restauración de un punto de recuperación	228
Eliminación de copias de seguridad	229
Replicación de sistemas de archivos	231
Configuración de replicación	232
Replicación en un nuevo sistema de archivos	232
Replicación en un sistema de archivos existente	234
Protección del sistema de archivos	234
Permisos necesarios	235
Costos	236
Rendimiento	236
Montaje de un sistema de archivos de destino	237
Conmutación por error y conmutación por recuperación del sistema de archivos	237
Crear configuraciones de replicación	238
Visualización de las configuraciones de replicación	241
Eliminar configuraciones de replicación	244
Supervisión de estado de replicación	245
Explicaciones	248

Tutorial: Cree y monte un sistema de archivos mediante AWS CLI	248
Antes de empezar	249
Configurando el AWS CLI	250
Paso 1: Crear los recursos de Amazon ECS	251
Paso 2: Crear los recursos de Amazon EFS	257
Paso 3: Montar y probar el sistema de archivos	260
Paso 4: Limpiar	264
Tutorial: Configurar un servidor web Apache y ofrecer archivos	266
Una sola instancia de EC2 para ofrecer archivos	266
Varias instancias de EC2 para ofrecer archivos	269
Tutorial: Crear subdirectorios grabables por usuario	274
Remontaje automático al reiniciar	276
Tutorial: Montar EFS en un cliente en las instalaciones	276
Antes de empezar	278
Paso 1: Crear los recursos de Amazon Elastic File System	278
Paso 2: Instalar el cliente NFS	280
Paso 3: Montar el sistema de archivos de Amazon EFS en su cliente en las instalaciones ..	281
Paso 4: Limpiar recursos y proteger la cuenta de AWS	282
Opcional: Cifrado de datos en tránsito	283
Tutorial: Montar un sistema de archivos desde una VPC distinta	286
Antes de empezar	287
Paso 1: Determinar el ID de la zona de disponibilidad del destino de montaje de EFS	288
Paso 2: Determinar la dirección IP del destino de montaje	289
Paso 3: Agregar una entrada de host para el destino de montaje	290
Paso 4: Montar el sistema de archivos con el ayudante de montaje de EFS	290
Paso 5: Limpiar recursos y proteger la cuenta de AWS	292
Tutorial: Aplicar cifrado en reposo a un sistema de archivos de Amazon EFS	293
Aplicación del cifrado en reposo	294
Habilite la eliminación de raíz mediante IAM para NFS	297
Seguridad	301
Cifrado de datos en Amazon EFS	302
Cifrado de datos en reposo	302
Cifrado de datos en tránsito	308
Cómo funciona el cifrado en tránsito	309
Resolución de problemas de cifrado	310
Administración de identidades y accesos	313

Público	313
Autenticación con identidades	314
Administración de acceso mediante políticas	318
Cómo funciona Amazon Elastic File System con IAM	320
Ejemplos de políticas basadas en identidades	328
Ejemplos de políticas basadas en recursos	333
Políticas administradas de AWS	336
Uso de etiquetas con Amazon EFS	343
Uso de roles vinculados a servicios para Amazon EFS	347
Solución de problemas	352
Controlar el acceso a los datos del sistema de archivos	354
Política predeterminada del sistema de archivos	355
Acciones de EFS para clientes	355
Claves de condición de EFS para clientes	355
Ejemplos de política del sistema de archivos	356
Control del acceso a la red	356
Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje	357
Puertos de origen	358
Consideraciones de seguridad para el acceso a la red	359
Uso de los puntos de enlace de la VPC	360
Usuarios, grupos y permisos de nivel NFS	361
Permisos de archivos y directorios	363
Ejemplo de permisos y casos de uso del sistema de archivos de Amazon EFS	363
Permisos de ID de usuario y grupo para los archivos y directorios de un sistema de archivos	364
Sin agrupación de raíz	366
Almacenamiento en caché de permisos	366
Cambio de propiedad de objeto del sistema de archivos	366
Puntos de acceso de EFS	367
Trabajo con puntos de acceso	367
Creación de un punto de acceso	368
Montaje con puntos de acceso	368
Aplicación de una identidad de usuario	368
Aplicación de un directorio raíz	369
Uso de puntos de acceso en políticas de IAM	371

Bloqueo del acceso público a los sistemas de archivos de Amazon EFS	372
Bloqueo de acceso público con AWS Transfer Family	373
Qué significa "pública"	374
Validación de conformidad	375
Resiliencia	377
Aislamiento de red	378
Cuotas	379
Cuotas de Amazon EFS que puede incrementar	379
Solicitud de aumento de cuota	381
Cuotas de recursos de Amazon EFS que no puede cambiar.	381
Cuotas para clientes NFS	383
Cuotas para sistemas de archivos de Amazon EFS	384
Funciones de NFSv4.0 y 4.1 no compatibles	385
Consideraciones adicionales	386
Solución de errores de operación de archivos	387
El comando falla con el error "Cuota de disco superada"	387
El comando falla con "error de E/S"	387
El comando falla con el error "El nombre de archivo es demasiado largo"	388
El comando produce el error "Archivo no encontrado"	388
El comando falla con el error "Demasiados vínculos"	389
El comando falla con el error "Archivo demasiado grande"	389
API de Amazon EFS	390
Punto de enlace de la API	391
Versión de API	391
Temas relacionados	391
Trabajando con la tasa de solicitudes de la API de consultas para Amazon EFS	392
Sondeo	392
Reintentos para procesamiento por lotes	392
Calcular el intervalo de sueño	392
Acciones	393
CreateAccessPoint	395
CreateFileSystem	403
CreateMountTarget	419
CreateReplicationConfiguration	431
CreateTags	438
DeleteAccessPoint	441

DeleteFileSystem	443
DeleteFileSystemPolicy	447
DeleteMountTarget	450
DeleteReplicationConfiguration	454
DeleteTags	457
DescribeAccessPoints	460
DescribeAccountPreferences	465
DescribeBackupPolicy	468
DescribeFileSystemPolicy	471
DescribeFileSystems	475
DescribeLifecycleConfiguration	481
DescribeMountTargets	485
DescribeMountTargetSecurityGroups	491
DescribeReplicationConfigurations	495
DescribeTags	499
ListTagsForResource	504
ModifyMountTargetSecurityGroups	508
PutAccountPreferences	512
PutBackupPolicy	515
PutFileSystemPolicy	518
PutLifecycleConfiguration	524
TagResource	533
UntagResource	537
UpdateFileSystem	540
UpdateFileSystemProtection	548
Data Types	552
AccessPointDescription	553
BackupPolicy	556
CreationInfo	557
Destination	559
DestinationToCreate	561
FileSystemDescription	563
FileSystemProtectionDescription	568
FileSystemSize	569
LifecyclePolicy	571
MountTargetDescription	573

PosixUser	576
ReplicationConfigurationDescription	578
ResourceIdPreference	580
RootDirectory	581
Tag	583
Historial de documentos	584
.....	dcix

¿Qué es Amazon Elastic File System?

Amazon Elastic File System (Amazon EFS) proporciona un almacenamiento de archivos totalmente elástico y sin servidor para que pueda compartir datos de archivos sin aprovisionar ni administrar la capacidad de almacenamiento ni el rendimiento. Amazon EFS está diseñado para ampliarse a petabytes según la demanda sin interrumpir las aplicaciones, es decir que aumenta y disminuye automáticamente a medida que se agregan o eliminan archivos. Amazon EFS dispone de una sencilla interfaz de servicios web que le permite crear y configurar sistemas de archivos rápida y fácilmente. El servicio se encarga de administrar toda la infraestructura de almacenamiento de archivos, por lo que puede evitar la complejidad de implementación, aplicación de parches y mantenimiento de configuraciones complejas de sistemas de archivos.

Amazon EFS es compatible con la versión 4 (NFSv4.1 y NFSv4.0) del protocolo Network File System, para que las aplicaciones y herramientas que utiliza actualmente funcionen sin problemas con Amazon EFS. Se puede acceder a Amazon EFS en la mayoría de los tipos de instancias informáticas de Amazon Web Services, incluidas Amazon EC2, Amazon ECS AWS Lambda, Amazon EKS y AWS Fargate

El servicio se ha diseñado para ser muy escalable, de alta disponibilidad y de larga duración. Amazon EFS ofrece los siguientes tipos de sistemas de archivos para satisfacer sus necesidades de disponibilidad y durabilidad:

- **Regional (recomendado):** los sistemas de archivos regionales (recomendado) almacenan datos de forma redundante en varias zonas de disponibilidad separadas geográficamente dentro de una misma zona. Región de AWS El almacenamiento de datos en varias zonas de disponibilidad proporciona una disponibilidad continua de los datos, incluso cuando una o más zonas de disponibilidad de una zona de disponibilidad Región de AWS no están disponibles.
- **Una zona:** los sistemas de archivos de una zona almacenan los datos en una única zona de disponibilidad. El almacenamiento de datos en una única zona de disponibilidad proporciona una disponibilidad continua de los datos. Sin embargo, en el improbable caso de pérdida o daño de toda o parte de la zona de disponibilidad, es posible que se pierdan los datos almacenados en estos tipos de sistemas de archivos.

Para obtener más información sobre los tipos de sistema de archivos, consulte [Tipos de sistemas de archivos EFS](#).


Amazon EFS se ha diseñado para ofrecer el rendimiento, IOPS y baja latencia necesarios para una amplia gama de cargas de trabajo. Los sistemas de archivos de EFS pueden aumentar a escala de petabytes, ofrecer altos niveles de rendimiento y permitir el acceso en paralelo masivo a sus datos desde instancias de computación. Para la mayoría de las cargas de trabajo, recomendamos utilizar los modos predeterminados, que son el modo de rendimiento de uso general y los modos de rendimiento elástico.

- **Uso general:** el modo de rendimiento de uso general es ideal para aplicaciones sensibles a la latencia, como entornos de servidores web, sistemas de administración de contenido, directorios principales y servidores de archivos generales.
- **Elástico:** el modo de rendimiento elástico está diseñado para aumentar o reducir automáticamente el rendimiento del rendimiento a fin de satisfacer las necesidades de la actividad de la carga de trabajo.

Para obtener más información sobre el rendimiento y los modos de rendimiento de EFS, consulte [Rendimiento de Amazon EFS](#).

Amazon EFS proporciona file-system-access semántica, como una sólida coherencia de datos y bloqueo de archivos. Para obtener más información, consulte [Coherencia de datos en Amazon EFS](#). Amazon EFS además permite controlar el acceso a sus sistemas de archivos a través de los permisos de POSIX (Portable Operating System Interface). Para obtener más información, consulte [Seguridad en Amazon EFS](#).

Amazon EFS admite capacidades de autenticación, autorización y cifrado para ayudarle a cumplir sus requisitos de seguridad y conformidad. Amazon EFS admite dos formas de cifrado para sistemas de archivos, el cifrado en tránsito y en reposo. Puede habilitar el cifrado en reposo al crear un sistema de archivos de Amazon EFS. Si lo hace, se cifran todos los datos y metadatos. Puede habilitar el cifrado en tránsito, cuando monte el sistema de archivos. El acceso de los clientes NFS a EFS se controla mediante políticas AWS Identity and Access Management (IAM) y políticas de seguridad de red, como los grupos de seguridad. Para obtener más información, consulte [Cifrado de datos en Amazon EFS](#), [Administración de identidades y acceso Amazon Elastic File System](#) y [Control del acceso de red a sistemas de archivos de Amazon EFS para clientes NFS](#).

 Note

No se admite el uso de Amazon EFS con instancias de Amazon EC2 basadas en Microsoft Windows.

¿Es la primera vez que usa Amazon EFS?

Si es la primera vez que utiliza Amazon EFS, le recomendamos que lea las siguientes secciones en orden:

1. Para información general del producto Amazon EFS y precios, consulte [Amazon EFS](#).
2. Para una descripción general técnica de Amazon EFS, consulte [Cómo funciona Amazon EFS](#).
3. Pruebe los ejercicios de introducción:
 - [Introducción](#)
 - [Explicaciones](#)

Si desea obtener más información sobre Amazon EFS, los siguientes temas analizan el servicio más detalladamente:

- [Uso de recursos de Amazon EFS](#)
- [Gestión de sistemas de archivos de Amazon EFS](#)
- [API de Amazon EFS](#)

Cómo funciona Amazon EFS

A continuación, puede encontrar una descripción acerca de cómo funciona Amazon EFS, sus detalles de implementación y las consideraciones de seguridad.

Temas

- [Información general](#)
- [Cómo funciona Amazon EFS con Amazon EC2](#)
- [Cómo funciona Amazon EFS con una AWS Direct Connect VPN AWS gestionada](#)
- [Cómo funciona Amazon EFS con AWS Backup](#)
- [Resumen de implementación](#)
- [Autenticación y control de acceso](#)
- [Coherencia de datos en Amazon EFS](#)
- [Clases de almacenamiento de EFS](#)
- [Replicación](#)

Información general

Amazon Elastic File System (EFS) proporciona un sistema de archivos set-and-forget elástico, simple y sin servidor. Con Amazon EFS, puede crear un sistema de archivos, montar el sistema de archivos en una instancia de Amazon EC2 y leer y escribir datos en su sistema de archivos. Puede montar un sistema de archivos de Amazon EFS en su nube privada virtual (VPC) a través del protocolo Network File System versiones 4.0 y 4.1 (NFSv4). Recomendamos utilizar un cliente Linux NFSv4.1 de generación actual, como los que se encuentran en las últimas AMI de Amazon Linux, Amazon Linux 2, Redhat, Ubuntu y macOS Big Sur, junto con el ayudante de montaje de Amazon EFS. Para ver instrucciones, consulte [Instalación de las herramientas de Amazon EFS](#).

Para obtener una lista de imágenes de máquina de Amazon (AMI) de macOS y Linux de Amazon EC2 que admiten este protocolo, consulte [Compatibilidad con NFS](#). Para algunas AMI, tendrá que instalar un cliente NFS para montar su sistema de archivos en la instancia de Amazon EC2. Para ver instrucciones, consulte [Instalación del cliente NFS](#).

Puede obtener acceso a su sistema de archivos de Amazon EFS simultáneamente desde varios clientes NFS, de manera que las aplicaciones que se escalan más allá de una única conexión puedan obtener acceso a un sistema de archivos. Las instancias de Amazon EC2 que se ejecutan en

varias zonas de disponibilidad dentro de la misma Región de AWS pueden obtener acceso al sistema de archivos, de modo que muchos usuarios puedan obtener acceso y compartir un origen de datos común.


Para obtener una lista de los Regiones de AWS lugares en los que puede crear un sistema de archivos Amazon EFS, consulte la [Referencia general de Amazon Web Services](#).

Para obtener acceso al sistema de archivos de Amazon EFS en una VPC, cree uno o varios destinos de montaje en la VPC.

- En el caso de sistemas de archivos regionales, se puede crear un destino de montaje en cada zona de disponibilidad de la Región de AWS.
- En el caso de sistemas de archivos One Zone, solo se crea un único destino de montaje que se encuentre en la misma zona de disponibilidad que el sistema de archivos.

Para obtener más información, consulte [Clases de almacenamiento de EFS](#).

Un destino de montaje proporciona una dirección IP para un punto de conexión de NFSv4 en el que puede montar un sistema de archivos de Amazon EFS. El sistema de archivos se monta utilizando su nombre DNS (Servicio de nombres de dominio), que se resuelve en la dirección IP del destino de montaje de EFS en la misma zona de disponibilidad que la instancia EC2. Puede crear un destino de montaje en cada zona de disponibilidad de una Región de AWS. Si la VPC tiene varias subredes en una zona de disponibilidad, puede crear un destino de montaje en tan solo una de las subredes. Todas las instancias EC2 de la zona de disponibilidad compartirán ese destino de montaje.

 Note

Un sistema de archivos de Amazon EFS solo puede tener destinos de montaje en una VPC a la vez.

Los propios destinos de montaje están diseñados para ofrecer alta disponibilidad. A medida que diseña para alta disponibilidad y conmutación por error en otras zonas de disponibilidad (AZ), tenga en cuenta que, aunque las direcciones IP y DNS de los destinos de montaje en cada AZ son estáticos, son componentes redundantes respaldados por varios recursos.

Después de montar el sistema de archivos mediante su nombre de DNS, lo podrá usar como cualquier otro sistema de archivos compatible con POSIX. Para obtener información sobre los niveles

de permisos y consideraciones relacionadas, consulte [Trabajar con usuarios, grupos y permisos a nivel del sistema de archivos de red \(NFS\)](#).

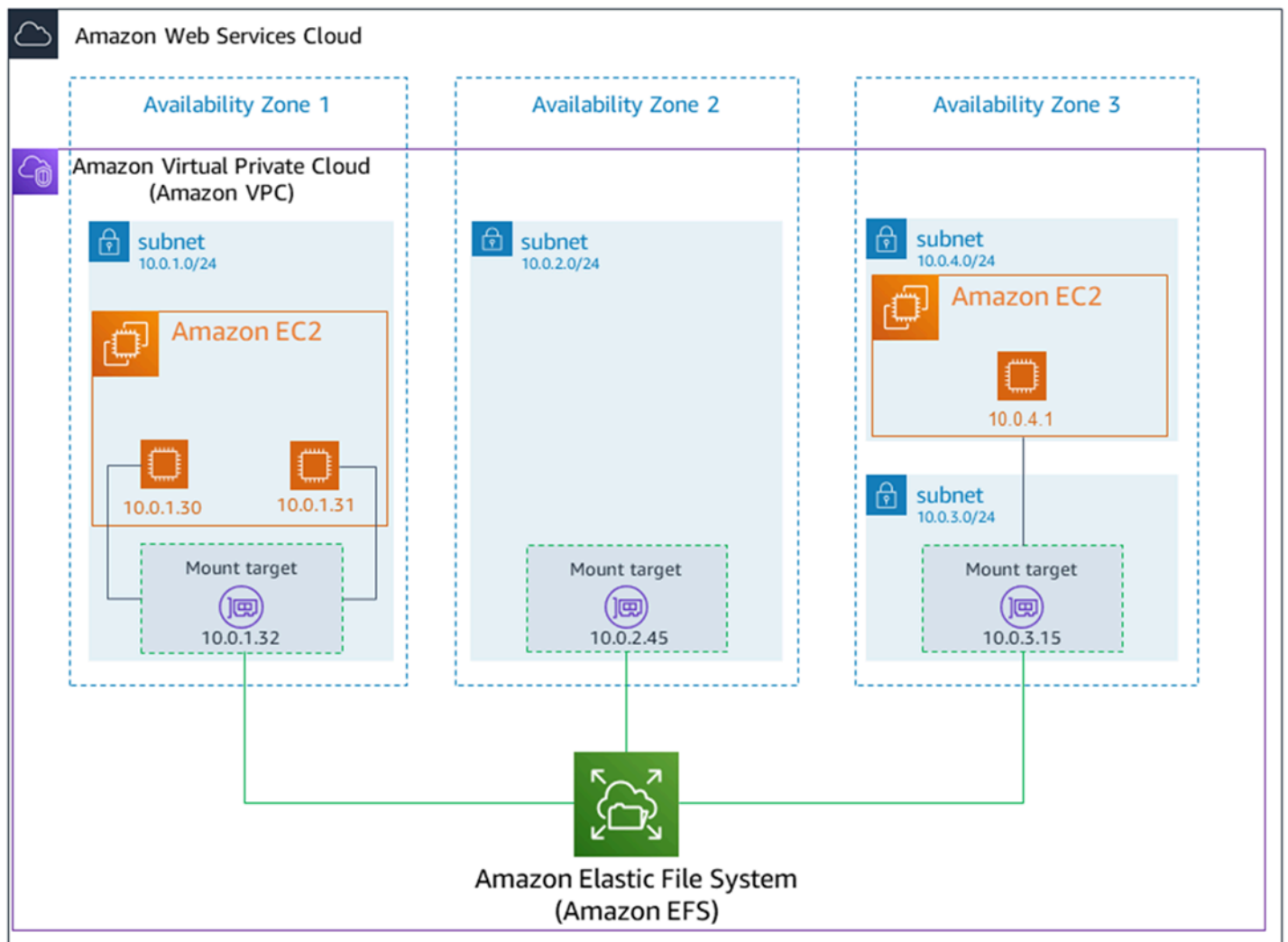
Puede montar sus sistemas de archivos Amazon EFS en los servidores de sus centros de datos locales cuando esté conectado a su Amazon VPC AWS Direct Connect AWS VPN o puede montar sus sistemas de archivos EFS en servidores locales para migrar conjuntos de datos a EFS, habilitar escenarios de nube explosiva o hacer copias de seguridad de sus datos locales en Amazon EFS.

Cómo funciona Amazon EFS con Amazon EC2

En esta sección, se explica cómo se montan los sistemas de archivos regionales y One Zone de Amazon EFS en las instancias EC2 de una Amazon VPC.

Sistemas de archivos regionales de Amazon EFS

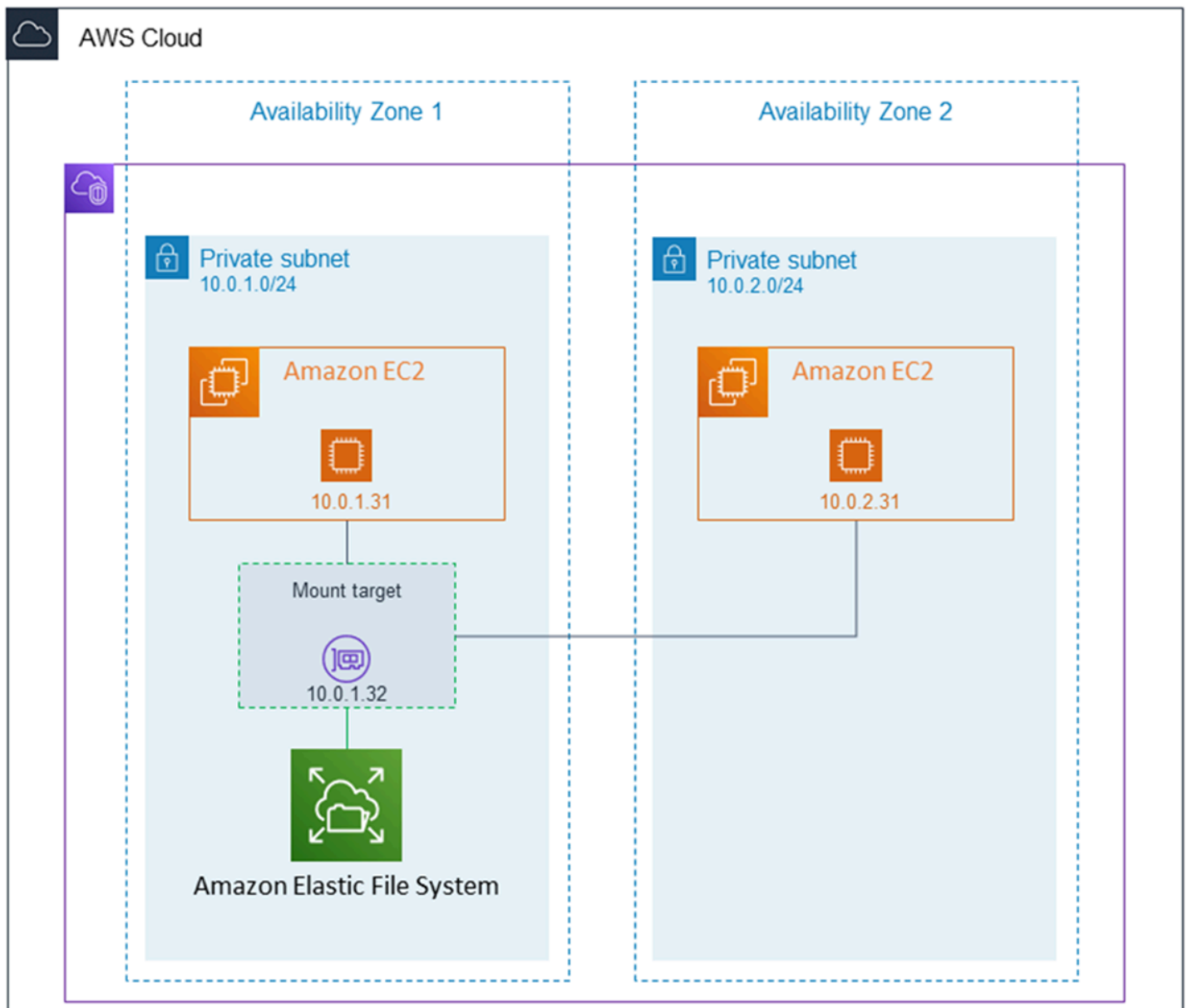
La siguiente ilustración muestra varias instancias de EC2 que acceden a un sistema de archivos de Amazon EFS que está configurado para varias zonas de disponibilidad en una Región de AWS.



En esta ilustración, la nube privada virtual (VPC) tiene tres zonas de disponibilidad. Como el sistema de archivos es Regional, se puede crear un destino de montaje en cada zona de disponibilidad. Le recomendamos que obtenga acceso al sistema de archivos desde un destino de montaje dentro de la misma zona de disponibilidad por motivos de costes y rendimiento. Una de las zonas de disponibilidad tiene dos subredes. Sin embargo, se crea un destino de montaje en tan solo una de las subredes. Para obtener más información, consulte [Montaje del sistema de archivos de EFS mediante el ayudante de montaje de EFS..](#)

Sistemas de archivos One Zone de Amazon EFS

La siguiente ilustración muestra varias instancias de EC2 que acceden a un sistema de archivos One Zone de varias zonas de disponibilidad en una sola Región de AWS.



En esta ilustración, la VPC tiene dos zonas de disponibilidad, cada una con una subred. Como el tipo de sistema de archivos es One Zone, solo puede tener un único destino de montaje. Para un mejor rendimiento y coste, le recomendamos que obtenga acceso al sistema de archivos desde un destino de montaje dentro de la misma zona de disponibilidad que la instancia de EC2 en la que lo está montando.

En este ejemplo, la instancia de EC2 de la zona de disponibilidad us-west-2c pagará los cargos de acceso a los datos de EC2 por acceder a un destino de montaje situado en una zona de disponibilidad diferente. Para obtener más información, consulte [Montaje de sistemas de archivos One Zone](#).

Cómo funciona Amazon EFS con una AWS Direct Connect VPN AWS gestionada

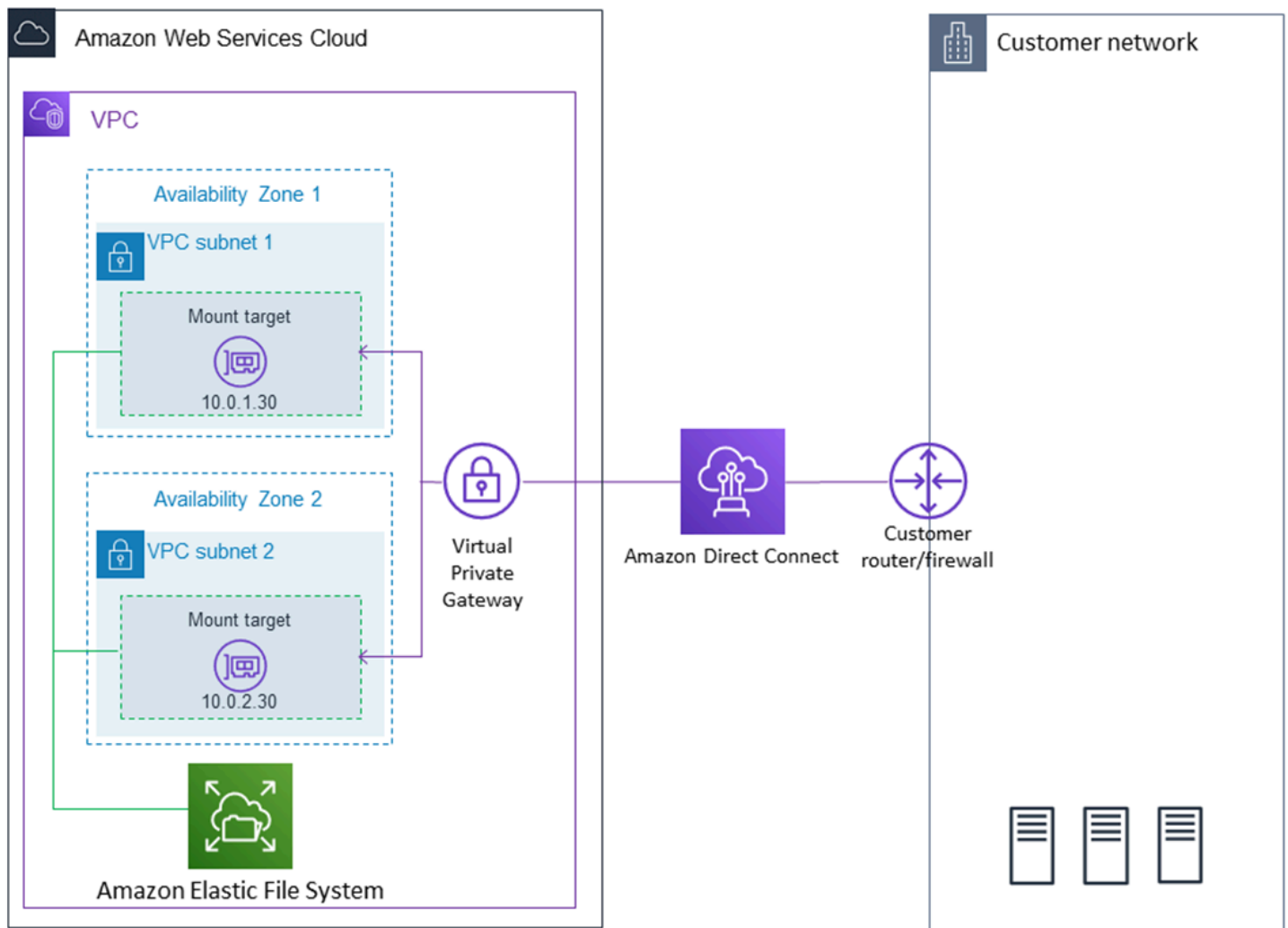
Al utilizar un sistema de archivos Amazon EFS montado en un servidor local, puede migrar los datos locales al sistema de archivos Nube de AWS alojado en un servidor Amazon EFS. También puede utilizar la transmisión por ráfagas. Es decir, puede mover los datos de sus servidores en las instalaciones a Amazon EFS y analizarlos en una flota de instancias de Amazon EC2 en su Amazon VPC. A continuación, puede almacenar los resultados de forma permanente en el sistema de archivos o mover los resultados al servidor local.

Tenga en cuenta las siguientes consideraciones al utilizar Amazon EFS con un servidor en las instalaciones:

- Su servidor local debe tener un sistema operativo basado en Linux. Recomendamos Linux kernel versión 4.0 o posterior.
- A efectos de simplicidad, le recomendamos montar un sistema de archivos de Amazon EFS en un servidor en las instalaciones mediante una dirección IP de destino de montaje en lugar de un nombre de DNS.

No se aplica ningún coste adicional por el acceso on-premise a sus sistemas de archivos de Amazon EFS. Se te cobrará por la AWS Direct Connect conexión a tu Amazon VPC. Para más información, consulte [Precios de AWS Direct Connect](#).

En la siguiente ilustración se muestra un ejemplo de cómo obtener acceso a un sistema de archivos de Amazon EFS on-premise (los servidores en las instalaciones tienen los sistemas de archivos montados).



Puedes usar cualquier destino de montaje en tu VPC si puedes llegar a la subred de ese destino de montaje mediante una AWS Direct Connect conexión entre tu servidor local y la VPC. Para obtener acceso a Amazon EFS desde un servidor en las instalaciones, añade una regla a su grupo de seguridad de destino de montaje para permitir el tráfico entrante al puerto NFS (2049) desde el servidor en las instalaciones. Para obtener más información, incluidos los procedimientos detallados, consulte [Tutorial: Crear y montar un sistema de archivos en las instalaciones con AWS Direct Connect y una VPN](#).

Cómo funciona Amazon EFS con AWS Backup

Para una implementación integral de copias de seguridad para sus sistemas de archivos, puede utilizar Amazon EFS con AWS Backup. AWS Backup es un servicio de copias de seguridad totalmente gestionado que facilita la centralización y la automatización de las copias de seguridad de los datos en todos AWS los servicios de la nube y en las instalaciones. Con él AWS Backup, puede

configurar de forma centralizada las políticas de respaldo y monitorear la actividad de respaldo de sus AWS recursos. Amazon EFS siempre prioriza las operaciones del sistema de archivos sobre las operaciones de copia de seguridad. Para obtener más información sobre cómo realizar copias de seguridad de los sistemas de archivos EFS mediante AWS Backup, consulte [Copia de seguridad de los sistemas de archivos de Amazon EFS](#).

Resumen de implementación

En Amazon EFS, un sistema de archivos es el recurso principal. Cada sistema de archivos tiene propiedades como, por ejemplo, el ID, token de creación, hora de creación, tamaño del sistema de archivos en bytes, número de destinos de montaje creados para el sistema de archivos y el estado del ciclo de vida del sistema de archivos. Para obtener más información, consulte [CreateFileSystem](#).

Amazon EFS también admite otros recursos para configurar el recurso principal. Estos incluyen objetivos de montaje y puntos de acceso:

- Destino de montaje: para obtener acceso a su sistema de archivos, debe crear destinos de montaje en la VPC. Cada destino de montaje tiene las siguientes propiedades: el ID del destino de montaje, el ID de la subred en el que se ha creado, el ID del sistema de archivos para el que se ha creado, una dirección IP en la que se puede montar el sistema, grupos de seguridad de la VPC y el estado del destino de montaje. Puede utilizar la dirección IP o el nombre de DNS en su comando mount.

Cada sistema de archivos tiene un nombre de DNS de la siguiente forma.

```
file-system-id.efs.aws-region.amazonaws.com
```

Puede especificar el nombre de DNS de su comando mount para montar el sistema de archivos de Amazon EFS. Supongamos que crea un subdirectorio `efs-mount-point` fuera del directorio principal en su instancia EC2 o servidor local. A continuación, puede utilizar el comando de montaje para montar el sistema de archivos. Por ejemplo, en una AMI de Amazon Linux, puede utilizar el siguiente comando mount.

```
$ sudo mount -t nfs -o  
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport file-  
system-DNS-name:/ ~/efs-mount-point
```

Para obtener más información, consulte [Administrar destinos de montaje](#).

- **Puntos de acceso:** Un punto de acceso aplica una ruta de usuario, grupo y sistema de archivos del sistema operativo a cualquier solicitud del sistema de archivos realizada mediante el punto de acceso. El usuario y el grupo del sistema operativo del punto de acceso anulan cualquier información de identidad proporcionada por el cliente NFS. La ruta del sistema de archivos se expone al cliente como directorio raíz del punto de acceso. Esto garantiza que cada aplicación siempre utilice la identidad correcta del sistema operativo y el directorio correcto al acceder a conjuntos de datos basados en archivos compartidos. Las aplicaciones que utilizan el punto de acceso solo pueden acceder a los datos en su propio directorio e inferiores. Para obtener más información, consulte [Trabajo con puntos de acceso de Amazon EFS](#).

Los destinos de montaje y las etiquetas son subrecursos asociados a un sistema de archivos. Sólo se pueden crear en el contexto de un sistema de archivos existente.

Amazon EFS proporciona operaciones de API para que pueda crear y administrar estos recursos. Además de las operaciones de creación y eliminación para cada recurso, Amazon EFS es compatible con una operación de descripción que le permite recuperar información de recursos. Dispone de las siguientes opciones para la creación y la administración de estos recursos:

- Utilice la consola de Amazon EFS: para ver un ejemplo, consulte [Introducción](#).
- Utilice la interfaz de línea de comandos (CLI) de Amazon EFS: para ver un ejemplo, consulte [Tutorial: Cree un sistema de archivos Amazon EFS y móntelo en una instancia de Amazon EC2 mediante AWS CLI](#).
- También puede administrar estos recursos mediante programación de la siguiente manera:
 - Utilice los AWS SDK: los AWS SDK simplifican las tareas de programación al empaquetar la API Amazon EFS subyacente. Los clientes de SDK también autentican sus solicitudes mediante el uso de claves de acceso que proporcione. Para obtener más información, consulte [Código de muestra y bibliotecas](#).
 - Llame al API de Amazon EFS directamente desde la aplicación. Si no puede utilizar los SDK por algún motivo, puede hacer que el API de Amazon EFS llame directamente desde su aplicación. No obstante, tiene que escribir el código necesarios para autenticar las solicitudes si utiliza esta opción. Para obtener más información acerca de la API de Amazon EFS, consulte [API de Amazon EFS](#).

Autenticación y control de acceso

Debe disponer de credenciales válidas para hacer solicitudes de API de Amazon EFS como, por ejemplo, crear un sistema de archivos. Además, debe tener permisos para crear u obtener acceso a los recursos.

Los usuarios y roles que cree en AWS Identity and Access Management (IAM) deben tener permisos para crear recursos o acceder a ellos. Para obtener más información sobre los permisos, consulte [Administración de identidades y acceso Amazon Elastic File System](#).

La autorización de IAM para clientes NFS es una opción de seguridad adicional para Amazon EFS que utiliza IAM para simplificar la administración de acceso a clientes del sistema de archivo de red (NFS) a escala. Con la autorización de IAM para los clientes NFS, puede utilizar IAM para gestionar el acceso a un sistema de archivos EFS de una forma inherentemente escalable. La autorización de IAM para clientes NFS también está optimizada para entornos de nube. Para obtener más información sobre el uso de la autorización de IAM para clientes NFS, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#).

Coherencia de datos en Amazon EFS

Amazon EFS proporciona la semántica de close-to-open coherencia que las aplicaciones esperan de NFS.

En Amazon EFS, las operaciones de escritura de los sistemas de archivos regionales se almacenan de forma duradera en zonas de disponibilidad cuando:

- Una aplicación realiza una operación de escritura síncrona (por ejemplo, utilizando el comando de Linux `open` con la marca `O_DIRECT` o el comando de Linux `fsync`).
- Una aplicación cierra un archivo.

Según el patrón de acceso, Amazon EFS puede ofrecer garantías de coherencia más sólidas que la close-to-open semántica. Las aplicaciones que realizan un acceso sincrónico a los datos y realizan escrituras no anexadas tienen read-after-write coherencia en el acceso a los datos.

Bloqueo de archivos

Las aplicaciones cliente de NFS pueden utilizar el bloqueo de archivos de la versión 4 de NFS (incluido el bloqueo por rango de bytes) para las operaciones de lectura y escritura en los archivos de Amazon EFS.

Recuerde lo siguiente acerca de cómo Amazon EFS bloquea los archivos:

- Amazon EFS solo admite el bloqueo por aviso, por lo que las operaciones de lectura/escritura no comprueban si hay bloqueos conflictivos antes de ejecutarse. Por ejemplo, para evitar problemas de sincronización de archivos con las operaciones atómicas, la aplicación debe conocer la semántica de NFS (como la close-to-open coherencia).
- Cualquier archivo particular puede tener hasta 512 bloqueos en todas las instancias conectadas y entre todos los usuarios que acceden al archivo.

Clases de almacenamiento de EFS

Amazon EFS ofrece diferentes clases de almacenamiento para distintas necesidades de almacenamiento de datos. Estándar es la primera clase de almacenamiento en la que se escriben los datos y es la clase de almacenamiento para los datos a los que se accede con frecuencia. Para los archivos a los que se accede con menos frecuencia, Amazon EFS ofrece las clases de almacenamiento de Acceso poco frecuente (IA) y Archivado de EFS. La clase de almacenamiento IA optimiza los costes para los datos a los que se accede varias veces cada trimestre y la clase de almacenamiento Archivado optimiza los costes para los datos a los que se accede solo unas pocas veces al año o menos. Para obtener más información acerca de las clases de almacenamiento de Amazon EFS, consulte [Clases de almacenamiento de EFS](#).

Administración del ciclo de vida

Para gestionar sus sistemas de archivos de forma que se almacenen de forma rentable durante todo su ciclo de vida, utilice la gestión del ciclo de vida. La administración del ciclo de vida transfiere automáticamente los datos entre las clases de almacenamiento de acuerdo con la configuración del ciclo de vida definida para el sistema de archivos. La configuración del ciclo de vida es un conjunto de políticas de ciclo de vida que definen cuándo hacer la transición de los datos del sistema de archivos a otra clase de almacenamiento. Para obtener más información, consulte [Administrar el almacenamiento del sistema de archivos](#).

Replicación

Puede crear una réplica de su sistema Región de AWS de archivos Amazon EFS según sus preferencias mediante la replicación. La replicación replica de forma automática y transparente los datos y metadatos del sistema de archivos EFS en un nuevo sistema de archivos EFS de destino que se crea en el sistema de archivos EFS Región de AWS que usted elija. EFS mantiene sincronizados automáticamente los sistemas de archivos de origen y destino. La replicación es continua y está diseñada para proporcionar un objetivo de punto de recuperación (RPO) y un objetivo de tiempo de recuperación (RTO) de minutos. Estas características le ayudan a cumplir sus objetivos de conformidad y continuidad empresarial. Para obtener más información, consulte [Replicación de sistemas de archivos](#).

Introducción a Amazon Elastic File System

Descubra cómo empezar rápidamente a utilizar Amazon Elastic File System (Amazon EFS). En este ejercicio de introducción, creará su sistema de archivos EFS y lanzará su instancia EC2. También transferirá los archivos al sistema de archivos EFS mediante los recursos AWS DataSync y, a continuación, los limpiará.

En este ejercicio de introducción se incluyen los siguientes pasos.

1. [Revise los requisitos previos para realizar este ejercicio de introducción](#)
2. [Cree su sistema de archivos EFS y lance su instancia EC2](#)
3. [Transfiera archivos a su sistema de archivos Amazon EFS mediante AWS DataSync](#)
4. [Limpie los recursos y proteja su AWS cuenta](#)

Requisitos previos para empezar

Antes de comenzar el ejercicio de iniciación, asegúrese de cumplir los siguientes requisitos:

- Está configurado con Amazon EC2 y está familiarizado con el lanzamiento de instancias de EC2. Necesita un Cuenta de AWS, un usuario con acceso administrativo, un key pair y un grupo de seguridad. Para obtener más información, consulte [Configuración para utilizar Amazon EC2](#).
- Sus recursos de Amazon VPC, Amazon EC2 y Amazon EFS están todos en la misma Región de AWS. En este ejercicio se utiliza la región EE.UU. Oeste (Oregón) (us-west-2).
- Tiene una VPC predeterminada en la Región de AWS que está utilizando para este ejercicio de introducción. Si no tiene una VPC predeterminada o si desea montar el sistema de archivos desde una VPC nueva con grupos de seguridad nuevos o existentes, consulte. [Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje](#)
- No ha cambiado la regla predeterminada de acceso de entrada para el grupo de seguridad predeterminado.

También puede realizar un ejercicio de introducción similar con los comandos AWS Command Line Interface (AWS CLI) para realizar las llamadas a la API de Amazon EFS. Para obtener más información, consulte [Tutorial: Cree un sistema de archivos Amazon EFS y móntelo en una instancia de Amazon EC2 mediante AWS CLI](#).

Cree su sistema de archivos EFS y lance su instancia EC2

Tras comprobar que cumple los requisitos previos para este ejercicio de introducción, puede crear su sistema de archivos EFS y lanzar su instancia de Amazon EC2. La forma más rápida de completar todos los pasos necesarios para empezar a utilizar el primer sistema de archivos EFS es utilizar el nuevo asistente de lanzamiento de EC2 durante el lanzamiento de la instancia.

Note

No se puede usar Amazon EFS con instancias de Amazon EC2 basadas en Microsoft Windows.

Para crear el sistema de archivos EFS y lanzar la instancia de Amazon EC2 mediante el asistente de lanzamiento de EC2

Para obtener instrucciones sobre cómo crear y montar el sistema de archivos EFS al crear un lanzamiento de instancia EC2, consulte [Uso de Amazon EFS con Amazon EC2](#).

Los siguientes son los pasos que debe realizar al crear un sistema de archivos EFS durante el lanzamiento de la instancia.

1. Cree una instancia EC2 que se ejecute en un sistema operativo Linux con el par de claves y la configuración de red que elija.
2. Cree un sistema de archivos EFS compartido que tenga la configuración recomendada y que se monte automáticamente en la instancia EC2.
3. Inicie la instancia EC2 para que el sistema de archivos EFS esté fácilmente disponible para las transferencias de archivos.

Como alternativa, en la consola de Amazon EFS, puede crear sistemas de archivos con la configuración recomendada o con una configuración personalizada. También puede usar la AWS CLI y la API para crear sistemas de archivos. Para obtener más información sobre todas las opciones para crear un sistema de archivos, consulte [Creación de sistemas de archivos de Amazon EFS](#).

Transfiera archivos a su sistema de archivos Amazon EFS mediante AWS DataSync

Tras crear un sistema de archivos EFS, puede transferirle archivos desde un sistema de archivos existente mediante AWS DataSync. DataSync es un servicio de transferencia de datos que simplifica, automatiza y acelera el traslado y la replicación de datos entre sistemas de almacenamiento locales y servicios de almacenamiento a través de Internet o de AWS Direct Connect. DataSync puede transferir los datos de sus archivos y también los metadatos del sistema de archivos, como la propiedad, las marcas horarias y los permisos de acceso.

Para obtener más información acerca de DataSync, consulte [AWS DataSync](#).

Requisitos previos para transferir archivos a Amazon EFS mediante AWS DataSync

Antes de transferir archivos al sistema de archivos EFS, asegúrese de tener lo siguiente:

- Un sistema de archivos NFS de origen desde el que puede transferir archivos. Este sistema de origen debe ser accesible mediante NFS versión 3, 4 o 4.1. Entre los ejemplos de sistemas de archivos se incluyen los que se encuentran en el centro de datos en las instalaciones, los sistemas de archivos en la nube administrados automáticamente y los sistemas de archivos de Amazon EFS.
- Está preparado para usar DataSync. Para obtener más información, consulte [Configuración con AWS DataSync](#) en la Guía del AWS DataSync usuario.

Para transferir archivos al sistema de archivos EFS mediante AWS DataSync

Para obtener instrucciones sobre cómo transferir archivos a un sistema de archivos EFS, consulte [Transferir los datos con AWS DataSync](#) en la Guía del AWS DataSync usuario. DataSync

Los siguientes son los pasos que realizará al transferir archivos al sistema de archivos EFS mediante DataSync.

1. Conéctese a la instancia de Amazon EC2.
2. Descargue, implemente y active un agente en su entorno.
3. Cree y configure una ubicación de origen y destino.
4. Cree y configure una tarea.

5. Ejecute la tarea para transferir archivos desde el origen al destino.

Limpie los recursos y proteja su AWS cuenta

Esta guía incluye tutoriales que puede usar para explorar Amazon EFS en mayor profundidad. Antes de realizar este paso de limpieza, puedes usar los recursos que has creado y a los que te has conectado en este ejercicio de introducción en esos tutoriales. Para obtener más información, consulte [Explicaciones](#). Después de terminar los tutoriales o si no desea explorarlos, realice los pasos siguientes para limpiar los recursos y proteger su Cuenta de AWS.

Para limpiar los recursos y proteger su cuenta

1. Conéctese a la instancia de Amazon EC2.
2. Desmonte el sistema de archivos de EFS; con el siguiente comando.

```
$ sudo umount efs
```

3. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
4. Elimine el sistema de archivos EFS que creó en el primer paso del ejercicio de introducción.
 - a. Elija el sistema de archivos de EFS; que desea eliminar de la lista de sistemas de archivos.
 - b. En Acciones, seleccione Eliminar sistema de archivos.
 - c. En el cuadro de diálogo Eliminar sistema de archivos permanentemente, escriba el ID del sistema de archivos de EFS; que quiera eliminar y luego seleccione Eliminar sistema de archivos.
5. Finalice la instancia de Amazon EC2 que lanzó para este ejercicio de introducción. Para obtener instrucciones, consulte [Finalizar instancias de Amazon EC2](#) en la Guía del AWS IAM Identity Center usuario.
6. Elimine el grupo de seguridad que creó para este ejercicio de introducción. Para obtener instrucciones, consulte [Eliminar un grupo de seguridad](#) en la Guía del AWS IAM Identity Center usuario.

Warning

No elimine el grupo de seguridad predeterminado para la VPC.

Descripción de los tipos de sistemas de archivos y clases de almacenamiento de Amazon EFS

En esta sección se describen los tipos de sistemas de archivos y las opciones de clases de almacenamiento para los sistemas de archivos de Amazon Elastic File System (Amazon EFS).

Tipos de sistemas de archivos EFS

Amazon EFS ofrece tipos de sistemas de archivos regionales y One Zone.

- **Regionales:** los sistemas de archivos regionales (recomendados) almacenan datos de forma redundante en varias zonas de disponibilidad separadas geográficamente dentro de una misma zona. Región de AWS El almacenamiento de datos en varias zonas de disponibilidad proporciona una disponibilidad continua de los datos, incluso cuando una o más zonas de disponibilidad de una zona Región de AWS no están disponibles.
- **Una zona:** los sistemas de archivos de una zona almacenan los datos dentro de una única zona de disponibilidad. El almacenamiento de datos en una única zona de disponibilidad proporciona una disponibilidad continua de los datos. Sin embargo, en el improbable caso de pérdida o daño de la totalidad o parte de la zona de disponibilidad, es posible que se pierdan los datos almacenados en estos tipos de sistemas de archivos.

En el improbable caso de pérdida o daño de la totalidad o parte de una zona de AWS disponibilidad, es posible que se pierdan los datos de una clase de almacenamiento de una sola zona. Por ejemplo, daños provocados por incendios o agua podrían provocar la pérdida de datos. Además de este tipo de eventos, nuestras clases de almacenamiento One Zone utilizan diseños de ingeniería similares a los de nuestras clases de almacenamiento regional para proteger los objetos de fallos independientes a nivel de disco, host y rack, y cada una de ellas está diseñada para ofrecer una durabilidad de los datos del 99,999999999 %.

Para una mayor protección de los datos, Amazon EFS realiza automáticamente copias de seguridad de los sistemas de archivos One Zone con AWS Backup. Puede restaurar las copias de seguridad del sistema de archivos en cualquier zona de disponibilidad operativa dentro de una Región de AWS, o puede restaurarlas en una diferente Región de AWS. Las copias de seguridad del sistema de archivos EFS que se crean y AWS Backup administran mediante ellas se replican en tres zonas de disponibilidad y están diseñadas para ofrecer durabilidad. Para obtener más información, consulte [Resiliencia en AWS Backup](#).

Note

Los sistemas de archivos de One Zone solo están disponibles para determinadas zonas de disponibilidad. Para ver una tabla en la que se enumeran las zonas de disponibilidad en las que puede utilizar los sistemas de archivos de One Zone, consulte [Zonas de disponibilidad compatibles para los sistemas de archivos One Zone](#).

En la siguiente tabla se comparan los tipos de sistemas de archivos, incluidas su disponibilidad, durabilidad y otras cuestiones.

Tipo de sistema de archivos	Diseñada para	Durabilidad (según diseño)	Disponibilidad	Zonas de disponibilidad	Otras consideraciones
Regional	Datos que requieren la máxima durabilidad y disponibilidad.	99,999999 999 % (11 9s)	99,99%	>=3	Ninguna
One Zone	Datos que no requieren la máxima durabilidad y disponibilidad.	99,999999 999 % (11 9s)	99,99%	1	No resiste la pérdida de la zona de disponibilidad

Zonas de disponibilidad compatibles para los sistemas de archivos One Zone

Los sistemas de archivos de One Zone solo están disponibles para determinadas zonas de disponibilidad. En la siguiente tabla se enumeran los ID de zona de disponibilidad Región de AWS y los ID de zona de disponibilidad en los que puede utilizar los sistemas de archivos de One Zone. Para ver la asignación de los ID de zona de disponibilidad a las zonas de disponibilidad de su cuenta, consulte [los ID de zonas de disponibilidad de sus AWS recursos](#) en la Guía del usuario de AWS Resource Access Manager.

Zonas de disponibilidad compatibles con los sistemas de archivos de One Zone

Región de AWS Nombre	Región de AWS Código	ID AZ compatibles
Este de EE. UU. (Ohio)	us-east-2	use2-az1, use2-az2, use2-az3
Este de EE. UU. (Norte de Virginia)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
Oeste de EE. UU. (Norte de California)	us-west-1	usw1-az1, usw1-az3
Oeste de EE. UU. (Oregón)	us-west-2	usw2-az1, usw2-az2, usw2-az3, usw2-az4
África (Ciudad del Cabo)	af-south-1	afs1-az1, afs1-az2, afs1-az3
Asia-Pacífico (Hong Kong)	ap-east-1	ape1-az1, ape1-az2, ape1-az3
Asia Pacífico (Mumbai)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
Asia Pacífico (Osaka)	ap-northeast-3	apne3-az1, apne3-az2, apne3-az3
Asia Pacífico (Seúl)	ap-northeast-2	apne2-az1, apne2-az2, apne2-az3
Asia Pacífico (Singapur)	ap-southeast-1	apse1-az1, apse1-az2
Asia Pacífico (Sídney)	ap-southeast-2	apse2-az1, apse2-az2, apse2-az3
Asia Pacífico (Tokio)	ap-northeast-1	apne1-az1, apne1-az4
Canadá (Central)	ca-central-1	cac1-az1, cac1-az2
China (Pekín)	cn-north-1	cnn1-az1, cnn1-az2
China (Ningxia)	cn-northwest-1	cnnw1-az1, cnnw1-az2, cnnw1-az3

Región de AWS Nombre	Región de AWS Código	ID AZ compatibles
Europa (Frankfurt)	eu-central-1	euc1-az1, euc1-az2, euc1-az3
Europa (Irlanda)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europa (Londres)	eu-west-2	euw2-az1, euw2-az2
Europa (Milán)	eu-south-1	eus1-az1, eus1-az2, eus1-az3
Europa (París)	eu-west-3	euw3-az1, euw3-az3
Europa (Estocolmo)	eu-north-1	eun1-az1, eun1-az2, eun1-az3
Medio Oriente (Baréin)	me-south-1	mes1-az1, mes1-az2, mes1-az3
América del Sur (São Paulo)	sa-east-1	sae1-az1, sae1-az2, sae1-az3
AWS GovCloud (EEUU-Este)	us-gov-east-1	usge1-az1, usge1-az2, usge1-az3
AWS GovCloud (US-Oeste)	us-gov-west-1	usgw1-az1, usgw1-az2, usgw1-az3

Clases de almacenamiento de EFS

Amazon EFS ofrece distintas clases de almacenamiento diseñadas para ofrecer el almacenamiento más eficaz en función de los casos de uso.

- **EFS Estándar:** la clase de almacenamiento EFS Estándar utiliza almacenamiento en unidades de estado sólido (SSD) para ofrecer los niveles más bajos de latencia para archivos a los que se accede con frecuencia. Los nuevos datos del sistema de archivos se escriben primero en la clase de almacenamiento EFS Standard y, después, se pueden agrupar en niveles en las clases de almacenamiento EFS Infrequent Access y EFS Archive mediante la administración del ciclo de vida.
- **Acceso poco frecuente (IA) de EFS:** una clase de almacenamiento con coste optimizado para datos a los que se accede solo unas pocas veces cada trimestre.

- Archivado de EFS: una clase de almacenamiento con coste optimizado para datos a los que se accede varias veces al año o menos.

La clase de almacenamiento EFS Archive es compatible con los sistemas de archivos EFS con rendimiento elástico. No puede actualizar el rendimiento del sistema de archivos a Por ráfagas o Aprovisionado una vez que el sistema de archivos tenga datos de la clase de almacenamiento Archivado.

Optimización de costos de almacenamiento

Las clases de almacenamiento IA y Archivado tienen un coste optimizado para los archivos que no requieren el rendimiento de latencia del almacenamiento estándar. La latencia del primer byte al leer desde cualquiera de las clases de almacenamiento de acceso infrecuente es mayor que en la clase de almacenamiento Estándar.


Con la administración del ciclo de vida, puede optimizar los costos de almacenamiento al organizar automáticamente los datos en niveles entre las clases de almacenamiento en función de los patrones de acceso de su carga de trabajo. Puede mover archivos de las clases de almacenamiento IA o Archivado a la clase de almacenamiento Estándar si establece la política de Transición al ciclo de vida Estándar en su sistema de archivos. Esta configuración hace que los archivos de IA o Archivado vuelvan a ser Estándar al acceder a ellos. Si desea que sus archivos permanezcan en la clase de almacenamiento estándar, a la que se accede con más frecuencia, desactive la administración del ciclo de vida en el sistema de archivos. Para obtener más información, consulte [Administrar el almacenamiento del sistema de archivos](#).

Comparación de clases de almacenamiento

En la tabla siguiente se comparan las clases de almacenamiento. Para obtener más información sobre el rendimiento de cada clase de almacenamiento, consulte [Rendimiento de Amazon EFS](#).

Clase de almacenamiento	Diseñada para	Latencia de lectura del primer byte	Durabilidad (diseñada para) ¹	SLA de disponibilidad	Zonas de disponibilidad	Cargo de facturación mínimo por archivo ²	Duración mínima del almacenamiento
EFS Standard	Datos activos que requieren	Inferior a un	99,999999 999%	99,99 % (Regional)	=>3 (Regional)	No aplicable	No aplica

Clase de almacenamiento	Diseñada para	Latencia de lectura del primer byte	Durabilidad (diseñada para) ¹	SLA de disponibilidad	Zonas de disponibilidad	Cargo de facturación mínimo por archivo ²	Duración mínima del almacenamiento
	un rendimiento rápido de latencia inferior a un milisegundo	milisegundo		99,9 % (One Zone)			
Acceso poco frecuente de EFS	Datos inactivos a los que se accede solo unas cuantas veces cada trimestre.	Decenas de milisegundos	(11 9's)		1 (One Zone)	128 KiB	No aplica
Archivado de EFS	Datos inactivos a los que se accede solo unas cuantas veces cada año o menos	Decenas de milisegundos		99,9 % (Regional)	=>3 (Regional)	128 KiB	90 días

 Note

¹ Como los sistemas de archivos de una zona almacenan los datos en una única zona de AWS disponibilidad, los datos que se almacenan en estos tipos de sistemas de archivos pueden perderse en caso de un desastre u otro error que afecte a todas las copias de los datos de la zona de disponibilidad, o en caso de que se destruya la zona de disponibilidad.

² Las políticas de ciclo de vida actualizadas a las 12 (PT) del 26 de noviembre de 2023 o después de esa fecha clasificarán los archivos de menos de 128 KiB en la clase IA. Para obtener más información sobre cómo Amazon EFS mide y factura los archivos y metadatos individuales, consulte [Medición: cómo Amazon EFS registra el tamaño del sistema de archivos y el tamaño de los objetos](#).

Precios de clases de almacenamiento

Se le facturará por la cantidad de datos en cada clase de almacenamiento. También se le facturan cargos por el acceso a los datos cuando se leen los archivos de IA o Archive Storage, o por los datos que se transfieren de una clase de almacenamiento a otra mediante la administración del ciclo de vida. La factura de AWS muestra la capacidad de cada clase de almacenamiento y el acceso medido con respecto a la clase de almacenamiento del sistema de archivos. Para obtener más información, consulte [Precios de Amazon EFS](#).

Además, las clases de almacenamiento de Acceso poco frecuente (IA) y Archivado tienen un cargo mínimo de facturación por archivo de 128 KiB. La compatibilidad con archivos de menos de 128 KiB solo está disponible para las políticas de ciclo de vida actualizadas a partir de las 12:00 (PT) del 26 de noviembre de 2023. Para obtener más información sobre cómo Amazon EFS mide y factura los archivos y metadatos individuales, consulte [Medición: cómo Amazon EFS registra el tamaño del sistema de archivos y el tamaño de los objetos](#).

Se aplican precios adicionales a los sistemas de archivos que utilizan un rendimiento aprovisionado o en ráfaga.

- Para los sistemas de archivos con el modo de rendimiento aprovisionado, se le cobrará por el rendimiento aprovisionado por encima del proporcionado en función de la cantidad de datos en la clase de almacenamiento Estándar de EFS.
- Para los sistemas de archivos con rendimiento por ráfagas, la velocidad permitida se determina en función de la cantidad de datos almacenados únicamente en la clase de almacenamiento Estándar de EFS.

Para obtener más información sobre los modos de rendimiento de EFS, consulte [Modos de rendimiento](#).

Note

No incurre en cargos de acceso a los datos cuando los utiliza AWS Backup para hacer copias de seguridad de los sistemas de archivos EFS habilitados para la administración del ciclo de vida. Para obtener más información sobre la administración del ciclo de vida AWS Backup, consulte [Clases de almacenamiento de EFS](#).

Visualización del tamaño de clases de almacenamiento

Puede ver la cantidad de datos almacenados en cada clase de almacenamiento de su sistema de archivos mediante la consola Amazon EFS AWS CLI, o la API de EFS.

Visualización del tamaño de datos de almacenamiento en la consola de Amazon EFS

La pestaña Tamaño medido de la página Detalles del sistema de archivos muestra el tamaño medido actual del sistema de archivos en múltiplos binarios de bytes (kibibytes, mebibytes, gibibytes y tebibytes). La métrica se emite cada 15 minutos y le permite ver el tamaño medido del sistema de archivos a lo largo del tiempo. El tamaño medido muestra la siguiente información sobre el tamaño de almacenamiento del sistema de archivos:

- El tamaño total es el tamaño (en bytes binarios) de los datos almacenados en el sistema de archivos, incluidas todas las clases de almacenamiento.
- El tamaño en Estándar es el tamaño (en bytes binarios) de los datos almacenados en la clase de almacenamiento Estándar de EFS o One Zone de EFS.
- El tamaño en IA es el tamaño (en bytes binarios) de los datos almacenados en la clase de almacenamiento de Acceso poco frecuente de EFS. Los archivos de menos de 128 KB se redondean al alza a 128 KB.
- El tamaño en Archivado es el tamaño (en bytes binarios) de los datos almacenados en la clase de almacenamiento Archivado de EFS. Los archivos de menos de 128 KB se redondean al alza a 128 KB.

También puede ver la métrica `Storage bytes` en la pestaña Monitorización de la página Detalles del sistema de archivos de la consola de Amazon EFS. Para obtener más información, consulte [Acceder a CloudWatch las métricas](#).

Visualización del tamaño de los datos de almacenamiento mediante AWS CLI

Puede ver la cantidad de datos almacenados en cada clase de almacenamiento de su sistema de archivos mediante la API AWS CLI o EFS. Vea los detalles del almacenamiento de datos llamando al comando `describe-file-systems` de la CLI (la operación de API correspondiente es [DescribeFileSystems](#)).

```
$ aws efs describe-file-systems \  
--region us-west-2 \  
--profile adminuser
```


En la respuesta, `ValueInIA` muestra el último tamaño medido en bytes de la clase de almacenamiento de Acceso poco frecuente del sistema de archivos. `ValueInStandard` muestra el último tamaño medido en bytes de la clase de almacenamiento Estándar. `ValueInArchive` muestra el último tamaño medido en bytes de la clase de almacenamiento Archivado. La suma de los tres valores equivale al tamaño de todo el sistema de archivos, que se muestra en `Value`.

```
{
  "FileSystems":[
    {
      "OwnerId":"251839141158",
      "CreationToken":"MyFileSystem1",
      "FileSystemId":"fs-47a2c22e",
      "PerformanceMode" : "generalPurpose",
      "CreationTime": 1403301078,
      "LifecycleState":"created",
      "NumberOfMountTargets":1,
      "SizeInBytes":{
        "Value": 29313746702,
        "ValueInIA": 675432,
        "ValueInStandard": 29312741784,
        "ValueInArchive":329486
      },
      "ThroughputMode": "elastic"
    }
  ]
}
```

Para conocer otras formas de ver y medir el uso de los discos, consulte [Medición de objetos del sistema de archivos de Amazon EFS](#).

Uso de recursos de Amazon EFS

Amazon EFS ofrece almacenamiento de archivos compartido elástico que es compatible con POSIX. El sistema de archivos que cree admite el acceso simultáneo de lectura y escritura desde varias instancias de Amazon EC2. También se puede acceder al sistema de archivos desde todas las zonas de disponibilidad en las Región de AWS que se creó.

Puede montar un sistema de archivos de Amazon EFS en instancias EC2 en su nube privada virtual (VPC) basada en Amazon VPC mediante el protocolo Network File System versiones 4.0 y 4.1 (NFSv4). Para obtener más información, consulte [Cómo funciona Amazon EFS](#).

Por ejemplo, suponga que tiene una o varias instancias EC2 lanzadas en su VPC. Ahora desea crear y utilizar un sistema de archivos en estas instancias. A continuación, se indican los pasos típicos que necesita realizar para utilizar los sistemas de archivos de EFS en la VPC:

- Cree un sistema de archivos Amazon EFS: al crear un sistema de archivos, le recomendamos que utilice la etiqueta Nombre. El valor de la etiqueta de Nombre aparece en la consola y facilita la identificación del sistema de archivos. También puede añadir otras etiquetas opcionales al sistema de archivos.
- Cree destinos de montaje para el sistema de archivos: para obtener accesos al sistema de archivos en la VPC y montar el sistema de archivos en la instancia de Amazon EC2, debe crear destinos de montaje en las subredes de la VPC.
- Cree grupos de seguridad: es necesario que tanto una instancia de Amazon EC2 como un destino de montaje dispongan de grupos de seguridad asociados. Estos grupos de seguridad actúan como un firewall virtual que controla el tráfico entre ellos. Puede usar el grupo de seguridad que asoció al destino de montaje para controlar el tráfico entrante a su sistema de archivos. Para ello, añada una regla de entrada al grupo de seguridad de destino de montaje que permita el acceso desde una instancia de EC2 específica. A continuación, puede montar el sistema de archivos únicamente en esa instancia EC2.

Temas

- [ID de recursos](#)
- [Idempotencia y token de creación](#)
- [Creación de sistemas de archivos de Amazon EFS](#)
- [Eliminar los sistemas de archivos Amazon EFS](#)

- [Administrar destinos de montaje](#)
- [Creación de grupos de seguridad](#)
- [Creación de políticas de sistema de archivos](#)
- [Crear puntos de acceso](#)
- [Eliminar puntos de acceso](#)
- [Etiquetado de los recursos de Amazon EFS](#)

ID de recursos

Amazon EFS asigna identificadores de recursos (ID) únicos a todos los recursos de EFS cuando se crean. Todos los ID de recursos de EFS constan de un identificador de recurso y una combinación de dígitos del 0 al 9 y letras minúsculas de la a a la f.

Antes de octubre de 2021, los identificadores que se asignaban cuando se creaban los recursos de destino nuevos tenían 8 caracteres después del guion (por ejemplo, fs-12345678). Entre mayo y octubre de 2021, cambiamos los identificadores de estos tipos de recursos para que utilizaran 17 caracteres después del guion (por ejemplo, fs-1234567890abcdef0). En función del momento en que se creó su cuenta, es posible que tenga recursos de sistema de archivo y destino de montaje con identificadores cortos, aunque cualquier recurso nuevo de estos tipos recibe identificadores más largos. El ID del recurso nunca cambia.

Idempotencia y token de creación

La idempotencia garantiza que una solicitud de API se complete solo una vez. Con solicitudes idempotentes, si la solicitud original se completa correctamente, las solicitudes posteriores no tienen ningún efecto adicional. Esto resulta útil para evitar que se creen trabajos duplicados al interactuar con la API de Amazon EFS.

La API de Amazon EFS admite la idempotencia con los tokens de solicitud de los clientes. Un token de solicitud de cliente es una cadena única que se especifica cuando se realiza una solicitud de trabajo.

Un token de solicitud de cliente puede ser cualquier cadena que incluya hasta 64 caracteres ASCII. Si reutiliza el token de solicitud de un cliente en un plazo de un minuto desde que la solicitud se realizara correctamente, la API devolverá los detalles del trabajo de la solicitud original.

Si utiliza la consola, genera el token por usted. Si utiliza el flujo de Creación personalizada en la consola, el token de creación que se genera automáticamente tiene el siguiente formato:

```
"CreationToken": "console-d215fa78-1f83-4651-b026-facafd8a7da7"
```

Si usa Quick Create para crear un sistema de archivos con la configuración recomendada por el servicio, el token de creación tiene el siguiente formato:

```
"CreationToken": "quickCreated-d7f56c5f-e433-41ca-8307-9d9c0f8a77a2"
```

Creación de sistemas de archivos de Amazon EFS

A continuación, puede aprender a crear un sistema de archivos Amazon EFS mediante el AWS Management Console y el AWS CLI.

Temas

- [Permisos necesarios para crear sistemas de archivos](#)
- [Opciones de configuración para los sistemas de archivos](#)

Permisos necesarios para crear sistemas de archivos

Para crear recursos de EFS, como un sistema de archivos y puntos de acceso, debe tener permisos AWS Identity and Access Management (IAM) para la operación y el recurso de API correspondientes.

Cree usuarios de IAM y concédales permisos para las acciones de Amazon EFS con políticas de usuario. También puede utilizar roles para conceder permisos entre cuentas. Amazon Elastic File System también utiliza una función vinculada al servicio de IAM que incluye los permisos necesarios para llamar a otras personas Servicios de AWS en su nombre. Para obtener más información sobre la administración de permisos para operaciones de API, consulte [Administración de identidades y acceso Amazon Elastic File System](#).

Opciones de configuración para los sistemas de archivos

Puede crear un sistema de archivos mediante la consola de Amazon EFS o utilizando AWS Command Line Interface (AWS CLI). También puede crear sistemas de archivos mediante programación mediante AWS SDK o directamente con la API de Amazon EFS. Si utiliza la API de Amazon EFS o un AWS SDK, puede utilizar la acción de la API de `CreateFileSystem` EFS para crear políticas del sistema de archivos.

Al crear un sistema de archivos Amazon EFS mediante el flujo de creación personalizado de la consola o AWS CLI, puede elegir los ajustes para las siguientes opciones de configuración y funciones del sistema.

Tipo de sistema de archivos

El tipo de sistema de archivos determina la disponibilidad y durabilidad con las que un sistema de archivos Amazon EFS almacena los datos dentro de una Región de AWS. Para el tipo de sistema de archivos, tiene las siguientes opciones:

- Elija **Regional** para crear un sistema de archivos que almacene datos y metadatos de forma redundante en todas las zonas de disponibilidad de una Región de AWS. También puede crear destinos de montaje en cada zona de disponibilidad de Región de AWS. **Regional** ofrece los niveles más altos de disponibilidad y durabilidad.
- Elija **One Zone** para crear un sistema de archivos que almacene datos y metadatos de forma redundante en una única zona de disponibilidad. Los sistemas de archivos que utilizan clases de almacenamiento solo pueden tener un único destino de montaje. Este destino de montaje debe estar ubicado en la zona de disponibilidad en la que se creó el sistema de archivos.

Copias de seguridad automáticas

Las copias de seguridad automáticas siempre están habilitadas de forma predeterminada cuando crea un sistema de archivos mediante la consola. Cuando utiliza la CLI o la API para crear un sistema de archivos, las copias de seguridad automáticas se habilitan de forma predeterminada solo cuando crea sistemas de archivos que utilizan sistemas **One Zone**. Para obtener más información, consulte [Copias de seguridad automáticas](#).

Política del ciclo de vida

La administración del ciclo de vida utiliza políticas de ciclo de vida para mover automáticamente los archivos dentro y fuera de la clase de almacenamiento de acceso infrecuente (IA), de menor costo, en función de los patrones de acceso. Al crear un sistema de archivos mediante la AWS Management Console, la política de ciclo de vida del sistema de archivos se configura con los siguientes ajustes predeterminados:

- Transición hacia IA se establece en 30 días desde el último acceso.
- `TransitionToArchivo` establecido en 90 días desde el último acceso.
- Transición a Estándar se establece en Ninguna.

Cuando crea un sistema de archivos mediante la AWS CLI API de Amazon EFS o AWS los SDK, no puede establecer una política de ciclo de vida al mismo tiempo. Debe esperar a que se cree el sistema de archivos y, a continuación, utilizar la operación de la API de [PutLifecycleConfiguration](#) para actualizar la política del ciclo de vida. Para obtener más información, consulte [Administrar el almacenamiento del sistema de archivos](#).

Cifrado

Puede habilitar el cifrado en reposo a la hora de crear un sistema de archivos. Si habilita el cifrado en reposo en su sistema de archivos, se cifrarán todos los datos y metadatos almacenados en él. Puede habilitar el cifrado en tránsito más adelante, cuando monte el sistema de archivos. Para obtener más información sobre el cifrado de Amazon EFS, consulte [Cifrado de datos en Amazon EFS](#).

Para crear los destinos de montaje del sistema de archivos en su VPC, debe especificar subredes de VPC. La consola rellena previamente la lista de los VPC de su cuenta que están en la Región de AWS seleccionada. En primer lugar, seleccione la VPC y, a continuación, la consola muestra las zonas de disponibilidad de la VPC. Para cada zona de disponibilidad, puede seleccionar una subred de la lista o utilizar la subred predeterminada si existe. Después de seleccionar una subred, puede especificar una dirección IP disponible en la subred o dejar que Amazon EFS seleccione una dirección automáticamente.

Modos de rendimiento

Hay tres modos de rendimiento entre los que elegir:


- **Elástico (recomendado):** proporciona un rendimiento que se escala y reduce verticalmente de forma automática en tiempo real, para satisfacer las necesidades de rendimiento de la carga de trabajo.

Note

El rendimiento elástico solo está disponible para los sistemas de archivos que tienen el modo de rendimiento de uso general.

- **Aprovisionado:** proporciona el nivel de rendimiento que se especifique, independientemente del tamaño del sistema de archivos.
- **Transmisión por ráfagas:** proporciona un rendimiento que se escala con la cantidad de datos del almacenamiento estándar.

Para obtener más información, consulte [Modos de rendimiento](#).


 Note

Existen cargos adicionales asociados al uso del rendimiento elástico y aprovisionado. Para obtener más información, consulte [precios de Amazon EFS](#).

Modos de rendimiento

Al crear un sistema de archivos, también elige un modo de desempeño. Puede elegir entre dos modos: uso general y E/S máx.

- El modo de uso general tiene la latencia por operación más baja y se recomienda para todos los sistemas de archivos.
- El E/S máx. es un tipo de rendimiento de generación anterior que está diseñado para cargas de trabajo altamente paralelizadas que pueden tolerar latencias más altas que el modo de uso general. El modo de E/S máx. no es compatible con los sistemas de archivos One Zone ni con los sistemas de archivos que utilizan rendimiento elástico.

 Important

Debido a las latencias por operación más altas con una E/S máx., recomendamos utilizar el modo de rendimiento de uso general para todos los sistemas de archivos.

Para obtener más información, consulte [Modos de rendimiento](#).

Cree rápidamente un sistema de archivos con la configuración recomendada (consola)

En este paso, utilice la consola Amazon EFS para crear un sistema de archivos Amazon EFS con la configuración recomendada. Si desea crear un sistema de archivos con una configuración personalizada, consulte [Cree un sistema de archivos con ajustes personalizados \(consola\)](#).

Para crear rápidamente un sistema de archivos Amazon EFS con la configuración recomendada

1. Inicie sesión en la consola de Amazon EFS AWS Management Console y ábrala en <https://console.aws.amazon.com/efs/>.
2. Seleccione Crear sistema de archivos para abrir el cuadro de diálogo Crear sistema de archivos.

3. De forma opcional, puede ingresar un nombre para el sistema de archivos.
4. Para nube privada virtual (VPC), seleccione su VPC o mantenga la opción configurada como la VPC predeterminada.
5. Seleccione Crear para crear un sistema de archivos que utilice las siguientes configuraciones recomendadas para el servicio:
 - Copias de seguridad automáticas habilitadas. Para obtener más información, consulte [Copia de seguridad de los sistemas de archivos de Amazon EFS](#).
 - Monte los destinos configurados con los siguientes ajustes:
 - Se crea en cada zona de disponibilidad Región de AWS en la que se crea el sistema de archivos.
 - Ubicada en las subredes predeterminadas de la VPC que ha seleccionado.
 - Uso del grupo de seguridad predeterminado de la VPC: puede administrar los grupos de seguridad una vez creado el sistema de archivos.

Para obtener más información, consulte [Gestión de la accesibilidad de red del sistema de archivos](#).

- Tipo de sistema de archivos regionales: para obtener más información, consulte [Tipos de sistemas de archivos EFS](#).
- Rendimiento de uso general: para obtener más información, consulte [Modos de rendimiento](#).
- Rendimiento elástico: para obtener más información, consulte [Modos de rendimiento](#).
- Cifrado de datos en reposo habilitado con la clave predeterminada para Amazon EFS (aws/elasticfilesystem) – Para obtener más información, consulte [Cifrado de datos en reposo](#).
- administración del ciclo de vida: Amazon EFS crea el sistema de archivos con las siguientes políticas del ciclo de vida:
 - Transición hacia IA se establece en 30 días desde el último acceso.
 - TransitionToArchivo establecido en 90 días desde el último acceso.
 - Transición a Estándar se establece en Ninguna.

Para obtener más información, consulte [Administrar el almacenamiento del sistema de archivos](#).

Después de crear el sistema de archivos, puede personalizar la configuración del sistema de archivos con la excepción de la disponibilidad y durabilidad, el cifrado y el modo de rendimiento.

La página Sistemas de archivos aparece con un encabezado en la parte superior que muestra el estado del sistema de archivos que ha creado. Cuando el sistema de archivos esté disponible, aparecerá un enlace para acceder a la página de detalles del nuevo sistema de archivos en el encabezado.

Para obtener más información acerca del estado del sistema de archivos, consulte [Estado del sistema de archivos](#).

Cree un sistema de archivos con ajustes personalizados (consola)

En esta sección se describe el proceso de uso de la consola de Amazon EFS para crear un sistema de archivos EFS con una configuración personalizada en lugar de utilizar la configuración recomendada por el servicio. Para obtener más información acerca de cómo crear un sistema de archivos mediante la configuración recomendada por el servicio, consulte [Cree rápidamente un sistema de archivos con la configuración recomendada \(consola\)](#).

La creación de un sistema de archivos de Amazon EFS con ajustes personalizados mediante la consola es un proceso de cuatro pasos:

- Paso 1: Configurar los ajustes generales del sistema de archivos, incluida la clase de almacenamiento y el modo de rendimiento.
- Paso 2: Configurar los ajustes de red del sistema de archivos, incluida la nube privada virtual (VPC) y los destinos de montaje. Para cada destino de montaje, establezca la zona de disponibilidad, la subred, la dirección IP y los grupos de seguridad.
- Paso 3: (opcional) Crear una política de sistema de archivos para controlar el acceso de los clientes de NFS al sistema de archivos.
- Paso 4: Revisar la configuración del sistema de archivos, realizar los cambios necesarios y, a continuación, crear el sistema de archivos.

Paso 1: Configurar los ajustes del sistema de archivos

1. Inicie sesión en la consola de Amazon EFS AWS Management Console y ábrala en <https://console.aws.amazon.com/efs/>.
2. Seleccione Crear sistema de archivos para abrir el cuadro de diálogo Crear sistema de archivos.

3. Seleccione Personalizar para crear un sistema de archivos personalizado en lugar de crear un sistema de archivos con la configuración recomendada por el servicio. Se abre la página de Ajustes del sistema de archivos.
4. En los ajustes Generales, haga lo siguiente.
 - a. (Opcional) Escriba un Nombre para el sistema de archivos.
 - b. En el Tipo de sistema de archivos, elige una opción de disponibilidad:
 - Elija Regional para crear un sistema de archivos que almacene datos y metadatos de forma redundante en todas las zonas de disponibilidad de una Región de AWS. Regional ofrece los niveles más altos de disponibilidad y durabilidad.
 - Elija One Zone para crear un sistema de archivos que almacene datos y metadatos de forma redundante en una única zona de disponibilidad. Si elige One Zone, seleccione la Zona de disponibilidad en la que desee crear el sistema de archivos o mantenga el valor predeterminado. Para obtener más información, consulte [Clases de almacenamiento de EFS](#).
 - c. Las Copias de seguridad automáticas no están activadas de forma predeterminada. Puede desactivar las copias de seguridad automáticas si desactiva la casilla de verificación. Para obtener más información, consulte [Copia de seguridad de los sistemas de archivos de Amazon EFS](#).
 - d. Para la Administración del ciclo de vida, cambie las políticas del ciclo de vida, si es necesario.
 - Transición a IA: seleccione cuándo realizar la transición de los archivos a la clase de almacenamiento de acceso poco frecuente (IA), en función del tiempo transcurrido desde la última vez que se accedió a ellos en el almacenamiento estándar.
 - Transición a Archivado: seleccione cuándo realizar la transición de los archivos a la clase de almacenamiento Archivado, en función del tiempo transcurrido desde la última vez que se accedió a ellos en el almacenamiento estándar.
 - Transición a Estándar: seleccione si desea realizar la transición del sistema de archivos a la clase de almacenamiento.

Para obtener más información acerca de políticas de ciclo de vida, consulte [Administrar el almacenamiento del sistema de archivos](#).
 - e. En el caso del Cifrado, el cifrado de los datos en reposo está activado de forma predeterminada. Amazon EFS utiliza su AWS Key Management Service clave de servicio

EFS (`aws/elasticfilesystem`) () de forma predeterminada. AWS KMS Para elegir una clave de KMS diferente para usarla en el cifrado, expanda Personalizar la configuración de cifrado y elija una clave de la lista. También puede introducir una ID de clave de KMS o un nombre de recurso de Amazon (ARN) para la clave de KMS que quiera utilizar.

Si necesita crear una clave nueva, elija Crear una AWS KMS key para iniciar la AWS KMS consola y crear una clave nueva.

Puede desactivar el cifrado de datos en reposo si desactiva la casilla de verificación.

5. En la configuración de Rendimiento, haga lo siguiente:

- a. En el Modo de rendimiento, el modo Elástico está seleccionado de forma predeterminada.
 - Para usar el rendimiento aprovisionado, elija Aprovisionado y, en Rendimiento aprovisionado (MIB/s), introduzca la cantidad de rendimiento que se va a aprovisionar para las solicitudes del sistema de archivos. La cantidad de Rendimiento máximo de lectura se muestra tres veces mayor que la cantidad de rendimiento que introduzca.
 - Para utilizar el rendimiento por ráfagas, seleccione Transmisión por ráfagas.

Los sistemas de archivos Amazon EFS miden las solicitudes de lectura a un tercio de la velocidad de otras solicitudes. Tras entrar en el modo de rendimiento, se muestra una estimación del coste mensual del sistema de archivos. Puede cambiar el modo de rendimiento una vez que el sistema de archivos esté disponible.

Para obtener más información sobre cómo elegir el modo de rendimiento correcto para sus necesidades de rendimiento, consulte [Modos de rendimiento](#).

- b. En Modo de rendimiento, mantenga la opción predeterminada de Uso general. Para cambiar el modo de rendimiento, expanda Configuración adicional y, a continuación, seleccione E/S máx.

No se puede cambiar el modo de rendimiento una vez que el sistema de archivos esté disponible. Para obtener más información, consulte [Modos de rendimiento](#).

 Important

Debido a las latencias por operación más altas con una E/S máx., recomendamos utilizar el modo de rendimiento de uso general para todos los sistemas de archivos.

6. (Opcional) Agregue pares clave-valor de etiquetas al sistema de archivos.
7. Elija Siguiente para configurar el acceso a la red para el sistema de archivos.

Paso 2: Configurar un acceso a la red

En el paso 2, se configuran los ajustes de red del sistema de archivos, incluidos la VPC y los destinos de montaje.

1. Seleccione la Nube Privada Virtual (VPC) en la que desea que las instancias de EC2 se conecten a su sistema de archivos. Para obtener más información, consulte [Gestión de la accesibilidad de red del sistema de archivos](#).
2. Para Destinos de montaje, debe crear uno o más destinos para el sistema de archivos. Para cada destino de montaje, establezca las siguientes propiedades:
 - Zona de disponibilidad: de forma predeterminada, se configura un destino de montaje en cada zona de disponibilidad de una Región de AWS. Si no desea un destino de montaje en una zona de disponibilidad concreta, seleccione Eliminar para eliminar el destino de montaje de esa zona. Cree un destino de montaje en cada zona de disponibilidad desde la que tenga previsto acceder al sistema de archivos; esta acción no tiene ningún coste.
 - ID de subred: elija entre las subredes disponibles en una zona de disponibilidad. La subred predeterminada está preseleccionada.
 - Dirección IP: de forma predeterminada, Amazon EFS elige automáticamente la dirección IP entre las direcciones disponibles en la subred. O bien puede introducir una dirección IP específica que esté en la subred. Si bien los destinos de montaje tienen una única dirección IP, son recursos de red redundantes y de alta disponibilidad.
 - Grupos de seguridad: puede especificar uno o varios grupos de seguridad para el destino de montaje. Para obtener más información, consulte [Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje](#).

Para añadir otro grupo de seguridad o cambiar el grupo de seguridad, elija Elegir grupos de seguridad y añada otro grupo de seguridad de la lista. Si no desea utilizar el grupo de seguridad predeterminado, puede eliminarlo. Para obtener más información, consulte [Creación de grupos de seguridad](#).

3. Seleccione Añadir destino de montaje para crear un destino de montaje para una zona de disponibilidad que no lo tenga. Si se configura un destino de montaje para cada zona de disponibilidad, esta opción no estará disponible.

4. Seleccione Guardar para establecer la política del sistema de archivos.

Paso 3: Crear una política de sistema de archivos (opcional)

Existe la opción de crear una política de sistema de archivos para el sistema de archivos. Una política de sistema de archivos EFS es una política de recursos de IAM que se utiliza para controlar el acceso del cliente NFS al sistema de archivos. Para obtener más información, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#).

1. En las Opciones de política, puede elegir cualquier combinación de las políticas preconfiguradas disponibles:
 - Impedir el acceso de la raíz de forma predeterminada
 - Imponer el acceso de solo lectura de forma predeterminada
 - Imponer el cifrado en tránsito a todos los clientes
2. Utilice el Editor de políticas para personalizar una política preconfigurada o crear la suya propia. Al elegir una de las políticas preconfiguradas, la definición de la política de JSON aparece en el editor de políticas. Puede editar el JSON para crear la política que desee. Para deshacer los cambios, seleccione Borrar.

Las políticas preconfiguradas vuelven a estar disponibles en Opciones de políticas.

3. Seleccione Siguiente para revisar y crear el sistema de archivos.

Paso 4: Revisar y crear

1. Revise cada uno de los grupos de configuración del sistema de archivos. Puede realizar cambios en cada grupo en este momento seleccionando Editar.
2. Seleccione Crear para crear su sistema de archivos y volver a la página Sistemas de archivos.

Un banner en la parte superior indica que se está creando el nuevo sistema de archivos. Cuando el sistema de archivos esté disponible, aparecerá un enlace para acceder a la página de detalles del nuevo sistema de archivos en el encabezado.

Cree un sistema de archivos (AWS CLI)

Cuando utiliza el AWS CLI, crea estos recursos en orden. En primer lugar, debe crear un sistema de archivos. A continuación, puede crear objetivos de montaje y cualquier etiqueta opcional adicional para el sistema de archivos mediante AWS CLI los comandos correspondientes.

Los ejemplos siguientes utilizan `adminuser` para los valores del parámetro `--profile`. Debe utilizar un perfil de usuario adecuado para proporcionar sus credenciales. Para obtener más información, consulte [los requisitos previos para su uso AWS CLI en la](#) Guía del AWS Command Line Interface usuario.

- Para crear un sistema de archivos cifrados que utilice las clases de almacenamiento Archivado de EFS, con las copias de seguridad automáticas habilitadas, utilice el comando de CLI `create-file-system` de Amazon EFS (la operación correspondiente es [CreateFileSystem](#)), tal y como se muestra a continuación.

```
aws efs create-file-system \  
--creation-token creation-token \  
--encrypted \  
--backup \  
--performance-mode generalPurpose \  
--throughput-mode bursting \  
--region aws-region \  
--tags Key=key,Value=value Key=key1,Value=value1 \  
--profile adminuser
```

Por ejemplo, el siguiente comando `create-file-system` crea un sistema de archivos en la Región de AWS `us-west-2`. El comando especifica `MyFirstFS` como token de creación. Para obtener una lista de los Regiones de AWS lugares en los que puede crear un sistema de archivos de Amazon EFS, consulte los [puntos de enlace y las cuotas de Amazon EFS](#) en Referencia general de Amazon Web Services

```
aws efs create-file-system \  
--creation-token MyFirstFS \  
--backup \  
--encrypted \  
--performance-mode generalPurpose \  
--throughput-mode bursting \  
--region us-west-2 \  
--tags Key=Name,Value="Test File System" Key=developer,Value=rhoward \  

```

```
--profile adminuser
```

Después de crear correctamente el sistema de archivos, Amazon EFS devuelve la descripción del sistema de archivos como JSON, tal y como se muestra en el siguiente ejemplo.

```
{
  "OwnerId": "123456789abcd",
  "CreationToken": "MyFirstFS",
  "Encrypted": true,
  "FileSystemId": "fs-c7a0456e",
  "CreationTime": 1422823614.0,
  "LifecycleState": "creating",
  "Name": "Test File System",
  "NumberOfMountTargets": 0,
  "SizeInBytes": {
    "Value": 6144,
    "ValueInIA": 0,
    "ValueInStandard": 6144
    "ValueInArchive": 0
  },
  "PerformanceMode": "generalPurpose",
  "ThroughputMode": "bursting",
  "Tags": [
    {
      "Key": "Name",
      "Value": "Test File System"
    }
  ]
}
```

- El siguiente ejemplo crea un sistema de archivos que utiliza clases de almacenamiento Estándar en la zona de disponibilidad us-west-2a mediante la propiedad `availability-zone-name`.

```
aws efs create-file-system \
--creation-token MyFirstFS \
--availability-zone-name us-west-2a \
--backup \
--encrypted \
--performance-mode generalPurpose \
--throughput-mode bursting \
--region us-west-2 \
--tags Key=Name,Value="Test File System" Key=developer,Value=rhoward \
```

```
--profile adminuser
```

Después de crear correctamente el sistema de archivos, Amazon EFS devuelve la descripción del sistema de archivos como JSON, tal y como se muestra en el siguiente ejemplo.

```
{
  "AvailabilityZoneId": "usw-az1",
  "AvailabilityZoneName": "us-west-2a",
  "OwnerId": "123456789abcd",
  "CreationToken": "MyFirstFS",
  "Encrypted": true,
  "FileSystemId": "fs-c7a0456e",
  "CreationTime": 1422823614.0,
  "LifecycleState": "creating",
  "Name": "Test File System",
  "NumberOfMountTargets": 0,
  "SizeInBytes": {
    "Value": 6144,
    "ValueInIA": 0,
    "ValueInStandard": 6144,
    "ValueInArchive": 0
  },
  "PerformanceMode": "generalPurpose",
  "ThroughputMode": "bursting",
  "Tags": [
    {
      "Key": "Name",
      "Value": "Test File System"
    }
  ]
}
```

Amazon EFS también ofrece el comando de CLI `describe-file-systems` (la operación de la API correspondiente es [DescribeFileSystems](#)) que puede utilizar para recuperar una lista de sistemas de archivos en su cuenta, tal y como se muestra a continuación.

```
aws efs describe-file-systems \
--region aws-region \
--profile adminuser
```


Amazon EFS devuelve una lista de los sistemas de archivos que Cuenta de AWS creó en la región especificada.

Eliminar los sistemas de archivos Amazon EFS

La eliminación de sistemas de archivos es una acción destructiva que no puede deshacer. Perderá el sistema de archivos y todos los datos que contenga. Los datos que se eliminan de un sistema de archivos se pierden y no se pueden restaurar. Cuando los usuarios eliminan datos de un sistema de archivos, estos datos quedan inutilizados de inmediato. EFS sobrescribe forzosamente los datos de forma eventual.

Note

No se puede eliminar un sistema de archivos que forme parte de una configuración de replicación. Debe eliminarse primero la configuración de reproducción. Para obtener más información, consulte [Eliminar configuraciones de replicación](#).

Important

Siempre debe desmontar un sistema de archivos antes de eliminarlo.

Eliminar un sistema de archivos (consola)

Para eliminar un sistema de archivos

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. Seleccione el sistema de archivos que desea eliminar en la página de Sistemas de archivos.
3. Elija Eliminar.
4. En el cuadro de diálogo Eliminar sistema de archivos, introduzca el identificador del sistema de archivos que se muestra y seleccione Confirmar para confirmar la eliminación.

La consola simplifica la eliminación del sistema de archivos. En primer lugar, elimina los destinos de montaje asociados y, a continuación, elimina el sistema de archivos.

Eliminar un sistema de archivos (CLI)

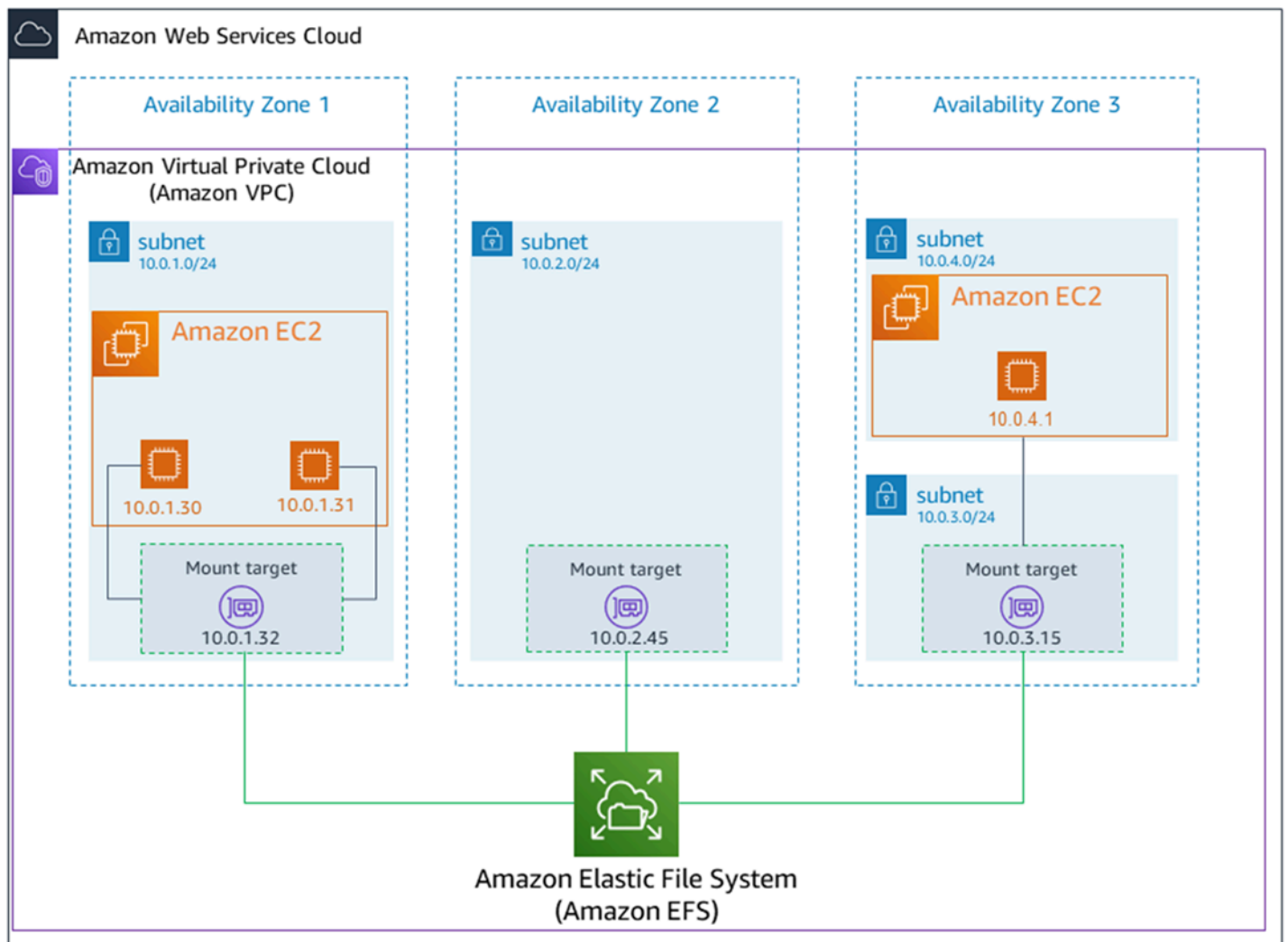
Antes de poder utilizar el AWS CLI comando para eliminar un sistema de archivos, debe eliminar todos los destinos de montaje y los puntos de acceso que se crearon para el sistema de archivos.

Para ver ejemplos de AWS CLI comandos, consulte [Paso 4: Limpiar](#).

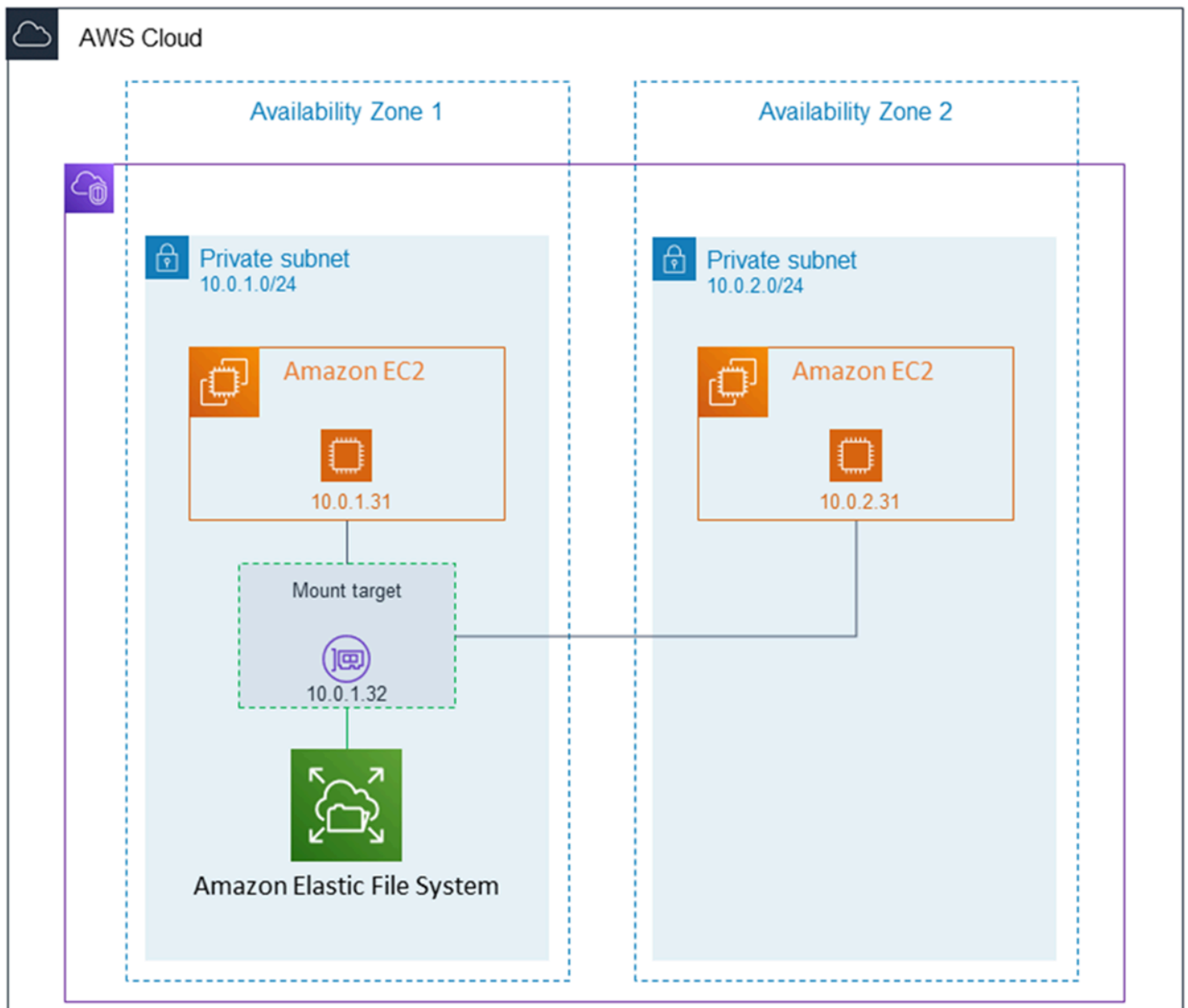
Administrar destinos de montaje

Una vez creado un sistema de archivos de Amazon EFS, puede crear destinos de montaje. En el caso de sistemas de archivos de Amazon EFS que utilizan clases de almacenamiento Regional, se puede crear un destino de montaje en cada zona de disponibilidad de una Región de AWS. En el caso de sistemas de archivos One Zone, solo se puede crear un único destino de montaje en la misma zona de disponibilidad que el sistema de archivos. A continuación, puede montar el sistema de archivos en instancias informáticas, incluidas Amazon EC2 y Amazon ECS, y AWS Lambda en su nube privada virtual (VPC).

El siguiente diagrama muestra un sistema de archivos regional con destinos de montaje creados en todas las zonas de disponibilidad de la VPC.



El siguiente diagrama muestra un sistema de archivos One Zone, con un único destino de montaje creado en la misma zona de disponibilidad que el sistema de archivos. El acceso al sistema de archivos mediante la instancia EC2 de la zona de disponibilidad us-west2c conlleva gastos de acceso a los datos, ya que se encuentra en una zona de disponibilidad diferente a la del destino de montaje.



El grupo de seguridad del destino de montaje funciona como un firewall virtual que controla el tráfico. Por ejemplo, determina qué clientes pueden acceder al sistema de archivos. En esta sección se explica lo siguiente:

- Administración de grupos de seguridad de destinos de montaje y habilitación del tráfico.
- Montaje del sistema de archivos en sus clientes.
- Consideraciones de permisos en el nivel de NFS.

Inicialmente, solo el usuario root de la instancia de Amazon EC2 tiene read-write-execute permisos en el sistema de archivos. En este tema se explican los permisos en el nivel de NFS y se ofrecen

ejemplos que le muestran cómo otorgar permisos en situaciones comunes. Para obtener más información, consulte [Trabajar con usuarios, grupos y permisos a nivel del sistema de archivos de red \(NFS\)](#).

Puede crear objetivos de montaje para un sistema de archivos mediante los AWS Management Console SDK AWS CLI o mediante programación mediante los SDK. AWS Cuando se utiliza la consola, puede crear destinos de montaje al crear por primera vez un sistema de archivos o después de que se haya creado el sistema de archivos.

Para obtener instrucciones sobre cómo crear destinos de montaje mediante la consola Amazon EFS al crear un sistema de archivos, consulte [Paso 2: Configurar un acceso a la red](#).

Administre los objetivos de montaje (consola)

Utilice el siguiente procedimiento para agregar o modificar destinos de montaje para un sistema de archivos existente de Amazon EFS.

Para gestionar los destinos de montaje en un sistema de archivos Amazon EFS

1. Inicie sesión en la consola de Amazon EFS AWS Management Console y ábrala en <https://console.aws.amazon.com/efs/>.
2. En el panel de navegación izquierdo, elija Sistemas de archivos. La página Sistemas de archivos muestra los sistemas de archivos EFS de su cuenta.
3. Seleccione el sistema de archivos para el que desee administrar los destinos de montaje; para ello, seleccione su Nombre o el ID del sistema de archivos y se mostrará la página de detalles del sistema de archivos.
4. Seleccione Red para ver la lista de destinos de montaje existentes.
5. Seleccione Administrar para visualizar la página de la Zona de disponibilidad y realizar modificaciones.

En esta página, para los destinos de montaje existentes, puede añadir y eliminar grupos de seguridad o eliminar el destino de montaje. También puede crear nuevos destinos de montaje.

Note

En el caso de sistemas de archivos One Zone, solo se puede crear un único destino de montaje que se encuentre en la misma zona de disponibilidad que el sistema de archivos.

- Para eliminar un grupo de seguridad de un destino de montaje, elija una X junto al ID del grupo de seguridad.
- Para añadir un grupo de seguridad a un destino de montaje, elija Seleccionar grupos de seguridad para ver una lista de los grupos de seguridad disponibles. O bien, introduzca un ID de grupo de seguridad en el campo de búsqueda situado en la parte superior de la lista.
- Para poner en cola un destino de montaje para eliminarlo, seleccione Eliminar.

Note

Antes de eliminar un destino de montaje, desmonte primero el sistema de archivos.

- Para añadir un destino de montaje, seleccione Añadir destino de montaje. Esta opción solo está disponible para los sistemas de archivos que utilizan clases de almacenamiento Regional de EFS y si aún no existen destinos de montaje en cada zona de disponibilidad para la Región de AWS.

6. Elija Guardar para guardar cualquier cambio.

Para cambiar la VPC de un sistema de archivos de Amazon EFS (consola)

Para cambiar la VPC de la configuración de red de un sistema de archivos, debe eliminar todos los destinos de montaje existentes del sistema de archivos.

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. En el panel de navegación izquierdo, elija Sistemas de archivos. La página Sistemas de archivos muestra los sistemas de archivos EFS de su cuenta.
3. Para el sistema de archivos por el que desee cambiar la VPC, elija el Nombre o ID del sistema de archivos. Aparece la página de detalles del sistema de archivos.
4. Seleccione Red para ver la lista de destinos de montaje existentes.

5. Elija Administrar. Aparece la página de la Zona de disponibilidad.
6. Elimine todos los detalles de montaje que se muestran en la página.
7. Seleccione Guardar para guardar los cambios y eliminar los detalles de montaje. La pestaña Red muestra el estado de los detalles de montaje como borrado.
8. Cuando todos los estados de los objetivos de montaje aparezcan como eliminados, seleccione Administrar. Aparece la página de la Zona de disponibilidad.
9. Elija la nueva VPC de la lista de Nube privada virtual (VPC).
10. Seleccione Añadir destino de montaje para añadir un nuevo destino de montaje. Para cada destino de montura que añada, introduzca lo siguiente:
 - Una Zona de disponibilidad
 - Un ID de subred
 - Una Dirección IP, o manténgalo en Automático
 - Uno o más Grupos de seguridad
11. Elija Guardar para implementar la VPC y los cambios de destino de montaje.

Administrar los objetivos de montaje (CLI)

Note

En el caso de sistemas de archivos One Zone, solo se puede crear un único destino de montaje que se encuentre en la misma zona de disponibilidad que el sistema de archivos.

Para crear un destino de montaje (CLI)

- Para crear un destino de montaje, use el comando de CLI `create-mount-target` (la operación correspondiente es [CreateMountTarget](#)), tal y como se muestra a continuación.

```
$ aws efs create-mount-target \  
--file-system-id file-system-id \  
--subnet-id subnet-id \  
--security-group ID-of-the-security-group-created-for-mount-target \  
--region aws-region \  
--profile adminuser
```

El ejemplo siguiente muestra el comando con datos de muestra.

```
$ aws efs create-mount-target \  
--file-system-id fs-0123467 \  
--subnet-id subnet-b3983dc4 \  
--security-group sg-01234567 \  
--region us-east-2 \  
--profile adminuser
```

Después de crear correctamente el destino de montaje, Amazon EFS devuelve la descripción del destino de montaje como JSON tal y como se muestra en el siguiente ejemplo.

```
{  
  "MountTargetId": "fsmt-f9a14450",  
  "NetworkInterfaceId": "eni-3851ec4e",  
  "FileSystemId": "fs-b6a0451f",  
  "LifecycleState": "available",  
  "SubnetId": "subnet-b3983dc4",  
  "OwnerId": "23124example",  
  "IpAddress": "10.0.1.24"  
}
```

Para recuperar una lista de destinos de montaje para un sistema de archivos (CLI)

- También puede recuperar una lista de destinos de montaje creada para un sistema de archivos mediante el comando de CLI [describe-mount-targets](#) (la operación correspondiente es [DescribeMountTargets](#)), tal y como se muestra a continuación.

```
$ aws efs describe-mount-targets --file-system-id fs-a576a6dc
```

```
{  
  "MountTargets": [  
    {  
      "OwnerId": "111122223333",  
      "MountTargetId": "fsmt-48518531",  
      "FileSystemId": "fs-a576a6dc",  
      "SubnetId": "subnet-88556633",  
      "LifecycleState": "available",  
      "IpAddress": "172.31.25.203",
```



```

    "NetworkInterfaceId": "eni-0123456789abcdef1",
    "AvailabilityZoneId": "use2-az2",
    "AvailabilityZoneName": "us-east-2b"
  },
  {
    "OwnerId": "111122223333",
    "MountTargetId": "fsmt-5651852f",
    "FileSystemId": "fs-a576a6dc",
    "SubnetId": "subnet-44223377",
    "LifecycleState": "available",
    "IpAddress": "172.31.46.181",
    "NetworkInterfaceId": "eni-0123456789abcdefa",
    "AvailabilityZoneId": "use2-az3",
    "AvailabilityZoneName": "us-east-2c"
  },
  {
    "OwnerId": "111122223333",
    "MountTargetId": "fsmt-5751852e",
    "FileSystemId": "fs-a576a6dc",
    "SubnetId": "subnet-a3520bcb",
    "LifecycleState": "available",
    "IpAddress": "172.31.12.219",
    "NetworkInterfaceId": "eni-0123456789abcdef0",
    "AvailabilityZoneId": "use2-az1",
    "AvailabilityZoneName": "us-east-2a"
  }
]
}

```

Para eliminar un destino de montaje existente (CLI)

- Para eliminar un destino de montaje existente, utilice el `delete-mount-target` AWS CLI comando (la operación correspondiente es [DeleteMountTarget](#)), como se muestra a continuación.

Note

Antes de eliminar un destino de montaje, desmonte primero el sistema de archivos.

```
$ aws efs delete-mount-target \
```

```
--mount-target-id mount-target-ID-to-delete \  
--region aws-region-where-mount-target-exists
```

A continuación se muestra un ejemplo con datos de muestra.

```
$ aws efs delete-mount-target \  
--mount-target-id fsmt-5751852e \  
--region us-east-2 \  

```

Para modificar el grupo de seguridad de un destino de montaje existente

- Para modificar los grupos de seguridad que están en vigor para un destino de montaje, utilice el `modify-mount-target-security-group` AWS CLI comando (la operación correspondiente es [ModifyMountTargetSecurityGroups](#)) para reemplazar los grupos de seguridad existentes, como se muestra a continuación.

```
$ aws efs modify-mount-target-security-groups \  
--mount-target-id mount-target-ID-whose-configuration-to-update \  
--security-groups security-group-ids-separated-by-space \  
--region aws-region-where-mount-target-exists \  
--profile adminuser
```

A continuación se muestra un ejemplo con datos de muestra.

```
$ aws efs modify-mount-target-security-groups \  
--mount-target-id fsmt-5751852e \  
--security-groups sg-1004395a sg-1114433a \  
--region us-east-2
```

Para obtener más información, consulte [Tutorial: Cree un sistema de archivos Amazon EFS y móntelo en una instancia de Amazon EC2 mediante AWS CLI](#).

Creación de grupos de seguridad

Tanto una instancia de Amazon EC2 como un destino de montaje tienen grupos de seguridad asociados. Estos grupos de seguridad actúan como un firewall virtual que controla el tráfico entre

ellos. Si no proporciona un grupo de seguridad al crear un destino de montaje, Amazon EFS le asocia el grupo de seguridad predeterminado de la VPC.

Independientemente, para habilitar el tráfico entre una instancia EC2 y un destino de montaje (y, por lo tanto, el sistema de archivos), debe configurar las siguientes reglas en estos grupos de seguridad:

- Los grupos de seguridad que se asocian a un destino de montaje deben permitir el acceso de entrada al protocolo TCP en el puerto NFS desde todas las instancias EC2 en las que se desea montar el sistema de archivos.
- Cada instancia EC2 que monta el sistema de archivos debe tener un grupo de seguridad que permite el acceso de salida al destino de montaje en el puerto NFS.

Para cambiar los grupos de seguridad asociados a los destinos de montaje de los sistemas de archivos EFS, consulte [Administrar destinos de montaje](#).

Para obtener más información sobre los grupos de seguridad, consulte los [grupos de seguridad de Amazon EC2 para instancias de Linux](#) en la Guía del usuario de Amazon EC2.

Note

La siguiente sección es específica de Amazon EC2 y explica cómo crear grupos de seguridad para que pueda utilizar Secure Shell (SSH) para conectarse a las instancias en las que ha montado los sistemas de archivos de Amazon EFS. Si no utiliza SSH para conectarse a sus instancias de Amazon EC2, puede omitir esta sección.

Cree un grupo de seguridad mediante la consola

Puede usarlo AWS Management Console para crear grupos de seguridad en su VPC. Para conectar su sistema de archivos de Amazon EFS a su instancia de Amazon EC2, debe crear dos grupos de seguridad: uno para su instancia de Amazon EC2 y otra para su destino de montaje de Amazon EFS.

1. Cree dos grupos de seguridad en su VPC. Para obtener instrucciones, consulte [Crear un grupo de seguridad](#) en la Guía del usuario de Amazon VPC.
2. En la consola de la VPC, compruebe las reglas predeterminadas para estos grupos de seguridad. Ambos grupos de seguridad deben tener una única regla de salida que permita la salida de tráfico.

3. Debe autorizar el acceso adicional a los grupos de seguridad tal y como se indica a continuación:
 - a. Agregue una regla al grupo de seguridad de EC2 para permitir el acceso SSH a la instancia en el puerto 22 como se muestra a continuación. Esto es útil si planea utilizar un cliente de SSH como PuTTY para conectarse y administrar su instancia EC2 a través de una interfaz de terminal. De forma opcional, puede restringir la dirección Source (Origen).

Para obtener instrucciones, consulte [Añadir reglas a un grupo de seguridad](#) en la Guía del usuario de Amazon VPC.

- b. Añada una regla al grupo de seguridad Mount Target para permitir el acceso entrante desde el grupo EC2Security en el puerto TCP 2049. El grupo de seguridad asignado como origen es el grupo de seguridad asociado a la instancia EC2.

Para ver los grupos de seguridad asociados a los destinos de montaje de los sistemas de archivos, en la consola EFS, seleccione la pestaña Red en la página de detalles del sistema de archivos. Para obtener más información, consulte [Administrar destinos de montaje](#).

Note

No es necesario añadir una regla de salida, ya que la regla de salida predeterminada permite que salga todo el tráfico. (Si elimina la regla de salida predeterminada, debe añadir una regla de salida para abrir una conexión TCP en el puerto NFS e identificar el grupo de seguridad de destino de montaje como destino.)

4. Compruebe que ambos grupos de seguridad autorizan ahora el acceso entrante y saliente tal y como se describe en esta sección.

Crear un grupo de seguridad mediante la CLI

Para ver un ejemplo que muestra cómo crear grupos de seguridad mediante el AWS CLI, consulte [Paso 1: Crear los recursos de Amazon ECS](#).

Creación de políticas de sistema de archivos

Puede crear una política de sistema de archivos mediante la consola de Amazon EFS o utilizando la AWS CLI. También puede crear una política de sistema de archivos mediante programación

mediante AWS SDK o directamente con la API de Amazon EFS. Las políticas del sistema de archivos EFS tienen un límite de 20 000 caracteres. Para obtener más información sobre el uso de una política de sistema de archivos EFS y ejemplos, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#).

Note

Los cambios en la política del sistema de archivos de Amazon EFS pueden tardar varios minutos en surtir efecto.

Cree una política de sistema de archivos (consola)

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. Elija File Systems (Sistemas de archivos).
3. En la página File systems (Sistemas de archivos) elija el sistema de archivos que quiere editar o para el que desea crear una política de sistema de archivos. Aparece la página de detalles de ese sistema de archivos.
4. Elija Política del sistema de archivos y, a continuación, elija Editar. Aparece la página File system policy (Política del sistema de archivos).

5. En las Opciones de política, puede elegir cualquier combinación de las políticas de sistemas de archivos preconfiguradas:

- Impedir el acceso a la raíz de forma predeterminada: esta opción elimina `ClientRootAccess` del conjunto de acciones EFS permitidas.
- Imponer el acceso de solo lectura de forma predeterminada: esta opción elimina `ClientWriteAccess` del conjunto de acciones EFS permitidas.
- Impedir el acceso anónimo: esta opción elimina `ClientMount` del conjunto de acciones EFS permitidas.
- Imponer el cifrado en tránsito a todos los clientes: esta opción deniega el acceso a los clientes no cifrados.

Al elegir una política preconfigurada, el objeto JSON de la política se muestra en el panel del Editor de políticas.

6. Utilice Otorgar permisos adicionales para conceder permisos de sistema de archivos a otros directores de IAM, incluido otro. Cuenta de AWS Elija Añadir e introduzca el ARN de entidad principal de la entidad a la que está concediendo los permisos. A continuación, elija los Permisos que desea conceder. Los permisos adicionales se muestran en el Editor de políticas.
7. Puede utilizar el Editor de políticas para personalizar una política preconfigurada o crear su propia política de sistema de archivos. Al utilizar el editor, las opciones de política preconfiguradas dejan de estar disponibles. Para borrar la política actual del sistema de archivos y empezar a crear una nueva política, seleccione Borrar.

Al borrar el editor, las políticas preconfiguradas vuelven a estar disponibles.

8. Cuando termine de editar la política, seleccione Guardar.

Crear una política de sistema de archivos (CLI)

En el siguiente ejemplo, el comando [put-file-system-policy](#) CLI crea una política de sistema de archivos que permite el acceso de Cuenta de AWS solo lectura especificado al sistema de archivos EFS. El comando API equivalente es [PutFileSystemPolicy](#).

```
aws efs put-file-system-policy --file-system-id fs-01234567 --policy '{
  "Id": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientMount"
      ]
    }
  ]
}
```

```

    ],
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    }
  }
]
}'

```

```

{
  "FileSystemId": "fs-01234567",
  "Policy": "{
  "Version" : "2012-10-17",
  "Id" : "1",
  "Statement" : [
    {
      "Sid" : "efs-statement-7c8d8687-1c94-4fdc-98b7-555555555555",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "elasticfilesystem:ClientMount"
      ],
      "Resource" : "arn:aws:elasticfilesystem:us-east-2:555555555555:file-system/
fs-01234567"
    }
  ]
}
}

```

Crear puntos de acceso

Puede crear puntos de acceso de Amazon EFS mediante el AWS Management Console o el AWS CLI. También puede crear puntos de acceso mediante programación mediante los AWS SDK o la API de Amazon EFS directamente. No puede modificar un punto de acceso una vez creado. Un sistema de archivos puede tener un máximo de 1000 puntos de acceso. Para obtener más información acerca de los puntos de acceso de EFS, consulte [Trabajo con puntos de acceso de Amazon EFS](#).

Cree un punto de acceso (consola)

Puede crear y eliminar puntos de acceso de Amazon EFS mediante la AWS Management Console API y los SDK de Amazon EFS AWS Command Line Interface (AWS CLI). No puede modificar un punto de acceso una vez creado. Un sistema de archivos puede tener un máximo de 1000 puntos de acceso.

Note

Si se envían varias solicitudes para crear puntos de acceso en el mismo sistema de archivos en rápida sucesión y el sistema de archivos se acerca al límite de 1000 puntos de acceso, es posible que estas solicitudes reciban una respuesta limitadora. Esto es para garantizar que el sistema de archivos no supere la cuota de puntos de acceso indicada.

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. Elija Puntos de acceso para abrir la ventana Puntos de acceso.
3. Elija Crear puntos de acceso para mostrar la página Crear punto de acceso.

También puede abrir la página Crear punto de acceso seleccionando Sistemas de archivos. Elija un Nombre o ID de sistema de archivos y, a continuación, elija Puntos de acceso y Crear punto de acceso para crear un punto de acceso para ese sistema de archivos.


a. Introduzca la siguiente información en el panel Detalles:

- Sistema de archivos: introduzca un nombre o ID de sistema de archivos y elija el sistema de archivos correspondiente. También puede elegir el sistema de archivos de la lista que aparezca al elegir el campo de entrada.
- (Opcional) Nombre: escriba un nombre para el punto de acceso.
- (Opcional) Ruta del directorio raíz: se puede especificar un directorio raíz para el punto de acceso; la raíz del punto de acceso predeterminada es /. Para introducir una ruta de directorio raíz, utilice el formato /foo/bar. Para obtener más información, consulte [Aplicación de un directorio raíz con un punto de acceso](#).

b. (Opcional) En el panel de Usuario de POSIX, puede especificar la identidad POSIX completa que se utilizará para aplicar la información de usuarios y grupos a todas las operaciones de archivos que realicen los clientes de NFS que utilicen el punto de acceso.

Para obtener más información, consulte [Aplicación de una identidad de usuario mediante un punto de acceso](#).

- ID de usuario: introduzca un ID de usuario POSIX numérico para el usuario.
 - ID de grupo: introduzca un ID de grupo POSIX numérico para el usuario.
 - ID de grupos secundarios: introduzca una lista opcional de identificadores de grupos secundarios separados por comas.
- c. (Opcional) Para los Permisos de creación del directorio raíz, puede especificar los permisos que se utilizarán cuando Amazon EFS cree la ruta del directorio raíz, si se ha especificado y el directorio raíz aún no existe. Para obtener más información, consulte [Aplicación de un directorio raíz con un punto de acceso](#).

 Note

Si no se especifica la propiedad ni los permisos de ningún directorio raíz, y el directorio raíz aún no existe, EFS no creará el directorio raíz. Todo intento de montar el sistema de archivos mediante el punto de acceso fallará.

- ID de usuario propietario: introduzca el ID de usuario POSIX numérico que se utilizará como propietario del directorio raíz.
 - ID de grupo propietario: introduzca el ID de grupo POSIX numérico que se utilizará como grupo propietario del directorio raíz.
 - Permisos: introduzca el modo Unix del directorio. Una configuración común es 755. Asegúrese de que el bit de ejecución esté configurado para que el usuario del punto de acceso pueda montar.
4. Elija Crear punto de acceso para crear el punto de acceso mediante esta configuración.

Crear un punto de acceso (CLI)

El siguiente ejemplo, el comando de CLI `create-access-point` crea un punto de acceso para un sistema de archivos EFS. El comando API equivalente es [CreateAccessPoint](#).

```
aws efs create-access-point --file-system-id fs-abcdef0123456789a --client-token
010102020-3 \
--root-directory "Path=/efs/mobileapp/
east,CreationInfo={OwnerId=0,OwnerGid=11,Permissions=775}" \
```

```
--posix-user "Uid=22,Gid=4" \
--tags Key=Name,Value=east-users
```

Si la solicitud se realiza correctamente, la CLI responde con la descripción del punto de acceso.

```
{
  "ClientToken": "010102020-3",
  "Name": "east-users",
  "AccessPointId": "fsap-abcd1234ef5678901",
  "AccessPointArn": "arn:aws:elasticfilesystem:us-east-2:111122223333:access-point/
fsap-abcd1234ef5678901",
  "FileSystemId": "fs-01234567",
  "LifecycleState": "creating",
  "OwnerId": "111122223333",
  "PosixUser": {
    "Gid": 4,
    "Uid": 22
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": 0,
      "OwnerUid": 11,
      "Permissions": "775"
    },
    "Path": "/efs/mobileapp/east",
  },
  "Tags": []
}
```

Note

Si se envían varias solicitudes para crear puntos de acceso en el mismo sistema de archivos en rápida sucesión y el sistema de archivos se acerca al límite de 1000 puntos de acceso, es posible que estas solicitudes reciban una respuesta limitadora. Esto es para garantizar que el sistema de archivos no supere la cuota de puntos de acceso indicada.

Eliminar puntos de acceso

Al eliminar un punto de acceso, los clientes que utilicen dicho punto pierden el acceso al sistema de archivos Amazon EFS para el que está configurado.

Eliminar un punto de acceso (consola)

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. En el panel de navegación izquierdo, elija Puntos de acceso para abrir la página de Puntos de acceso.
3. Seleccione el punto de acceso que desee eliminar.
4. Elija Eliminar.
5. Elija Confirmar para confirmar la acción y eliminar el punto de acceso.

Eliminar un punto de acceso (CLI)

En el siguiente ejemplo, el comando `delete-access-point` de la CLI elimina el punto de acceso especificado. El comando API equivalente es [DeleteAccessPoint](#). Si el comando se ejecuta correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

```
aws efs delete-access-point --access-point-id fsap-092e9f80b3fb5e6f3 --client-token 010102020-3
```

Etiquetado de los recursos de Amazon EFS

Para ayudarle a administrar sus recursos de Amazon EFS, puede asignar sus propios metadatos a cada recurso en forma de etiquetas. Con las etiquetas, puede clasificar AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Esta categorización resulta útil cuando se tienen muchos recursos del mismo tipo: se puede identificar rápidamente un recurso específico en función de las etiquetas que se le hayan asignado. En este tema se describe qué son las etiquetas y cómo crearlas.

Conceptos básicos de etiquetas

Una etiqueta es una etiqueta que se asigna a un AWS recurso. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario.

Las etiquetas te permiten clasificar AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Por ejemplo, se podría definir un conjunto de etiquetas para los sistemas de archivo Amazon EFS de la cuenta que ayuden a realizar un seguimiento del propietario de cada sistema de archivos.

Recomendamos que cree un conjunto de claves de etiqueta que cumpla sus necesidades para cada tipo de recurso. Mediante el uso de un conjunto coherente de claves de etiquetas, podrá administrar los recursos de más fácilmente. Puede buscar y filtrar los recursos en función de las etiquetas que agregue.

Las etiquetas no tienen ningún significado semántico para Amazon EFS, por lo que se interpretan estrictamente como cadenas de caracteres. Además, las etiquetas no se asignan a los recursos automáticamente. Puede editar las claves y los valores de las etiquetas y también puede eliminar etiquetas de un recurso en cualquier momento. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- Número máximo de etiquetas por recurso: 50
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Longitud máxima de la clave: 128 caracteres Unicode en UTF-8
- Longitud máxima del valor: 256 caracteres Unicode en UTF-8
- Si bien Amazon EFS admite el uso de cualquier carácter en sus etiquetas, otros servicios son más restrictivos. Los caracteres permitidos en los servicios son: letras, números y espacios representables en UTF-8, además de los siguientes caracteres: + - = . _ : / @.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El `aws :` prefijo está reservado para su AWS uso. Si la etiqueta tiene una clave de etiqueta con este prefijo, no puede editar ni eliminar la clave o el valor de la etiqueta. Las etiquetas que tengan el prefijo `aws :` no cuentan para el límite de etiquetas por recurso.

No puede actualizar ni eliminar un recurso basándose únicamente en sus etiquetas; debe especificar el identificador del recurso. Por ejemplo, para eliminar sistemas de archivo que se etiquetaron con una clave de etiqueta llamada `DeleteMe`, debe utilizar la acción `DeleteFileSystem` con los identificadores de recursos del sistema de archivos, como `fs-1234567890abcdef0`.

Cuando etiqueta recursos públicos o compartidos, las etiquetas que asigne solo están disponibles para su Cuenta de AWS. Ninguna otra Cuenta de AWS persona tendrá acceso a esas etiquetas.

Para el control de acceso a los recursos compartidos basado en etiquetas, cada una Cuenta de AWS debe asignar su propio conjunto de etiquetas para controlar el acceso al recurso.

Se pueden etiquetar recursos de punto de acceso y de sistemas de archivos de Amazon EFS.

Uso de etiquetas para el control de acceso

Puede utilizar etiquetas para controlar el acceso a los recursos de Amazon EFS e implementar el control de acceso basado en atributos (ABAC).

Note

La replicación no admite el uso de etiquetas para el control de acceso basado en atributos (ABAC).

Etiquetar los recursos

Se pueden etiquetar recursos de punto de acceso y de sistemas de archivos de Amazon EFS que ya existan en la cuenta.

Etiquete un sistema de archivos o un recurso de punto de acceso (consola)

- Se puede utilizar la consola de Amazon EFS para aplicar etiquetas a los recursos existentes mediante la pestaña Etiquetas de la pantalla de detalles del recurso. En la consola de Amazon EFS se pueden especificar etiquetas para un recurso al crear dicho recurso. Por ejemplo, se puede añadir una etiqueta con una clave de Name y un valor que se especifique. En la mayoría de los casos, la consola aplica las etiquetas inmediatamente después de crear el recurso (y no durante la creación del mismo). Aunque la consola organiza los recursos según la etiqueta Name, dicha etiqueta no tiene ningún significado semántico para el servicio Amazon EFS.

Etiquetar un sistema de archivos o un recurso de punto de acceso (CLI)

- Si utiliza la API de Amazon EFS, el o un AWS SDK AWS CLI, puede utilizar la acción de la API de TagResource EFS para aplicar etiquetas a los recursos existentes. Además, algunas acciones de creación de recursos le permiten especificar etiquetas para un recurso al crear dicho recurso.

Los AWS CLI comandos para gestionar las etiquetas y las acciones equivalentes de la API Amazon EFS se muestran en la siguiente tabla.

Command de la CLI	Descripción	Operación de la API equivalente
tag-resource	Añadir nuevas etiquetas o actualizar etiquetas existentes	TagResource
list-tags-for-resource	Recuperar etiquetas existentes	ListTagsForResource
untag-resource	Eliminar etiquetas existentes	UntagResource

Instalación de las herramientas de Amazon EFS

El paquete `amazon-efs-utils` es una colección de código abierto de herramientas de Amazon EFS que también se denomina cliente de Amazon EFS. A continuación encontrará una descripción del cliente de Amazon EFS. El cliente de Amazon EFS incluye el asistente de montaje de Amazon EFS, que facilita el montaje de sistemas de archivos de EFS. El uso del cliente EFS permite utilizar Amazon CloudWatch para supervisar el estado de montaje de un sistema de archivos EFS. Tiene que instalar un cliente de Amazon EFS en la instancia de Amazon EC2 antes de montar el sistema de archivos de Amazon EFS.

Temas

- [Acerca del cliente Amazon EFS](#)
- [Utilización AWS Systems Manager para instalar o actualizar automáticamente el cliente Amazon EFS](#)
- [Instalación manual del cliente de Amazon EFS](#)
- [Instalación y actualización botocore](#)
- [Actualización de stunnel](#)

Acerca del cliente Amazon EFS

El cliente de Amazon EFS (`amazon-efs-utils`) es una colección de herramientas de Amazon EFS de código abierto. El uso del cliente Amazon EFS, que puede descargar desde GitHub aquí: <https://github.com/aws/efs-utils>.

El `amazon-efs-utils` paquete viene preinstalado en Amazon Machine Images (AMI) de Amazon Linux 2023 (AL2023), Amazon Linux 2 (AL2) y Amazon Linux (AL1). El paquete está disponible en los repositorios de paquetes de Amazon Linux y puede crear e instalar el paquete en otras distribuciones de Linux. También se puede utilizar AWS Systems Manager para instalar o actualizar automáticamente el paquete. Para obtener más información, consulte [Utilización AWS Systems Manager para instalar o actualizar automáticamente el cliente Amazon EFS](#).

Note

La AMI de Amazon Linux (AL1) alcanzó su valor end-of-life el 31 de diciembre de 2023 y no es compatible con los `amazon-efs-utils` paquetes publicados en abril de 2024

y versiones posteriores (versión 2.0 y posteriores). Le recomendamos que actualice las aplicaciones a Amazon Linux 2023 (AL2023), que incluye soporte a largo plazo hasta 2028.

El cliente de Amazon EFS incluye un asistente de montaje y herramientas que facilitan el cifrado de los datos en tránsito para los sistemas de archivos de Amazon EFS. Un ayudante de montaje es un programa que se usa para montar un tipo específico de sistema de archivos. Le recomendamos que utilice el ayudante de montaje incluido en el cliente de Amazon EFS para montar los sistemas de archivos de Amazon EFS. El uso del cliente de Amazon EFS simplifica el montaje de los sistemas de archivos de EFS y puede proporcionar un mejor rendimiento del sistema de archivos. Para obtener más información sobre el uso del cliente y el ayudante de montaje de EFS, consulte [Montaje de sistemas de archivos de EFS](#).

Existen las siguientes dependencias en `amazon-efs-utils` y se instalan al instalar el paquete de `amazon-efs-utils`:

- Cliente de NFS
 - `nfs-utils` para distribuciones de RHEL, CentOS, Amazon Linux y Fedora
 - `nfs-common` para distribuciones Debian y Ubuntu
- Retransmisión de red (paquete `stunnel`, versión 4.56 o posterior)
- Python (versión 3.4 o posterior)
- OpenSSL 1.0.2 o posterior

Note

De forma predeterminada, cuando se utiliza dicho ayudante de montaje de Amazon EFS con TLS (Transport Layer Security), este aplica la comprobación del nombre de host del certificado. El ayudante de montaje de Amazon EFS utiliza el programa `stunnel` para la funcionalidad de TLS. Algunas versiones de Linux no incluyen una versión de `stunnel` que admita estas características de TLS de forma predeterminada. Cuando se utiliza una de esas versiones de Linux, montar un sistema de archivos de Amazon EFS mediante TLS da error. Cuando haya instalado el paquete `amazon-efs-utils`, para actualizar la versión de `stunnel` del sistema, consulte [Actualización de stunnel](#).


Puede utilizarlo AWS Systems Manager para gestionar los clientes de Amazon EFS y automatizar las tareas necesarias para instalar o actualizar el `amazon-efs-utils` paquete

en sus instancias EC2. Para obtener más información, consulte [Utilización AWS Systems Manager para instalar o actualizar automáticamente el cliente Amazon EFS](#).

Si tiene problemas con el cifrado, consulte [Resolución de problemas de cifrado](#).

Distribuciones admitidas

El cliente de Amazon EFS se ha verificado con las siguientes distribuciones de Linux y Mac:

Distribución	Tipo de paquete	Sistema init
Amazon Linux 2023 (AL2023)	rpm	systemd
Amazon Linux 2 (AL2)	rpm	systemd
CentOS 7, 8	rpm	systemd
Amazon Linux (AL1) 2017-09	rpm	upstart
<div data-bbox="142 1037 181 1073" style="float: left; margin-right: 5px;">  </div> <div data-bbox="188 1037 264 1073" style="float: left; margin-right: 10px;"> Note </div> <div data-bbox="188 1094 652 1421" style="float: left;"> <p>La AMI de Amazon Linux (AL1) alcanzó su end-of-life valor el 31 de diciembre de 2023 y no es compatible con los <code>amazon-efs-utils</code> paquetes publicados en abril de 2024 o posteriores (versión 2.0 y posteriores).</p> </div> <div style="clear: both;"></div>		
Debian 9, 10	deb	systemd
Fedora 28 - 32	rpm	systemd
macOS Big Sur		launchd
macOS Monterey		launchd
macOS Ventura		launchd

Distribución	Tipo de paquete	Sistema init
OpenSUSE Leap, Tumbleweed	rpm	systemd
Oracle 8	rpm	systemd
Red Hat Enterprise Linux (RHEL) 7, 8, 9	rpm	systemd
SUSE Linux Enterprise Server (SLES) 12, 15	rpm	systemd
Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS	deb	systemd

[Para obtener una lista completa de las distribuciones compatibles con las que se ha verificado el paquete, consulta el archivo README](#) de `amazon-efs-utils` en Github.

Utilización AWS Systems Manager para instalar o actualizar automáticamente el cliente Amazon EFS

Puede utilizarlo AWS Systems Manager para simplificar la administración del cliente Amazon EFS (`amazon-efs-utils`). AWS Systems Manager es un AWS servicio que puede utilizar para ver y controlar su infraestructura AWS. Con AWS Systems Manager él, puede automatizar las tareas necesarias para instalar o actualizar el `amazon-efs-utils` paquete en sus instancias EC2. Las funciones de Systems Manager, como Distributor y State Manager, le permiten automatizar los siguientes procesos:

- Mantener el control de versiones del cliente de Amazon EFS.
- Almacenamiento centralizado y distribución sistemática del cliente de Amazon EFS a sus instancias de Amazon EC2.
- Automatizar el proceso de mantener las instancias de Amazon EC2 administradas en un estado definido.

Si quiere obtener más información, consulte la [Guía del usuario de AWS Systems Manager](#).

Qué hace el cliente de Amazon EFS durante la instalación

Utiliza el cliente Amazon EFS para automatizar la supervisión de CloudWatch los registros de Amazon para comprobar el estado de montaje del sistema de archivos y actualizar `stunnel` a la versión más reciente para determinadas distribuciones de Linux. Al instalar el cliente de Amazon EFS en sus instancias de Amazon EC2 mediante Systems Manager, este realiza las siguientes acciones:

- Instala el paquete `botocore` siguiendo los mismos pasos descritos en [Instalación y actualización botocore](#). El cliente de Amazon EFS utiliza `botocore` para supervisar el estado de montaje del sistema de archivos EFS.
- Permite monitorear el estado de montaje del sistema de archivos EFS en CloudWatch los registros mediante la actualización `efs-utils.conf`. Para obtener más información, consulte [Supervisión del estado exitoso o fallido del intento de montaje](#).
- Para las instancias de EC2 que ejecutan RHEL7 o CentOS7, el cliente de Amazon EFS actualiza automáticamente `stunnel` como se describe en [Actualización de stunnel](#). Es necesario actualizar `stunnel` para poder montar correctamente un sistema de archivos de EFS mediante TLS, y la versión `stunnel` enviada con RHEL7 y CentOS7 no admite el cliente de Amazon EFS (`amazon-efs-utils`).

Sistemas operativos compatibles con Systems Manager Distributor

Sus instancias de EC2 deben ejecutar uno de los siguientes sistemas operativos para poder utilizarlas con AWS Systems Manager para actualizar o instalar automáticamente el cliente de Amazon EFS.

Plataforma	Versión de la plataforma	Arquitectura
Amazon Linux 2023 (AL2023)	AL2023	x86_64, arm64 (procesadores Graviton2 o posteriores)
Amazon Linux 2 (AL2)	2.0	x86_64, arm64 (Amazon Linux 2, tipos de instancia A1)
Amazon Linux (AL1)	09 de septiembre de 2017, 03 de 2018	x86_64
CentOS	7, 8	x86_64

Plataforma	Versión de la plataforma	Arquitectura
Red Hat Enterprise Linux (RHEL)	7, 8	x86_64, arm64 (RHEL 7.6 y posteriores, tipos de instancia A1)
SUSE Linux Enterprise Server (SLES)	12, 15	x86_64
Servidor Ubuntu	16,04, 18,04, 20,04	x86_64, arm64 (Ubuntu Server 16 y posteriores, tipos de instancia A1)

Cómo utilizar para instalar o AWS Systems Manager actualizar automáticamente amazon-efs-utils

Se requieren dos configuraciones únicas para configurar Systems Manager para instalar o actualizar automáticamente el amazon-efs-utils paquete.

1. Configure un perfil de instancia AWS Identity and Access Management (IAM) con los permisos necesarios.
2. Configure una asociación (incluida la programación) que utilice State Manager para la instalación o las actualizaciones

Paso 1: Configure un perfil de instancia de IAM con los permisos necesarios.

De forma predeterminada, AWS Systems Manager no tiene permiso para administrar sus clientes de Amazon EFS ni para instalar o actualizar el amazon-efs-utils paquete. Para conceder acceso a Systems Manager debe utilizar un perfil de instancias de AWS Identity and Access Management (IAM). Un perfil de instancias es un contenedor que pasa información del rol de IAM a una instancia de Amazon EC2 en el momento del lanzamiento.

Utilice la política de permisos AmazonElasticFileSystemsUtils AWS administrados para asignar los permisos adecuados a las funciones. Puede crear un nuevo rol para su perfil de instancias o agregar la política de permisos de AmazonElasticFileSystemsUtils para un rol existente. A continuación, debe usar este perfil de instancias para lanzar sus instancias de Amazon

EC2. Para obtener más información, consulte [Paso 4: Crear un perfil de instancias de IAM para Systems Manager](#).

Paso 2: Configurar una asociación utilizada por State Manager para instalar o actualizar el cliente de Amazon EFS

El paquete `amazon-efs-utils` se incluye en Distributor y está listo para implementar en instancias de EC2 administradas. Para ver la última versión disponible para su instalación, puede utilizar la AWS Systems Manager consola o la herramienta de línea de AWS comandos que prefiera. `amazon-efs-utils` Para acceder a Distributor, abra <https://console.aws.amazon.com/systems-manager/> y elija Distributor en el panel de navegación izquierdo. Busque AmazonEFSUtils en la sección Propiedad de Amazon. Seleccione AmazonEFSUtils para ver los detalles del paquete. Para obtener más información, consulte [Ver paquetes](#).

Con State Manager, puede instalar o actualizar el paquete `amazon-efs-utils` en las instancias de EC2 administradas de forma inmediata o según una programación. Además, puede asegurarse de que `amazon-efs-utils` se instale automáticamente en las nuevas instancias de EC2. Para obtener más información sobre la instalación o actualización de paquetes mediante Distributor y State Manager, consulte [Trabajar con Distributor](#).

Para instalar o actualizar automáticamente el `amazon-efs-utils` paquete en las instancias mediante la consola de Systems Manager, consulte [Programar la instalación o actualización de un paquete \(consola\)](#). Esto le solicitará que cree una asociación para State Manager, que defina el estado que desea aplicar a un conjunto de instancias. Use las siguientes entradas al crear tu asociación:

- En Parámetros, seleccione Acción > Instalar y Tipo de instalación > Actualización in situ.
- Para Destinos, la configuración recomendada es Elegir todas las instancias para registrar todas las instancias de EC2 nuevas y existentes como destinos para instalar o actualizar AmazonEFSUtils automáticamente. Como alternativa, puede especificar etiquetas de instancias, seleccionar las instancias manualmente o elegir un grupo de recursos para aplicar la asociación a un subconjunto de instancias. Si especifica etiquetas de instancia, debe lanzar las instancias de EC2 con las etiquetas para permitir que AWS Systems Manager instale o actualice automáticamente el cliente Amazon EFS.
- Para Especificar programación, la configuración recomendada para AmazonEFSUtils es cada 30 días. Puede utilizar los controles para crear un programa de cron o rate para la asociación.

AWS Systems Manager Para utilizar el montaje de varios sistemas de archivos Amazon EFS en varias instancias de EC2, consulte [Montaje de EFS en varias instancias de EC2 mediante AWS Systems Manager](#).

Instalación manual del cliente de Amazon EFS

Puede instalar manualmente el cliente Amazon EFS en las instancias de Amazon EC2 Linux que ejecuten Amazon Linux 2023 (AL2023), Amazon Linux 2 (AL2), Amazon Linux (AL1) y otras distribuciones de Linux compatibles, y en las instancias EC2 Mac que ejecuten macOS Big Sur, macOS Monterey y macOS Ventura.

Los procedimientos de instalación de para estos sistemas operativos se describen en las siguientes secciones. Para obtener instrucciones sobre la instalación y actualización del cliente Amazon EFS, consulte [Instalación](#) en el amazon-efs-utils archivo README de Github.

Temas

- [Instalación del cliente Amazon EFS en instancias Linux de Amazon EC2](#)
- [Instalación del cliente de Amazon EFS en otras distribuciones Linux](#)
- [Instalación del cliente de Amazon EFS en instancias de Mac de EC2 que ejecuten macOS Big Sur, macOS Monterey o macOS Ventura](#)

Instalación del cliente Amazon EFS en instancias Linux de Amazon EC2

El amazon-efs-utils paquete para la instalación en las instancias Linux de Amazon EC2 desde las siguientes ubicaciones:

- Los repositorios de paquetes de imágenes de máquina de Amazon (AMI) para Amazon Linux. Las siguientes instrucciones sirven para instalar el amazon-efs-utils paquete desde los repositorios de paquetes de la AMI.
- El repositorio AWS [efs-utils](#) GitHub . Para obtener más información sobre cómo instalar el amazon-efs-utils paquete desde GitHub, consulte. [Instalación del cliente de Amazon EFS en otras distribuciones Linux](#)

Note

- Si lo está utilizando AWS Direct Connect, encontrará las instrucciones de instalación en [Tutorial: Crear y montar un sistema de archivos en las instalaciones con AWS Direct Connect y una VPN](#).
- La AMI de Amazon Linux (AL1) alcanzó su valor end-of-life el 31 de diciembre de 2023 y no es compatible con los `amazon-efs-utils` paquetes publicados en abril de 2024 y versiones posteriores (versión 2.0 y posteriores). Le recomendamos que actualice las aplicaciones a Amazon Linux 2023 (AL2023), que incluye soporte a largo plazo hasta 2028.

Para instalar el `amazon-efs-utils` paquete desde el repositorio de paquetes de la AMI en las instancias Linux de Amazon EC2

1. Asegúrese de haber creado una instancia EC2 de AL2023, Amazon Linux 2 (AL2) o Amazon Linux (AL1). Para obtener información sobre cómo hacerlo, consulte el [paso 1: lanzar una instancia](#).
2. Obtenga acceso al terminal de la instancia a través de Secure Shell (SSH) e inicie sesión con el nombre de usuario adecuado. Para obtener más información sobre cómo hacerlo, consulta [Conéctate a tu instancia de Linux desde Linux o macOS mediante SSH](#).
3. Ejecute el comando siguiente, para instalar el paquete `amazon-efs-utils`.

```
sudo yum install -y amazon-efs-utils
```

Instalación del cliente de Amazon EFS en otras distribuciones Linux

Si no desea obtener el `amazon-efs-utils` paquete de los repositorios de paquetes AMI de Amazon Linux, también está disponible en GitHub.

Después de clonar el paquete, puede crear e instalar `amazon-efs-utils` utilizando uno de los métodos que se indican a continuación, en función del tipo de paquete compatible con su distribución Linux:

- RPM: este tipo de paquete es compatible con Amazon Linux 2023 (AL2023), Amazon Linux 2 (AL2), Amazon Linux (AL1), Red Hat Linux, CentOS y similares.

- DEB : este tipo de paquete es compatible con Ubuntu, Debian y similares.

Para obtener instrucciones sobre cómo instalar el `amazon-efs-utils` paquete en otras distribuciones de Linux, consulte [Sobre otras distribuciones de Linux en el archivo README de Github](#). `amazon-efs-utils`

Instalación del cliente de Amazon EFS en instancias de Mac de EC2 que ejecuten macOS Big Sur, macOS Monterey o macOS Ventura

El paquete `amazon-efs-utils` está disponible para su instalación en instancias de Mac de EC2 que ejecuten macOS Big Sur, macOS Monterey o macOS Ventura.

Para obtener instrucciones sobre cómo instalar el `amazon-efs-utils` paquete en instancias de Mac, consulta [En la distribución macOS Big Sur, macOS Monterey, macOS Sonoma y macOS Ventura](#) en el `amazon-efs-utils` archivo README de Github.

Siguientes pasos

Tras la instalación de `amazon-efs-utils` en la instancia de EC2, continúe con los siguientes pasos para montar el sistema de archivos:

- [Instálelo](#) de `botocore` forma que pueda utilizar Amazon CloudWatch para supervisar el estado de montaje de su sistema de archivos.
- [Actualice a la última versión de `stunnel`](#) para habilitar el cifrado de los datos en tránsito.
- [Monte el sistema de archivos](#) con el ayudante de montaje de EFS.

Instalación y actualización **botocore**

El cliente Amazon EFS se utiliza `botocore` para interactuar con otros AWS servicios. Es obligatorio si desea supervisar los intentos de montaje correctos o fallidos de sus sistemas de archivos Amazon EFS en CloudWatch Logs. Para obtener más información, consulte [Supervisión del estado exitoso o fallido del intento de montaje](#).

Para obtener instrucciones sobre la instalación y la actualización `botocore`, consulte [Instalación `botocore`](#) en el `amazon-efs-utils` archivo README de Github.

Actualización de **stunnel**

El cifrado de datos en tránsito con el ayudante de montaje de Amazon EFS requiere OpenSSL versión 1.0.2 o posterior, y una versión de `stunnel` que admita OCSP y la comprobación del nombre de host del certificado. El ayudante de montaje de Amazon EFS utiliza el programa `stunnel` para la funcionalidad de TLS. Observe que algunas versiones de Linux no incluyen una versión de `stunnel` que admita estas características de TLS de forma predeterminada. Cuando se utiliza una de esas distribuciones de Linux, montar un sistema de archivos de Amazon EFS mediante TLS da error.

Después de instalar el ayudante de montaje de Amazon EFS, puede actualizar la versión del sistema de `stunnel` con las siguientes instrucciones.

Para actualizar **stunnel** en Amazon Linux, Amazon Linux 2 y otras distribuciones de Linux compatibles (excepto [SLES 12](#))

1. En un navegador web, vaya a la página de descargas de `stunnel` <https://stunnel.org/downloads.html>.
2. Localice la última versión de `stunnel` disponible en formato `tar.gz`. Anote el nombre del archivo, ya que lo necesitará en los pasos siguientes.
3. Abra un terminal en el cliente de Linux y ejecute los siguientes comandos en el orden que se muestran.
 - a. Para RPM:

```
sudo yum install -y gcc openssl-devel tcp_wrappers-devel
```

Para DEB:

```
sudo apt-get install build-essential libwrap0-dev libssl-dev
```

- b. Sustituya *latest-stunnel-version* por el nombre del archivo que anotó en el paso 2 anterior.

```
sudo curl -o latest-stunnel-version.tar.gz https://www.stunnel.org/downloads/latest-stunnel-version.tar.gz
```

- c.

```
sudo tar xvfz latest-stunnel-version.tar.gz
```

d. `cd latest-stunnel-version/`

e. `sudo ./configure`

f. `sudo make`

g. El paquete actual de `stunnel` está instalado en `bin/stunnel`. Por tanto, para que la nueva versión se pueda instalar, elimine ese directorio con el siguiente comando.

```
sudo rm /bin/stunnel
```

h. Instale la versión más reciente:

```
sudo make install
```

i. Cree un enlace simbólico

```
sudo ln -s /usr/local/bin/stunnel /bin/stunnel
```

Para actualizar stunnel en macOS

- Abra un terminal en su instancia Mac de EC2 y ejecute el siguiente comando para actualizar a la versión más reciente de `stunnel`.

```
brew upgrade stunnel
```

Actualización de stunnel para SLES 12

- Ejecute los siguientes comandos y siga las instrucciones del administrador de paquetes `zypper` para actualizar `stunnel` en tu instancia de computación que ejecuta SLES12.

```
sudo zypper addrepo https://download.opensuse.org/repositories/security:Stunnel/  
SLE_12_SP5/security:Stunnel.repo  
sudo zypper refresh  
sudo zypper install -y stunnel
```

Una vez instalada una versión de stunnel con las características necesarias, puede montar el sistema de archivos usando TLS con la configuración recomendada de Amazon EFS.

Deshabilitar la comprobación del nombre de host del certificado

Si no puede instalar las dependencias requeridas, tiene la opción de deshabilitar la comprobación del nombre de host del certificado en la configuración del ayudante de montaje de Amazon EFS. No es recomendable que desactive esta característica en entornos de producción. Para deshabilitar la comprobación del nombre de host del certificado, haga lo siguiente:

1. Con el editor de textos que prefiera, abra el archivo `/etc/amazon/efs/efs-utils.conf`.
2. Establezca el valor `stunnel_check_cert_hostname` en falso.
3. Guarde los cambios y cierre el archivo.

Para obtener más información sobre el uso de cifrado con datos en tránsito, consulte [Montaje de sistemas de archivos de EFS](#).

Habilitación del protocolo OCSP (Online Certificate Status Protocol)

Para maximizar la disponibilidad del sistema de archivos en caso de no poder conectarse a la entidad de certificación (CA) desde su VPC, el protocolo OCSP (Online Certificate Status Protocol) no está habilitado de forma predeterminada al elegir el cifrado de los datos en tránsito. Amazon EFS utiliza una [entidad de certificación de Amazon](#) para emitir y firmar los certificados TLS. Dicha entidad indica al cliente que utilice OCSP para comprobar los certificados revocados. Debe ser posible el acceso al punto de enlace OCSP a través de Internet desde su Virtual Private Cloud para comprobar el estado de un certificado. En este servicio, EFS monitoriza de forma continua el estado de los certificados y emite otros nuevos para reemplazar los certificados revocados que detecte.

Con el fin de ofrecer la mayor seguridad posible, puede habilitar OCSP para que los clientes de Linux puedan comprobar los certificados revocados. OCSP protege contra el uso malicioso de certificados revocados, lo que es poco probable que ocurra dentro de su VPC. En el caso de que un certificado TLS de EFS se revoque, Amazon publicará un boletín de seguridad y lanzará una nueva versión del ayudante de montaje de EFS que rechace el certificado revocado.

Para habilitar OCSP en el cliente de Linux para todas las conexiones TLS futuras en EFS

1. Abra un terminal en su cliente de Linux.
2. Con el editor de textos que prefiera, abra el archivo `/etc/amazon/efs/efs-utils.conf`.

3. Establezca el valor `stunnel_check_cert_validity` en `true`.
4. Guarde los cambios y cierre el archivo.

Para habilitar OCSP como parte del comando **mount**

- Utilice el siguiente comando de montaje para habilitar OCSP al montar el sistema de archivos.

```
$ sudo mount -t efs -o tls,ocsp fs-12345678:/ /mnt/efs
```

Montaje de sistemas de archivos de EFS

En las siguientes secciones, puede obtener información acerca de cómo montar su sistema de archivos de Amazon EFS mediante el ayudante de montaje de Amazon EFS. Además, aprenderá a utilizar el archivo `fstab` para volver a montar automáticamente el sistema de archivos después de los reinicios del sistema. Con el asistente de montaje de EFS, dispone de las siguientes opciones para montar su sistema de archivos de Amazon EFS:

- Montaje en instancias de EC2 compatibles
- Montaje con autorización de IAM
- Montaje con puntos de acceso de Amazon EFS
- Montaje con un cliente Linux en las instalaciones
- Montaje automático de sistemas de archivos EFS cuando se reinicia una instancia de EC2
- Montaje de un sistema de archivos al crear una nueva instancia de EC2

Note

Amazon EFS no admite el montaje desde instancias de Windows de Amazon EC2.

El asistente de montaje de EFS forma parte del paquete `amazon-efs-utils`. El paquete `amazon-efs-utils` es una colección de herramientas de Amazon EFS de código abierto. Para obtener más información, consulte [Instalación manual del cliente de Amazon EFS](#).

Antes de que estuviese disponible el ayudante de montaje de Amazon EFS, recomendábamos montar los sistemas de archivos de Amazon EFS mediante el cliente NFS de Linux estándar. Para obtener más información, consulte [Uso del Network File System para montar sistemas de archivos EFS](#).

Temas

- [Montaje del sistema de archivos de EFS mediante el ayudante de montaje de EFS](#)
- [Uso del Network File System para montar sistemas de archivos EFS](#)
- [Consideraciones de montaje adicionales](#)
- [Solución de problemas montaje](#)

Montaje del sistema de archivos de EFS mediante el ayudante de montaje de EFS.

El asistente de montaje de EFS le ayuda a montar los sistemas de archivos de EFS en las instancias de Linux y Mac de EC2 que ejecutan las distribuciones compatibles que se enumeran en [Acerca del cliente Amazon EFS](#).

El ayudante de montaje de Amazon EFS simplifica el montaje de los sistemas de archivos. Incluye las opciones de montaje de Amazon EFS recomendadas de forma predeterminada. Además, el ayudante de montaje tiene el registro integrado con fines de solución de problemas. Si tiene algún problema con su sistema de archivos Amazon EFS, puede compartir estos registros con AWS Support. Para obtener más información sobre cómo desmontar el sistema de archivos, consulte [Montaje de sistemas de archivos de EFS](#).

Note

Amazon EFS no admite el montaje desde instancias de Windows de Amazon EC2.

Temas

- [Funcionamiento](#)
- [Obtención de registros de soporte](#)
- [Requisitos previos para usar el asistente de montaje de EFS](#)
- [Montaje en instancias de Linux de Amazon EC2 mediante el asistente de montaje de EFS](#)
- [Montaje en instancias de Mac de Amazon EC2 mediante el asistente de montaje de EFS](#)
- [Montaje de sistemas de archivos Amazon EFS desde un sitio diferente Región de AWS](#)
- [Montaje de sistemas de archivos One Zone](#)
- [Montaje con autorización de IAM](#)
- [Montaje con puntos de acceso de EFS](#)
- [Montaje con clientes Linux locales mediante el asistente de montaje EFS y la VPN AWS Direct Connect](#)
- [Cómo montar su sistema de archivos de Amazon EFS automáticamente](#)
- [Montaje de EFS en varias instancias de EC2 mediante AWS Systems Manager](#)

- [Montaje de sistemas de archivos EFS desde otro Cuenta de AWS o desde una VPC](#)

Funcionamiento

El ayudante de montaje define un nuevo tipo de sistema de archivos de red, llamado `efs`, que es totalmente compatible con el comando `mount` estándar de Linux. El ayudante de montaje también permite montar un sistema de archivos de Amazon EFS automáticamente en el momento del arranque de la instancia utilizando entradas en el archivo de configuración `/etc/fstab` en instancias de Linux de EC2.

Warning

Use la opción `_netdev`, empleada para identificar los sistemas de archivos de red, cuando monte su sistema de archivos automáticamente. Si falta `_netdev`, la instancia EC2 puede dejar de responder. Este resultado se debe a que los sistemas de archivos de red se deben inicializar después de que la instancia de procesamiento inicia sus redes. Para obtener más información, consulte [Se produce un error de montaje automático y la instancia no responde](#).

Puede montar un sistema de archivos especificando una de las siguientes propiedades:

- Nombre de DNS del sistema de archivos: si utiliza el nombre de DNS del sistema de archivos y el asistente de montaje no puede resolverlo, por ejemplo, cuando monta un sistema de archivos en una VPC diferente, volverá a utilizar la dirección IP de destino del montaje. Para obtener más información, consulte [Montaje de sistemas de archivos EFS desde otro Cuenta de AWS o desde una VPC](#).
- ID del sistema de archivos: si utiliza el ID del sistema de archivos, el asistente de montaje lo resuelve en la dirección IP local de la interfaz de red elástica (ENI) de destino del montaje sin llamar a recursos externos.
- Dirección IP de destino de montaje: puede utilizar la dirección IP de uno de los destinos de montaje del sistema de archivos.

Puede encontrar el valor de todas estas propiedades en la consola de Amazon EFS. El nombre de DNS del sistema de archivos se encuentra en la pantalla de adjuntar.

Cuando el cifrado de datos en tránsito se declara como opción de montaje para el sistema de archivos de Amazon EFS, el ayudante de montaje inicializa un proceso de cliente `stunnel` y un

proceso de supervisor llamado `amazon-efs-mount-watchdog`. El proceso `amazon-efs-mount-watchdog` supervisa el estado de los montajes de TLS y se inicia automáticamente la primera vez que se monta un sistema de archivos de EFS sobre TLS. Si su cliente se ejecuta en Linux, este proceso lo gestiona `upstart` o `systemd` depende de su distribución de Linux. Para los clientes que se ejecutan en un macOS compatible, lo administra `launchd`.

`Stunnel` es una retransmisión de red multipropósito de código abierto. El proceso de `stunnel` cliente escucha en un puerto local el tráfico entrante y el ayudante de montaje de cliente NFS redirige el tráfico a este puerto local.

El ayudante de montaje usa TLS versión 1.2 para comunicarse con su sistema de archivos. El uso de TLS requiere certificados y estos certificados están firmados por una autoridad de certificación de confianza de Amazon. Para obtener más información acerca de cómo funciona el cifrado, consulte [Cifrado de datos en Amazon EFS](#).

Opciones de montaje utilizadas por el cliente de Amazon EFS

El cliente del ayudante de montaje de Amazon EFS utiliza las siguientes opciones de montaje optimizadas para Amazon EFS:

- `nfsvers=4.1`: se utiliza cuando se monta en instancias de EC2 de Linux
 - `nfsvers=4.0`: se utiliza cuando se monta en instancias de EC2 de Mac compatibles con macOS Big Sur, Monterey y Ventura
- `rsize=1048576`: establece el número máximo de bytes de datos que el cliente NFS puede recibir para cada solicitud de red READ hasta 1048576, el más grande disponible, para evitar un rendimiento reducido.
- `wsize=1048576`: establece el número máximo de bytes de datos que el cliente NFS puede recibir para cada solicitud de red WRITE hasta 1048576, el más grande disponible, para evitar un rendimiento reducido.
- `hard`: establece el comportamiento de recuperación del cliente NFS después de que se agote el tiempo de espera de una solicitud NFS, de modo que las solicitudes de NFS se vuelven a intentar indefinidamente hasta que el servidor responda, para garantizar la integridad de los datos.
- `timeo=600`: establece el valor de tiempo de espera que utiliza el cliente NFS para esperar una respuesta antes de volver a intentar una solicitud NFS en 600 décimas de segundo (60 segundos) para evitar un rendimiento reducido.
- `retrans=2`: establece en 2 el número de veces que el cliente de NFS reintenta una solicitud antes de intentar una acción de recuperación adicional.

- `noresvport`: indica al cliente NFS que utilice un nuevo puerto de origen de protocolo de control de transmisión (TCP) sin privilegios cuando se restablece la conexión a la red. La opción `noresvport` ayuda a garantizar que el sistema de archivos EFS tenga una disponibilidad ininterrumpida tras un evento de reconexión o recuperación de la red.
- `mountport=2049`: se utiliza solo cuando se monta en instancias de EC2 de Mac compatibles con macOS Big Sur, Monterey y Ventura

Obtención de registros de soporte

El ayudante de montaje tiene registro integrado para el sistema de archivos de Amazon EFS. Puede compartir estos registros con AWS Support para solucionar problemas. Puede encontrar los registros almacenados en `/var/log/amazon/efs` en los clientes mediante el asistente de montaje de EFS. Estos registros son para el ayudante de montaje de EFS, el proceso de `stunnel` (desactivado de forma predeterminada) y para el proceso `amazon-efs-mount-watchdog` que monitoriza el proceso `stunnel`.

Note

El proceso `amazon-efs-mount-watchdog` garantiza que cada proceso de `stunnel` del montaje se está ejecutando y detiene el proceso de `stunnel` cuando el sistema de archivos de Amazon EFS está desmontado. Si por alguna razón un proceso de `stunnel` termina de forma inesperada, el proceso del `watchdog` lo reinicia.

Puede cambiar la configuración de los registros en `/etc/amazon/efs/efs-utils.conf`. Para que los cambios en el registro surtan efecto, debe desmontar y volver a montar el sistema de archivos mediante el asistente de montaje de EFS. La capacidad de los registros del ayudante de montaje y del `watchdog` se limita a 20 MiB. Los registros para el proceso de `stunnel` están deshabilitados de forma predeterminada.

Important

Puede habilitar el registro para los registros del proceso de `stunnel`. Sin embargo, habilitar los registros de `stunnel` puede hacer un uso nada despreciable de espacio en el sistema de archivos.

Requisitos previos para usar el asistente de montaje de EFS

Puede montar un sistema de archivos de Amazon EFS en una instancia EC2 de Amazon con el ayudante de montaje de Amazon EFS. Para utilizar el ayudante de montaje, necesita lo siguiente:

- ID del sistema de archivos del sistema que se va a montar: el asistente de montaje de EFS resuelve el ID del sistema de archivos en la dirección IP local de la interfaz de red elástica (ENI) de destino del montaje sin llamar a recursos externos.
- Un destino de montaje de Amazon EFS: debe crear destinos de montaje en su nube privada virtual (VPC). Si crea su sistema de archivos en la consola con la configuración recomendada por el servicio, se crea un destino de montaje en cada zona de disponibilidad en la Región de AWS que se encuentre el sistema de archivos. Para obtener instrucciones para crear un destinos de montaje, consulte [Administrar destinos de montaje](#).


Note

Se recomienda esperar 60 segundos después de que el estado del ciclo de vida del destino de montaje recién creado sea disponible antes de montar el sistema de archivos mediante DNS. Esta espera permite que los registros DNS se propaguen por completo en el Región de AWS lugar donde reside el sistema de archivos.

Si utiliza el destino de montaje en una zona de disponibilidad distinta de la de su instancia EC2, incurre en cargos de EC2 estándar para datos enviados entre zonas de disponibilidad. También podría ver latencias más elevadas para las operaciones del sistema de archivos.

- Para montar sistemas de archivos One Zone desde una zona de disponibilidad diferente:
 - El nombre de la zona de disponibilidad del sistema de archivos: si va a montar un sistema de archivos One Zone de EFS que se encuentre en una zona de disponibilidad diferente a la de la instancia de EC2.
 - Nombre de DNS de destino de montaje: también puede especificar el nombre de DNS del destino de montaje en lugar de la zona de disponibilidad.
- Una instancia de Amazon EC2 que ejecute una de las distribuciones Linux o macOS compatibles: las distribuciones compatibles para montar el sistema de archivos con el asistente de montaje son las siguientes:
 - Amazon Linux 2
 - Amazon Linux 2023

- Amazon Linux 2017.09 y versiones posteriores
- macOS Big Sur
- Red Hat Enterprise Linux (y sus derivados como CentOS) versión 7 y posteriores
- Ubuntu 16.04 LTS y posterior

 Note

Las instancias de Mac de EC2 que ejecutan macOS Big Sur solo son compatibles con NFS v4.0.

- El asistente de montaje de Amazon EFS está instalado en la instancia de EC2: el asistente de montaje es una herramienta del paquete de utilidades `amazon-efs-utils`. Para obtener información acerca de cómo instalar `amazon-efs-utils`, consulte [Instalación automatizada del cliente EFS](#) e [Instalación manual de amazon-efs-utils](#).
- La instancia de EC2 es una VPC: La instancia EC2 de conexión debe estar en una nube virtual privada (VPC) en función del servicio de Amazon VPC. También debe configurarse para usar el servidor DNS proporcionado por AWS. Para obtener información sobre el servidor DNS de Amazon, consulte [Conjuntos de opciones de DHCP](#) en la Guía del usuario de Amazon VPC.
- VPC tiene nombres de host DNS habilitados: La VPC de la instancia EC2 de conexión debe tener los nombres de host DNS habilitados. Para obtener más información, consulte [Visualización de nombres de host DNS de la instancia de EC2](#) en la Guía del usuario de VPC de Amazon.
- Para instancias EC2 y sistemas de archivos distintos Regiones de AWS: si la instancia EC2 y el sistema de archivos que va a montar están ubicados en un Regiones de AWS lugar diferente, tendrá que editar la `region` propiedad del archivo `efs-utils.conf`. Para obtener más información, consulte [Montaje de sistemas de archivos Amazon EFS desde un sitio diferente Región de AWS](#).

Montaje en instancias de Linux de Amazon EC2 mediante el asistente de montaje de EFS

Este proceso requiere los siguientes elementos:

- Debe tener instalado el paquete `amazon-efs-utils` en la instancia de EC2. Para obtener más información, consulte [Instalación manual del cliente de Amazon EFS](#).

- Debe haber creado destinos de montaje para el sistema de archivos. Para obtener más información, consulte [Administrar destinos de montaje](#).

Para montar el sistema de archivos de Amazon EFS en una instancia EC2 de Linux con el ayudante de montaje de EFS.

1. Abra una ventana del terminal de la instancia a través de Secure Shell (SSH) e inicie sesión con el nombre de usuario adecuado. Para obtener más información, consulte [Conéctese a la instancia de Linux desde Linux o macOS mediante SSH](#).
2. Cree un directorio `efs` que utilizará como punto de montaje del sistema de archivos mediante el siguiente comando:

```
sudo mkdir efs
```

3. Ejecute uno de los siguientes comandos para montar el sistema de archivos.

Note

Si la instancia de EC2 y el sistema de archivos que va a montar se encuentran en Región de AWS diferentes, consulte [Montaje de sistemas de archivos Amazon EFS desde un sitio diferente Región de AWS](#) para editar la propiedad `region` del archivo `efs-utils.conf`.

- Para montar utilizando el id del sistema de archivos

```
sudo mount -t efs file-system-id efs-mount-point/
```

Utilice el ID del sistema de archivos que va a montar *file-system-id* y `efs` en lugar de *efs-mount-point*.

```
sudo mount -t efs fs-abcd123456789ef0 efs/
```

También, si desea utilizar el cifrado de datos en tránsito, puede montar el sistema de archivos con el siguiente comando.

```
sudo mount -t efs -o tls fs-abcd123456789ef0:/ efs/
```

- Para realizar el montaje utilizando el nombre de DNS del sistema de archivos:

```
sudo mount -t efs -o tls file-system-dns-name efs-mount-point/
```

```
sudo mount -t efs -o tls fs-abcd123456789ef0.efs.us-east-2.amazonaws.com efs/
```

- Para realizar el montaje mediante la dirección IP de destino del montaje:

```
sudo mount -t efs -o tls,mounttargetip=mount-target-ip file-system-id efs-mount-point/
```

```
sudo mount -t efs -o tls,mounttargetip=192.0.2.0 fs-abcd123456789ef0 efs/
```

Puede ver y copiar los comandos exactos para montar el sistema de archivos en el cuadro de diálogo Adjuntar.

- a. En la consola de Amazon EFS, elija el sistema de archivos que desee montar para que aparezca su página de detalles.
- b. Para ver los comandos de montaje que se van a utilizar en este sistema de archivos, seleccione Adjuntar en la esquina superior derecha.

La pantalla Adjuntar muestra los comandos exactos que se utilizarán para montar el sistema de archivos de las siguientes maneras:

- (Montaje mediante DNS) Uso del nombre de DNS del sistema de archivos con el asistente de montaje de EFS o un cliente de NFS.
- (Montaje mediante IP) Uso de la dirección IP de destino del montaje en la zona de disponibilidad seleccionada con un cliente NFS.

Montaje en instancias de Mac de Amazon EC2 mediante el asistente de montaje de EFS

Este proceso requiere los siguientes elementos:

- Debe tener instalado el paquete `amazon-efs-utils` en la instancia de Mac de EC2. Para obtener más información, consulte [Instalación del cliente de Amazon EFS en instancias de Mac de EC2 que ejecuten macOS Big Sur, macOS Monterey o macOS Ventura](#).
- Debe haber creado destinos de montaje para el sistema de archivos. Puede crear destinos de montaje al crear el sistema de archivos y añadirlos a los sistemas de archivos existentes. Para obtener más información, consulte [Administrar destinos de montaje](#).
- Está montando el sistema de archivos en una instancia Mac de EC2 que ejecuta macOS Big Sur, Monterey o Ventura. No se admiten otras versiones de macOS.

Note

Solo se admiten instancias de EC2 de Mac que ejecutan con macOS Big Sur, Monterey y Ventura. El uso de otras versiones de macOS con Amazon EFS no es compatible.

Cómo montar el sistema de archivos de Amazon EFS mediante el asistente de montaje de EFS en instancias Mac EC2 que ejecuten macOS Big Sur, Monterey o Ventura

1. Abra una ventana del terminal de la instancia Mac de EC2 a través de Secure Shell (SSH) e inicie sesión con el nombre de usuario adecuado. Para obtener más información, consulte [Conectarse a su instancia mediante SSH](#) para instancias de Mac, en la Guía del usuario de Amazon EC2.
2. Cree un directorio que utilizará como punto de montaje del sistema de archivos mediante el siguiente comando:

```
sudo mkdir efs
```

3. Ejecute el siguiente comando para montar el sistema de archivos.

Note

De forma predeterminada, el asistente de montaje de EFS utiliza el cifrado en tránsito cuando se monta en instancias de Mac de EC2, independientemente de que utilice o no la opción `tls` del comando `mount`.

```
sudo mount -t efs file-system-id efs-mount-point/
```

```
sudo mount -t efs fs-abcd123456789ef0 efs/
```

También puede utilizar la opción `tls` al montar.

```
sudo mount -t efs -o tls fs-abcd123456789ef0:/ efs
```

Para montar un sistema de archivos en una instancia de Mac de EC2 sin utilizar el cifrado en tránsito, utilice la opción `notls`, tal como se muestra en el siguiente comando.

```
sudo mount -t efs -o notls file-system-id efs-mount-point/
```

Puede ver y copiar los comandos exactos para montar el sistema de archivos en el cuadro de diálogo Adjuntar, descrito a continuación.

- a. En la consola de Amazon EFS, elija el sistema de archivos que desee montar para que aparezca su página de detalles.
- b. Para ver los comandos de montaje que se van a utilizar en este sistema de archivos, seleccione Adjuntar en la esquina superior derecha.

La pantalla Adjuntar muestra los comandos exactos que se utilizarán para montar el sistema de archivos de las siguientes maneras:

- (Montaje mediante DNS) Uso del nombre de DNS del sistema de archivos con el asistente de montaje de EFS o un cliente de NFS.
- (Montaje mediante IP) Uso de la dirección IP de destino del montaje en la zona de disponibilidad seleccionada con un cliente NFS.

Montaje de sistemas de archivos Amazon EFS desde un sitio diferente Región de AWS

Si va a montar el sistema de archivos EFS desde una instancia de Amazon EC2 que se encuentra en un sistema de archivos Región de AWS diferente al sistema de archivos, tendrá que editar el valor de la `region` propiedad del `efs-utils.conf` archivo.

Cómo editar la propiedad de la región en `efs-utils.conf`

1. Obtenga acceso al terminal de la instancia de EC2 a través de Secure Shell (SSH) e inicie sesión con el nombre de usuario adecuado. Para obtener más información sobre cómo hacerlo, consulte [Conexión a su instancia de Linux mediante SSH](#) en la Guía del usuario de Amazon EC2.
2. Localice el archivo `efs-utils.conf` y ábralo con el editor de texto que desee.
3. Localice la siguiente línea:

```
#region = us-east-1
```

- a. Quite el comentario de la línea.
 - b. Si el sistema de archivos no está ubicado en la región `us-east-1`, sustituya `us-east-1` por el identificador de la región en la que se encuentra el sistema de archivos.
 - c. Guarde los cambios.
4. Añada una entrada de host para el montaje entre regiones. Para obtener más información acerca de cómo hacerlo, consulte [Paso 3: Agregar una entrada de host para el destino de montaje](#).
 5. Monte el sistema de archivos mediante el asistente de montaje de EFS para instancias de [Linux](#) o [Mac](#).

Montaje de sistemas de archivos One Zone

Los sistemas de archivos One Zone de Amazon EFS solo admiten un único destino de montaje en la misma zona de disponibilidad que el sistema de archivos. No puede añadir objetivos de montaje adicionales. En esta sección se describen los aspectos que se deben tener en cuenta al montar sistemas de archivos One Zone.

Puede evitar los cargos por transferencia de datos entre zonas de disponibilidad y lograr un mejor rendimiento accediendo a un sistema de archivos de EFS mediante una instancia informática de Amazon EC2 ubicada en la misma zona de disponibilidad que la del destino de montaje del sistema de archivos.

Los procedimientos de esta sección requieren lo siguiente:

- Debe tener instalado el `amazon-efs-utils` package en la instancia de EC2. Para obtener más información, consulte [Instalación manual del cliente de Amazon EFS](#).

- Debe haber creado un destino de montaje para el sistema de archivos. Para obtener más información, consulte [Administrar destinos de montaje](#).

Montar sistemas de archivos One Zone en EC2 en una zona de disponibilidad diferente

Si va a montar un sistema de archivos One Zone en una instancia de EC2 que se encuentra en una zona de disponibilidad diferente, debe especificar el nombre de la zona de disponibilidad del sistema de archivos o el nombre de DNS del destino de montaje del sistema de archivos en el comando de montaje del asistente de montaje.

Cree un directorio llamado `efs` que utilizará como punto de montaje del sistema de archivos mediante el siguiente comando:

```
sudo mkdir efs
```

Utilice el comando siguiente para montar el sistema de archivos con el ayudante de montaje de EFS. El comando especifica el nombre de la zona de disponibilidad del sistema de archivos.

```
sudo mount -t efs -o az=availability-zone-name,tls file-system-id mount-point/
```

Este es el comando con valores de muestra:

```
sudo mount -t efs -o az=us-east-1a,tls fs-abcd1234567890ef efs/
```

El siguiente comando monta el sistema de archivos y especifica el nombre de DNS del destino de montaje del sistema de archivos.

```
sudo mount -t efs -o tls mount-target-dns-name mount-point/
```

Este es el comando con un ejemplo de nombre de DNS de destino de montaje.

```
sudo mount -t efs -o tls us-east-1a.fs-abcd1234567890ef9.efs.us-east-1.amazonaws.com  
efs/
```

Montaje automático de sistemas de archivos One Zone en una zona de disponibilidad diferente con el asistente de montaje de EFS

Si utiliza `/etc/fstab` para montar un sistema de archivos One Zone de EFS en una instancia de EC2 que se encuentra en una zona de disponibilidad diferente, debe especificar el nombre de la zona de disponibilidad del sistema de archivos o el nombre de DNS del destino de montaje del sistema de archivos en la entrada `/etc/fstab`.

```
availability-zone-name.file-system-id.efs.aws-region.amazonaws.com:/ efs-mount-point  
efs defaults,_netdev,noresvport,tls 0 0
```

```
us-east-1a.fs-abc123def456a7890.efs.us-east-1.amazonaws.com:/ efs-one-zone efs  
defaults,_netdev,noresvport,tls 0 0
```

Montaje automático de sistemas de archivos One Zone con NFS

Si utiliza `/etc/fstab` para montar un sistema de archivos de EFS con almacenamiento One Zone en una instancia de EC2 que se encuentra en una zona de disponibilidad diferente, debe especificar el nombre de la zona de disponibilidad del sistema de archivos con el nombre de DNS del sistema de archivos en la entrada `/etc/fstab`.

```
availability-zone-name.file-system-id.efs.aws-region.amazonaws.com:/ efs-mount-point  
nfs4  
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0  
0
```

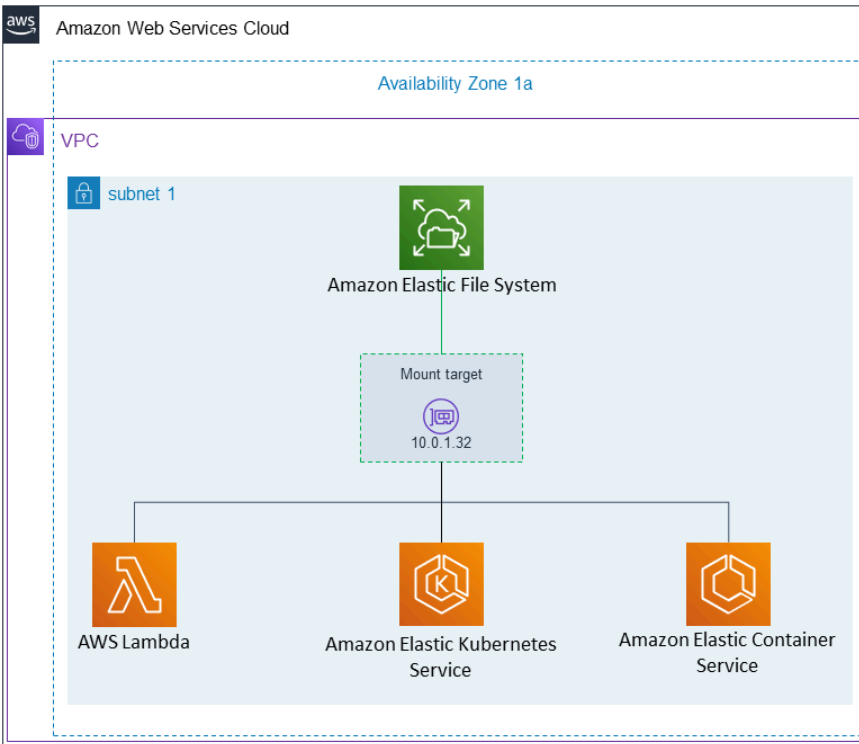
```
us-east-1a.fs-abc123def456a7890.efs.us-east-1.amazonaws.com:/ efs-one-zone nfs4  
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0  
0
```

Para obtener más información sobre cómo editar el archivo `/etc/fstab` y los valores utilizados en este comando, consulte [Uso de NFS para montar automáticamente sistemas de archivos de EFS](#).

Montar sistemas de archivos con el sistema de archivos One Zone en otras instancias AWS informáticas

Si utiliza un sistema de archivos de una zona con Amazon Elastic Container Service, Amazon Elastic Kubernetes Service AWS Lambda o bien, necesita configurar el servicio para que utilice la misma

zona de disponibilidad en la que se encuentra el sistema de archivos EFS, tal como se ilustra a continuación y se describe en las siguientes secciones.



Conexión desde de Amazon Elastic Container Service

Puede utilizar sistemas de archivos de Amazon EFS con Amazon ECS para compartir los datos del sistema de archivos a través de la flota de instancias de contenedor, de manera que sus tareas tengan acceso al mismo almacenamiento persistente, independientemente de la instancia en la que se encuentren. Para utilizar los sistemas de archivos One Zone de Amazon EFS con Amazon ECS, debe elegir solo las subredes que se encuentren en la misma zona de disponibilidad que su sistema de archivos al iniciar la tarea. Para obtener más información, consulte [Volúmenes de Amazon EFS](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Conexión desde de Amazon Elastic Kubernetes Service

Al montar un sistema de archivos One Zone desde Amazon EKS, puede utilizar el controlador [Container Storage Interface](#) (CSI) de Amazon EFS, que admite los puntos de acceso de Amazon EFS, para compartir un sistema de archivos entre varios pods de un clúster de Amazon EKS o de Kubernetes autogestionado. El controlador CSI de Amazon EFS está instalado en la pila Fargate. Si utiliza el controlador CSI de Amazon EFS con los sistemas de archivos One Zone de Amazon EFS,

puede utilizar la opción `nodeSelector` al lanzar el pod para asegurarse de que se programe en la misma zona de disponibilidad que su sistema de archivos.

Conectarse desde AWS Lambda

Puede usar Amazon EFS with AWS Lambda para compartir datos entre las invocaciones de funciones, leer archivos de datos de referencia de gran tamaño y escribir los resultados de las funciones en un almacén persistente y compartido. Lambda conecta de forma segura las instancias de función a los destinos de montaje de Amazon EFS que se encuentran en la misma zona de disponibilidad y subred. Cuando utilice Lambda con sistemas de archivos One Zone, configure la función para lanzar invocaciones únicamente en subredes que se encuentren en la misma zona de disponibilidad que su sistema de archivos.

Montaje con autorización de IAM

Para montar su sistema de archivos Amazon EFS en instancias de Linux mediante autorización AWS Identity and Access Management (IAM), utilice el asistente de montaje EFS. Para obtener más información sobre la autorización de IAM para clientes NFS, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#).

Debe crear un directorio que utilizará como punto de montaje del sistema de archivos en las siguientes secciones. Puede utilizar el siguiente comando para crear un directorio para el punto de montaje del disco `efs`:

```
sudo mkdir efs
```

A continuación, puede sustituir las instancias de `efs-mount-point` por `efs`.

Montaje con IAM mediante un perfil de instancia de EC2

Si va a montar con autorización de IAM en una instancia de Amazon EC2 con un perfil de instancia, utilice las opciones de montaje `tls` y `iam`, que se muestran a continuación.

```
$ sudo mount -t efs -o tls,iam file-system-id efs-mount-point/
```

Para montar automáticamente con autorización de IAM en una instancia de Amazon EC2 que tiene un perfil de instancia, agregue la siguiente línea al archivo `/etc/fstab` de la instancia de EC2.

```
file-system-id:/ efs-mount-point efs _netdev,tls,iam 0 0
```

Montaje con IAM mediante un perfil con nombre

Puede realizar el montaje con la autorización de IAM mediante las credenciales de IAM que se encuentran en el archivo de AWS CLI credenciales o en el archivo `~/.aws/credentials` de AWS CLI configuración. `~/.aws/config` Si no se especifica "awsprofile", se utiliza el perfil "predeterminado".

Para montar con autorización de IAM en una instancia de Linux mediante un archivo de credenciales, utilice las opciones de montaje `tls`, `awsprofile` y `iam` que se muestran a continuación.

```
$ sudo mount -t efs -o tls,iam,awsprofile=namedprofile file-system-id efs-mount-point/
```

Para montar automáticamente con autorización de IAM en una instancia de Linux mediante un archivo de credenciales, agregue la siguiente línea al archivo `/etc/fstab` en la instancia de EC2.

```
file-system-id:/ efs-mount-point efs _netdev,tls,iam,awsprofile=namedprofile 0 0
```

Montaje con puntos de acceso de EFS

Puede montar un sistema de archivos de EFS utilizando un punto de acceso con el ayudante de montaje de EFS.

Note

Debe configurar uno o más destinos de montaje para el sistema de archivos al montar un sistema de archivos mediante puntos de acceso de EFS.

Al montar un sistema de archivos mediante un punto de acceso, el comando `mount` incluye la opción de montaje `access-point-id` y `tls` además de las opciones normales de montaje. A continuación se muestra un ejemplo.

```
$ sudo mount -t efs -o tls,accesspoint=access-point-id file-system-id efs-mount-point
```

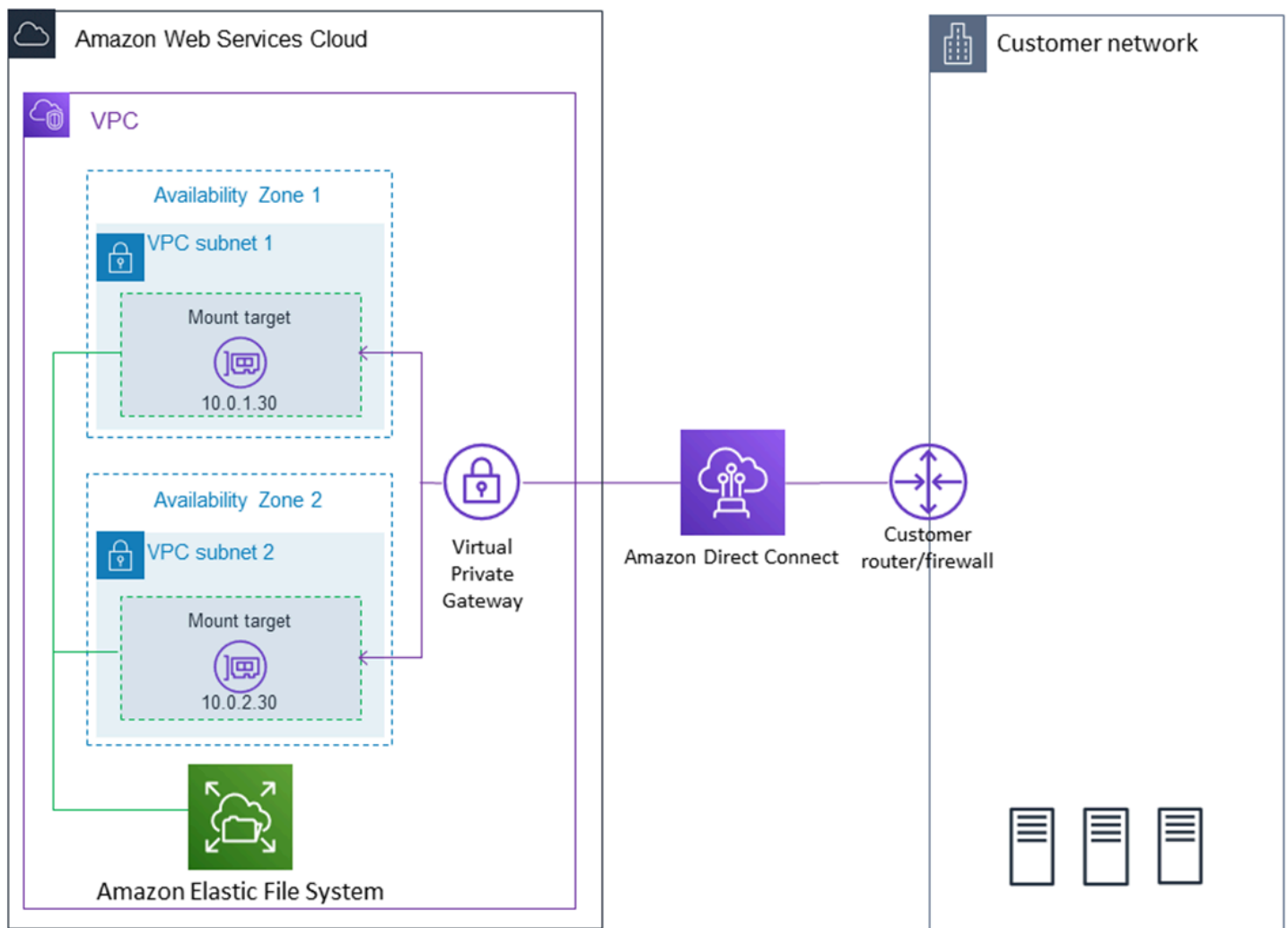
Para montar automáticamente un sistema de archivos utilizando un punto de acceso, añada la siguiente línea al archivo `/etc/fstab` en la instancia de EC2.

```
file-system-id efs-mount-point efs _netdev,tls,accesspoint=access-point-id 0 0
```

Para obtener más información acerca de los puntos de acceso de EFS, consulte [Trabajo con puntos de acceso de Amazon EFS](#).

Montaje con clientes Linux locales mediante el asistente de montaje EFS y la VPN AWS Direct Connect

Puede montar sus sistemas de archivos Amazon EFS en los servidores de sus centros de datos locales cuando esté conectado a su Amazon VPC mediante AWS Direct Connect una VPN. En el siguiente gráfico se muestra un diagrama esquemático de alto nivel de Servicios de AWS lo necesario para montar sistemas de archivos Amazon EFS desde instalaciones locales.



Para obtener más información sobre cómo utilizar `amazon-efs-utils` una VPN para montar sistemas de archivos Amazon EFS en clientes Linux locales, consulte [Tutorial: Crear y montar un sistema de archivos en las instalaciones con AWS Direct Connect y una VPN](#). AWS Direct Connect

Cómo montar su sistema de archivos de Amazon EFS automáticamente

Puede configurar una instancia de Amazon EC2 para que monte automáticamente un sistema de archivos de EFS cuando se reinicie mediante el asistente de montaje de EFS o NFS.

- Uso del ayudante de montaje de EFS:
 - Adjunte un sistema de archivos de EFS al crear una nueva instancia de Linux de EC2 con el asistente de inicialización de instancias de EC2.
 - Actualice el archivo `/etc/fstab` de EC2 con una entrada para el sistema de archivos de EFS.
- Uso de [NFS sin el asistente de montaje de EFS](#) para actualizar el archivo `/etc/fstab` de EC2, para admitir instancias de Linux y Mac de EC2.

Note

El asistente de montaje de EFS no admite el montaje automático en instancias de Mac de Amazon EC2 que ejecuten macOS Big Sur o Monterey. En su lugar, puede usar [NFS para configurar el archivo `/etc/fstab` en una instancia de Mac de EC2](#) para montar automáticamente un sistema de archivos de EFS.

Temas

- [Remontaje del sistema de archivos de EFS mediante el ayudante de montaje de EFS](#)
- [Uso de NFS para montar automáticamente sistemas de archivos de EFS](#)

Remontaje del sistema de archivos de EFS mediante el ayudante de montaje de EFS

Utilice el asistente de montaje de EFS para configurar `/etc/fstab` en las instancias de Linux de EC2 para volver a montar automáticamente los sistemas de archivos de EFS cuando la instancia se reinicie.


Temas

- [Adjunte un sistema de archivos de EFS al crear una instancia de EC2 para permitir el montaje automático al reiniciar](#)
- [Remontaje del sistema de archivos de EFS mediante `/etc/fstab` con el ayudante de montaje de EFS](#)

Adjunte un sistema de archivos de EFS al crear una instancia de EC2 para permitir el montaje automático al reiniciar


Este método utiliza el asistente de montaje de EFS para montar el sistema de archivos y actualizar el archivo `/etc/fstab` en la instancia de EC2. El ayudante de montaje forma parte del conjunto de herramientas [amazon-efs-utils](#).

Cuando crea una nueva instancia de Linux de Amazon EC2 mediante el asistente de inicialización de instancias de EC2, puede configurarla para montar el sistema de archivos de Amazon EFS automáticamente. La instancia EC2 monta el sistema de archivos de forma automática al iniciar la instancia por primera vez y también cada vez que se reinicia.

 Note

Los sistemas de archivos de Amazon EFS no admiten el montaje en instancias de Mac de Amazon EC2 que ejecuten macOS Big Sur o Monterey en el momento del lanzamiento de la instancia.

Antes de realizar este procedimiento, compruebe que ha creado su sistema de archivos de Amazon EFS. Para obtener más información, consulte [Cree rápidamente un sistema de archivos con la configuración recomendada \(consola\)](#) en el ejercicio de introducción de Amazon EFS.

 Note

No se puede usar Amazon EFS con instancias de Amazon EC2 basadas en Microsoft Windows.

Antes de poder lanzar y conectarse a una instancia de Amazon EC2, tiene que crear un par de claves, a menos que ya disponga de una. Siga los pasos de [Configuración para usar Amazon EC2](#) de la Guía del usuario de Amazon EC2 para crear un par de claves. Si ya tiene un par de claves, puede utilizarlo en este ejercicio.

Para configurar la instancia EC2 para montar un sistema de archivos EFS de forma automática en el momento del lanzamiento

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Elija Iniciar instancia.

3. En Step 1: Choose an Amazon Machine Image (AMI) (Paso 1: Elegir una Amazon Machine Image (AMI)), busque una AMI de Amazon Linux en la parte superior de la lista y elija Select (Seleccionar).
4. En el Step 2: Choose an Instance Type (Paso 2: Elegir un tipo de instancia), seleccione Next: Configure Instance Details (Siguiente: Configurar detalles de la instancia).
5. En el Step 3: Configure Instance Details (Paso 3: Configurar los detalles de la instancia), proporcione la siguiente información:
 - En Network (Red), elija la entrada de la misma VPC en la que se encuentra el sistema de archivos de EFS que va a montar.
 - En Subnet (Subred), elija una subred predeterminada en cualquier zona de disponibilidad.
 - En File systems (Sistemas de archivos), elija el sistema de archivos de EFS que desea montar. La ruta que se muestra junto al ID del sistema de archivos es el punto de montaje que utilizará la instancia EC2, que puede cambiar.
 - En Advanced details (Detalles avanzados), los datos de usuario se generan automáticamente e incluyen los comandos necesarios para montar los sistemas de archivos EFS especificados en File systems (Sistemas de archivos).
6. Elija Siguiente: Añadir almacenamiento.
7. Elija Next: Add Tags (Siguiente: Agregar etiquetas).
8. Asigne un nombre a la instancia y elija Next: Configure Security Group (Siguiente: Configurar grupo de seguridad).
9. En Step 6: Configure Security Group (Paso 6: Configurar grupo de seguridad), establezca Assign a security group (Asignar un grupo de seguridad) en Select an existing security group (Seleccionar un grupo de seguridad existente). Elija el grupo de seguridad predeterminado para asegurarse de que puede obtener acceso a su sistema de archivos de EFS.

No puede obtener acceso a la instancia EC2 mediante Secure Shell (SSH) con este grupo de seguridad. Para el acceso mediante SSH, puede editar más adelante la seguridad predeterminada y añadir una regla para permitir SSH o un nuevo grupo de seguridad que permita SSH. Puede utilizar la siguiente configuración:


- Tipo: SSH
- Protocolo: TCP
- Rango de puerto: 22
- Origen: cualquiera 0.0.0.0/0

10. Elija Revisar e iniciar.
11. Elija Iniciar.
12. Seleccione la casilla de verificación para el par de claves que ha creado y, a continuación, elija Launch Instances (Lanzar instancias).

La instancia EC2 ahora está configurada para montar el sistema de archivos de EFS cuando se lance y siempre que se reinicie.

Remontaje del sistema de archivos de EFS mediante **/etc/fstab** con el ayudante de montaje de EFS

El archivo `/etc/fstab` contiene información sobre los sistemas de archivos. El comando `mount -a`, que se ejecuta durante el arranque de la instancia, monta todos los sistemas de archivos enumerados en `/etc/fstab`. En este procedimiento, actualizará manualmente `/etc/fstab` en una instancia de Linux de EC2 para que la instancia utilice el asistente de montaje de EFS para volver a montar automáticamente un sistema de archivos de EFS cuando la instancia se reinicie.

 Note

Los sistemas de archivos de Amazon EFS no admiten el montaje automático con `/etc/fstab` con el asistente de montaje de EFS en instancias de Mac de Amazon EC2 que ejecutan macOS Big Sur o Monterey. En su lugar, puede usar [NFS con /etc/fstab](#) para montar automáticamente el sistema de archivos en instancias de Mac de EC2 que ejecuten macOS Big Sur y Monterey.

Este método utiliza el ayudante de montaje de EFS para montar el sistema de archivos. El ayudante de montaje forma parte del conjunto de herramientas `amazon-efs-utils`.

Las herramientas `amazon-efs-utils` están disponibles para su instalación en imágenes de Amazon Machine (AMI) de Amazon Linux y Amazon Linux 2. Para obtener más información acerca de `amazon-efs-utils`, consulte [Instalación de las herramientas de Amazon EFS](#). Si utiliza otra distribución de Linux, como Red Hat Enterprise Linux (RHEL), compile e instale `amazon-efs-utils` de forma manual. Para obtener más información, consulte [Instalación del cliente de Amazon EFS en otras distribuciones Linux](#).

Requisitos previos

Para poder implementar correctamente este procedimiento, es necesario cumplir los siguientes requisitos:

- Ya ha creado el sistema de archivos de Amazon EFS y desea que se vuelva a montar automáticamente. Para obtener más información, consulte [Cree rápidamente un sistema de archivos con la configuración recomendada \(consola\)](#).
- Ya ha creado la instancia de Linux de EC2 que desea configurar para volver a montar automáticamente un sistema de archivos de EFS.
- El asistente de montaje de EFS está instalado en la instancia de Linux de EC2. Para obtener más información, consulte [Instalación de las herramientas de Amazon EFS](#).

Para actualizar el archivo `/etc/fstab` en la instancia EC2

1. Conéctese a su instancia EC2:

- Para conectarse a la instancia desde un equipo que ejecute macOS o Linux, especifique el archivo `.pem` para su comando SSH. Para ello, use la opción `-i` y la ruta a su clave privada.
- Para conectarte a la instancia desde un ordenador con Windows, puedes usar PuTTY, MindTerm o bien. Para usar PuTTY, instálelo y convierta el archivo `.pem` en un archivo `.ppk`.

Para obtener más información, consulte los siguientes temas de la Guía del usuario de Amazon EC2:

- [Conéctate a tu instancia de Linux desde Windows con PuTTY](#)
- [Conéctate a tu instancia de Linux desde Linux o macOS mediante SSH](#)

2. Abra el archivo `/etc/fstab` en un editor.

3. Para montar automáticamente utilizando una autorización de IAM o un punto de acceso de EFS:

- Para montar automáticamente con autorización de IAM en una instancia de Amazon EC2 que tiene un perfil de instancia, agregue la siguiente línea al archivo `/etc/fstab`.

```
file-system-id:/ efs-mount-point efs _netdev,noresvport,tls,iam 0 0
```

- Para montar automáticamente con autorización de IAM en una instancia de Linux mediante un archivo de credenciales, agregue la siguiente línea al archivo `/etc/fstab`.

```
file-system-id:/ efs-mount-point efs
_netdev,noresvport,tls,iam,awsprofile=namedprofile 0 0
```

- Para montar automáticamente un sistema de archivos utilizando un punto de acceso de EFS, agregue la siguiente línea al archivo `/etc/fstab`.

```
file-system-id:/ efs-mount-point efs
_netdev,noresvport,tls,iam,accesspoint=access-point-id 0 0
```

Warning

Use la opción `_netdev`, empleada para identificar los sistemas de archivos de red, cuando monte su sistema de archivos automáticamente. Si falta `_netdev`, la instancia EC2 puede dejar de responder. Este resultado se debe a que los sistemas de archivos de red se deben inicializar después de que la instancia de procesamiento inicia sus redes. Para obtener más información, consulte [Se produce un error de montaje automático y la instancia no responde](#).

Para obtener más información, consulte [Montaje con autorización de IAM](#) y [Montaje con puntos de acceso de EFS](#).

4. Guarde los cambios en el archivo.
5. Pruebe la entrada `fstab` utilizando el comando `mount` con la opción `'fake'` junto con las opciones `'verbose'` y `'all'`.

```
$ sudo mount -fav
home/ec2-user/efs      : successfully mounted
```

La instancia EC2 está configurada ahora para montar el sistema de archivos de EFS cuando se reinicia.

Note

En algunos casos, es posible que su instancia de Amazon EC2 deba iniciarse independientemente del estado de su sistema de archivos de Amazon EFS montado. En

tales casos, agregue la opción `nofail` a la entrada de su sistema de archivos en el archivo `/etc/fstab`.

La línea de código que ha añadido al archivo `/etc/fstab` hace lo siguiente.

Campo	Descripción
<code>file-system-id</code> :/	El ID de su sistema de archivos de Amazon EFS. Puede obtener este ID desde la consola o mediante programación desde la CLI o un AWS SDK.
<code>efs-mount-point</code>	El punto de montaje para el sistema de archivos de EFS en su instancia EC2.
<code>efs</code>	El tipo de sistema de archivos. Cuando se utiliza el ayudante de montaje, este tipo es siempre <code>efs</code> .
<code>mount options</code>	<p>Opciones de montaje para el sistema de archivos. Se trata de una lista separada por comas de las siguientes opciones:</p> <ul style="list-style-type: none"> <code>_netdev</code>: indica al sistema operativo que el sistema de archivos reside en un dispositivo que requiere acceso a la red. Esta opción impide que la instancia monte el sistema de archivos hasta que se haya habilitado la red en el cliente. <code>noresvport</code> : indica al cliente NFS que utilice un nuevo puerto de origen de protocolo de control de transmisión (TCP) cuando se restablece la conexión a la red. Esto ayuda a garantizar que el sistema de archivos de EFS tiene una disponibilidad ininterrumpida después de un evento de recuperación de red. <code>tls</code>: activa el cifrado de datos en tránsito <code>iam</code>: utilice esta opción para montar con autorización de IAM en un Amazon EC2 que tenga un perfil de instancia. El uso de la opción de montaje <code>iam</code> requiere también el uso de la opción <code>tls</code>. Para obtener más información, consulte Uso de IAM para controlar el acceso a los datos del sistema de archivos.

Campo	Descripción
	<ul style="list-style-type: none"> • <code>awsprofile= <i>namedprofile</i></code> : utilice esta opción con las opciones <code>iam</code> y <code>tls</code> para realizar el montaje con autorización de IAM en una instancia de Linux mediante un archivo de credenciales. Para obtener más información acerca de los puntos de acceso de EFS, consulte Uso de IAM para controlar el acceso a los datos del sistema de archivos. • <code>accesspoint= <i>access-point-id</i></code> : utilice esta opción con la opción <code>tls</code> para realizar el montaje mediante un punto de acceso de EFS. Para obtener más información acerca de los puntos de acceso de EFS, consulte Trabajo con puntos de acceso de Amazon EFS.
0	Un valor distinto de cero indica que se debe hacer una copia de seguridad del sistema de archivos mediante <code>dump</code> . Para EFS, este valor debe ser 0.
0	El orden en que <code>fsck</code> comprueba los sistemas de archivos en el arranque. Para sistemas de archivos de EFS, este valor debe ser 0 para indicar que <code>fsck</code> no se debe ejecutar durante el <code>start-up</code> .

Uso de NFS para montar automáticamente sistemas de archivos de EFS

Para actualizar el archivo `/etc/fstab` en la instancia de EC2

1. Conéctese a su instancia EC2:

- Para conectarse a la instancia desde un equipo que ejecute macOS o Linux, especifique el archivo `.pem` para su comando SSH. Para ello, use la opción `-i` y la ruta a su clave privada.
- Para conectarte a la instancia desde un ordenador con Windows, puedes usar PuTTY, MindTerm o bien. Para usar PuTTY, instálelo y convierta el archivo `.pem` en un archivo `.ppk`.

Para obtener más información, consulte los siguientes temas de la Guía del usuario de Amazon EC2:

- [Conéctate a tu instancia de Linux desde Windows con PuTTY](#)

- [Conéctate a tu instancia de Linux desde Linux o macOS mediante SSH](#)
2. Abra el archivo `/etc/fstab` en un editor.
 3. Para montar automáticamente un sistema de archivos utilizando NFS en vez del ayudante de montaje de EFS, agregue la siguiente línea al archivo `/etc/fstab`.
 - Sustituya `file_system_id` por el ID del sistema de archivos que va a montar.
 - Sustituya `aws-region` por la que contiene Región de AWS el sistema de archivos, por ejemplo. `us-east-1`
 - Sustituya `mount_point` por el punto de montaje del sistema de archivos.

```
file_system_id.efs.aws-region.amazonaws.com:/ mount_point nfs4
nfsvers=4.1,rsiz=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
0 0
```

La línea de código que ha añadido al archivo `/etc/fstab` hace lo siguiente.

Campo	Descripción
<code>file-system-id</code> :/	El ID de su sistema de archivos de Amazon EFS. Puede obtener este ID desde la consola o mediante programación desde la CLI o un AWS SDK.
<code>efs-mount-point</code>	El punto de montaje para el sistema de archivos de EFS en su instancia EC2.
<code>nfs4</code>	Especifica el tipo de sistema de archivos.
<code>mount options</code>	Lista separada por comas de opciones de montaje para el sistema de archivos: <ul style="list-style-type: none"> • <code>nfsvers=4.1</code> : especifica el uso de NFS v4.1. • <code>rsiz=1048576</code> : para mejorar el rendimiento, establece el número máximo de bytes de datos que el cliente NFS puede recibir por cada solicitud READ de la red al leer datos de un archivo en un sistema de archivos EFS. 1048576 es el tamaño más grande posible.

Campo	Descripción
	<ul style="list-style-type: none"> • <code>wsize=1048576</code> : para mejorar el rendimiento, establece el número máximo de bytes de datos que el cliente NFS puede enviar por cada solicitud WRITE de la red al escribir datos en un archivo en un sistema de archivos EFS. 1048576 es el tamaño más grande posible. • <code>hard</code>: establece el comportamiento de recuperación del cliente NFS después de que se agote el tiempo de espera de una solicitud NFS, de modo que las solicitudes de NFS se vuelven a intentar indefinidamente hasta que el servidor responda. Le recomendamos que utilice la opción de montaje forzado (<code>hard</code>) para garantizar la integridad de los datos. Si utiliza un montaje <code>soft</code>, establezca el parámetro <code>timeo</code> en al menos 150 décimas de segundo (15 segundos). De esta forma, ayuda a reducir el riesgo de daño en los datos que es inherente con montajes flexibles. • <code>timeo=600</code> : establece el valor de tiempo de espera que utiliza el cliente NFS para esperar una respuesta antes de volver a intentar una solicitud en 600 décimas de segundo (60 segundos). Si debe cambiar el parámetro de tiempo de espera (<code>timeo</code>), le recomendamos que utilice un valor de al menos 150, lo que equivale a 15 segundos. De esta forma, se evita una reducción del rendimiento. • <code>retrans=2</code> : establece en 2 el número de veces que el cliente de NFS reintenta una solicitud antes de intentar una acción de recuperación adicional. • <code>noresvport</code> : indica al cliente NFS que utilice un nuevo puerto de origen de protocolo de control de transmisión (TCP) cuando se restablece la conexión a la red. Esto ayuda a garantizar que el sistema de archivos de EFS tiene una disponibilidad ininterrumpida después de un evento de recuperación de red. • <code>_netdev</code>: impide que el cliente intente montar el sistema de archivos de EFS hasta que se haya habilitado la red.
0	Especifica el valor <code>dump</code> ; 0 indica a la utilidad <code>dump</code> que no haga copias de seguridad del sistema de archivos.

Campo	Descripción
0	Indica a la utilidad fsck que no se ejecute durante el arranque.

Montaje de EFS en varias instancias de EC2 mediante AWS Systems Manager

Puede montar sistemas de archivos EFS en varias instancias de Amazon EC2 de forma remota y segura sin tener que iniciar sesión en las instancias mediante el AWS Systems Manager Run comando. Para obtener más información sobre AWS Systems Manager Run Command, consulte [AWS Systems Manager run command](#) en la Guía del AWS Systems Manager usuario. Se requieren los siguientes requisitos previos antes de montar sistemas de archivos de EFS mediante este método:

1. Las instancias de EC2 se lanzan con un perfil de instancia que incluye la política de permisos AmazonElasticFileSystemsUtils. Para obtener más información, consulte [Paso 1: Configure un perfil de instancia de IAM con los permisos necesarios.](#)
2. La versión 1.28.1 o posterior del cliente (amazon-efs-utils paquete) de Amazon EFS está instalada en las instancias EC2. Puede usar AWS Systems Manager para instalar automáticamente el paquete en sus instancias. Para obtener más información, consulte [Paso 2: Configurar una asociación utilizada por State Manager para instalar o actualizar el cliente de Amazon EFS.](#)

Montaje de varios sistemas de archivos de EFS en varias instancias de EC2 mediante la consola

1. Abra la AWS Systems Manager consola en <https://console.aws.amazon.com/systems-manager/>.
2. En el panel de navegación, elija Run Command (Ejecutar comando).
3. Elija Run a command (Ejecutar un comando).
4. Escriba **AWS-RunShellScript** en el campo de búsqueda Comandos.
5. Seleccione AWS- RunShell Script.
6. En Parámetros de comando, introduzca el comando mount que se utilizará para cada sistema de archivos de EFS que desee montar. Por ejemplo:

```
sudo mount -t efs -o tls fs-12345678:/ /mnt/efs
sudo mount -t efs -o tls,accesspoint=fsap-12345678 fs-01233210 /mnt/efs
```

Para más información sobre el uso de comandos de EFS utilizando el cliente de Amazon EFS, consulte [Montaje en instancias de Linux de Amazon EC2 mediante el asistente de montaje de EFS](#) o [Montaje en instancias de Mac de Amazon EC2 mediante el asistente de montaje de EFS](#).

7. Seleccione las instancias EC2 AWS Systems Manager gestionadas de destino en las que desea que se ejecute el comando.
8. Realice cualquier otra configuración adicional que desee. A continuación, seleccione Ejecutar para ejecutar el comando y montar los sistemas de archivos de EFS especificados en el comando.

Una vez que ejecute el comando, podrá ver su estado en el historial del comando.

Montaje de sistemas de archivos EFS desde otro Cuenta de AWS o desde una VPC

Puede montar su sistema de archivos de Amazon EFS utilizando una autorización de IAM para clientes NFS y puntos de acceso de EFS mediante el ayudante de montaje de EFS. De forma predeterminada, este ayudante utiliza el servicio de nombres de dominio (DNS) para resolver la dirección IP del destino de montaje de EFS. Si está montando el sistema de archivos desde otra cuenta o nube virtual privada (VPC), debe resolver el destino de montaje de EFS manualmente.

A continuación, encontrará instrucciones para determinar la dirección IP del destino de montaje de EFS correcta que debe utilizarse para el cliente de NFS. También encontrará instrucciones de configuración del cliente para montar el sistema de archivos de EFS utilizando esa dirección IP.

Montaje mediante IAM o puntos de acceso de otra VPC

Cuando utiliza una interconexión de VPC o una gateway de tránsito para conectar las VPC, las instancias de Amazon EC2 en una VPC pueden acceder a los sistemas de archivos de EFS en otra VPC, incluso si las VPC pertenecen a diferentes cuentas.

Requisitos previos

Antes de utilizar el procedimiento siguiente, realice estos pasos:

- Instale el cliente Amazon EFS, que forma parte del conjunto de utilidades `amazon-efs-utils`, en la instancia de procesamiento en la que va a montar el sistema de archivos de EFS. Utilice el asistente de montaje de EFS, que se incluye en `amazon-efs-utils`, para montar el sistema

de archivos. Para obtener instrucciones sobre cómo instalar `amazon-efs-utils`, consulte [Instalación de las herramientas de Amazon EFS](#).

- Permita la acción `ec2:DescribeAvailabilityZones` en la política de IAM para el rol de IAM que ha asignado a la instancia. Le recomendamos que adjunte la política AWS gestionada `AmazonElasticFileSystemsUtils` a una entidad de IAM para proporcionar los permisos necesarios a la entidad.
- Al montar desde otro Cuenta de AWS, actualice la política de recursos del sistema de archivos para permitir la `elasticfilesystem:DescribeMountTarget` acción para el ARN principal de otro. Cuenta de AWS Por ejemplo:

```
{
  "Id": "access-point-example03",
  "Statement": [
    {
      "Sid": "access-point-statement-example03",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::555555555555"},
      "Action": "elasticfilesystem:DescribeMountTargets",
      "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-
system/fs-12345678"
    }
  ]
}
```

Para obtener más información sobre las políticas de recursos de un sistema de archivos de EFS, consulte [Políticas basadas en recursos de Amazon EFS](#).

- Instale `botocore`. El cliente EFS usa `botocore` para recuperar la dirección IP del destino del montaje cuando el nombre de DNS del sistema de archivos no se puede resolver al montar un sistema de archivos en otra VPC. Para obtener más información, consulte [Instalar botocore](#) en el archivo README de `amazon-efs-utils`.
- Configure una interconexión de VPC o una gateway de tránsito de VPC.

Para conectar la VPC del cliente y la VPC del sistema de archivos de EFS, utilice una interconexión de VPC o una gateway de tránsito de VPC. Cuando utiliza una interconexión de VPC o una gateway de tránsito para conectar las VPC, las instancias de Amazon EC2 en una VPC pueden acceder a los sistemas de archivos de EFS en otra VPC, incluso si las VPC pertenecen a diferentes cuentas.

Una puerta de enlace de tránsito es un hub de tránsito de red que puede utilizar para interconectar sus VPC y redes en las instalaciones. Para obtener más información acerca del uso de gateways de tránsito de VPC, consulte [Introducción a gateways de tránsito](#) en la Guía de gateways de tránsito de Amazon VPC.

Una conexión de emparejamiento de VPC es una conexión de red entre dos instancias de VPC. Este tipo de conexión permite enrutar el tráfico entre ellas mediante direcciones de protocolo de Internet versión 4 (IPv4) o de protocolo de Internet versión 6 (IPv6) privadas. Puede utilizar el emparejamiento de VPC para conectar VPC dentro del mismo Región de AWS o entre uno y otro. Región de AWS Para obtener más información sobre la conexión de emparejamiento de las VPC, consulte [¿Qué es una conexión de emparejamiento de VPC?](#) en la Guía de conexión de emparejamiento de VPC de Amazon.

Para garantizar una alta disponibilidad del sistema de archivos, recomendamos utilizar siempre una dirección IP del destino de montaje de EFS que esté en la misma zona de disponibilidad (AZ) que su cliente de NFS. Si va a montar un sistema de archivos de EFS que esté en otra cuenta, asegúrese de que el cliente de NFS y el destino de montaje de EFS estén en el mismo ID de la zona de disponibilidad. Este requisito se aplica porque los nombres de zona de disponibilidad pueden ser distintos entre las cuentas.

Para montar un sistema de archivos de EFS en otra VPC mediante IAM o un punto de acceso

1. Conéctese a su instancia EC2:

- Para conectarse a la instancia desde un equipo que ejecute macOS o Linux, especifique el archivo `.pem` para su comando SSH. Para ello, use la opción `-i` y la ruta a su clave privada.
- Para conectarte a la instancia desde un ordenador con Windows, puedes usar PuTTY, MindTerm o bien. Para usar PuTTY, instálelo y convierta el archivo `.pem` en un archivo `.ppk`.

Para obtener más información, consulte los siguientes temas de la Guía del usuario de Amazon EC2:

- [Conéctate a tu instancia de Linux desde Windows con PuTTY](#)
- [Conéctate a tu instancia de Linux desde Linux o macOS mediante SSH](#)

2. Cree un directorio para montar el sistema de archivos mediante el comando siguiente.

```
$ sudo mkdir /mnt/efs
```

3. Para montar el sistema de archivos con una autorización de IAM, utilice el comando siguiente:

```
$ sudo mount -t efs -o tls,iam file-system-dns-name /mnt/efs/
```

Para obtener más información sobre cómo utilizar la autorización de IAM con EFS, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#).

Para montar el sistema de archivos con un punto de acceso EFS, utilice el comando siguiente:

```
$ sudo mount -t efs -o tls,accesspoint=access-point-id file-system-dns-name /mnt/efs/
```

Para obtener más información acerca de los puntos de acceso de EFS, consulte [Trabajo con puntos de acceso de Amazon EFS](#).

Montar sistemas de archivos de Amazon EFS desde otra Región de AWS

Si va a montar el sistema de archivos EFS desde otra VPC que se encuentra en un sistema de archivos Región de AWS distinto del sistema de archivos, tendrá que editar el `efs-utils.conf` archivo. En `/dist/efs-utils.conf`, busque la siguiente línea:

```
#region = us-east-1
```

Elimine los comentarios de la línea y sustituya el valor por el ID de la región en la que se encuentra el sistema de archivos, si no está en `us-east-1`.

Montaje desde otro Cuenta de AWS en el mismo VPC

Al utilizar VPC compartidas, puede montar un sistema de archivos Amazon EFS que sea propiedad Cuenta de AWS de una instancia de Amazon EC2 que sea propiedad de otra. Cuenta de AWS Para obtener más información acerca de la configuración de una VPC compartida, consulte [Trabajar con VPC compartidas](#) en la Guía de interconexión de Amazon VPC.

Después de configurar el uso compartido de VPC, las instancias EC2 pueden montar el sistema de archivos de EFS con la resolución de nombres del sistema de nombres de dominio (DNS) o el

ayudante de montaje de EFS. Se recomienda utilizar el ayudante de montaje de EFS para montar los sistemas de archivos de EFS.

Uso del Network File System para montar sistemas de archivos EFS

Note

En esta sección, aprenderá a montar el sistema de archivos Amazon EFS sin el `amazon-efs-utils` paquete. Para utilizar el cifrado de datos en tránsito con el sistema de archivos, debe montar el sistema de archivos con TLS (Transport Layer Security). Para ello, le recomendamos que utilice el `amazon-efs-utils` paquete. Para obtener más información, consulte [Instalación de las herramientas de Amazon EFS](#).

A continuación se ofrece información acerca de cómo instalar el cliente Network File System (NFS) y montar el sistema de archivos de Amazon EFS en una instancia de Amazon EC2. También puede encontrar una explicación sobre el comando `mount` y las opciones disponibles para especificar el sistema de nombres de dominio (DNS) de su sistema de archivos en el comando `mount`. Además, puede encontrar información acerca de cómo utilizar el archivo `fstab` para volver a montar automáticamente el sistema de archivos después de los reinicios del sistema.

Note

Antes de poder montar un sistema de archivos, debe crear, configurar y lanzar los recursos de AWS relacionados. Para obtener instrucciones detalladas, consulte [Introducción a Amazon Elastic File System](#).

Note

Antes de montar el sistema de archivos, debe crear grupos de seguridad de VPC para las instancias de Amazon EC2 y montar los destinos con el acceso entrante y saliente necesario. Para obtener más información, consulte [Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje](#).

Temas

- [Compatibilidad con NFS](#)
- [Instalación del cliente NFS](#)
- [Opciones recomendadas de montaje NFS](#)
- [Montaje en Amazon EC2 con un nombre de DNS](#)
- [Montaje con una dirección IP](#)

Compatibilidad con NFS

Amazon EFS es compatible con los protocolos de las versiones 4.0 y 4.1 de Network File System (NFSv4) a la hora de montar los sistemas de archivos en instancias de Amazon EC2. Aunque NFSv4.0 es compatible, le recomendamos que utilice NFSv4.1. Montar el sistema de archivos de Amazon EFS en la instancia de Amazon EC2 también requiere que un cliente NFS sea compatible con el protocolo NFSv4 elegido. Las instancias de Mac de Amazon EC2 que ejecutan macOS Big Sur solo son compatibles con NFS v4.0.

Amazon EFS no es compatible con la opción de montaje `nconnect`.


Note

Para las versiones 5.4.* del kernel de Linux, el cliente NFS de Linux utiliza un valor `read_ahead_kb` predeterminado de 128 KB. Se recomienda aumentar este valor a 15 MB. Para obtener más información, consulte [Optimización del tamaño de `read_ahead_kb` de NFS](#).


Para obtener un desempeño óptimo y evitar diversos errores conocidos del cliente NFS, le recomendamos trabajar con un kernel de Linux reciente. Si utiliza una distribución de Linux empresarial, le recomendamos lo siguiente:

- Amazon Linux 2
- Amazon Linux 2017.09 o posterior
- Red Hat Enterprise Linux (y sus derivados como CentOS) versión 7 y posteriores
- Ubuntu 16.04 LTS y posterior
- SLES 12 Sp2 o posterior

Si utiliza otra distribución o un kernel personalizado, le recomendamos la versión de kernel 4.3 o posterior.

 Note

RHEL 6.9 podría ser inadecuado para determinadas cargas de trabajo debido a [Rendimiento bajo al abrir muchos archivos en paralelo](#).

 Note

No se admite el montaje de sistemas de archivos Amazon EFS con instancias de Amazon EC2 que ejecuten Microsoft Windows.

Solución de problemas de versiones de kernel y AMI

Para solucionar problemas relacionados con determinadas versiones de AMI o kernel al utilizar Amazon EFS desde una instancia de EC2, consulte [Solución de problemas de AMI y de kernel](#).

Instalación del cliente NFS

Para montar el sistema de archivos de Amazon EFS en la instancia de Amazon EC2, primero tiene que instalar un cliente NFS. Para conectarse a la instancia de EC2 e instalar un cliente NFS, necesita el nombre de DNS público de la instancia EC2 y un nombre de usuario para iniciar sesión. Ese nombre de usuario para la instancia suele ser `ec2-user`.

Para conectar la instancia EC2 e instalar el cliente NFS

1. Conéctese a la instancia EC2. Tenga en cuenta lo siguiente en relación con la conexión a la instancia:
 - Para conectarse a la instancia desde un equipo que ejecute macOS o Linux, especifique el archivo `.pem` a su cliente SSH (Secure Shell) con la opción `-i` y la ruta a su clave privada.
 - Para conectarte a la instancia desde un ordenador con Windows, puedes usar PuTTY, MindTerm o bien. Si pretende utilizar PuTTY, debe instalarlo y utilizar el siguiente procedimiento para convertir el archivo `.pem` a un archivo `.ppk`.

Para obtener más información, consulte los siguientes temas de la Guía del usuario de Amazon EC2:

- [Conexión a la instancia Linux desde Windows utilizando PuTTY](#)
- [Conexión a la instancia de Linux mediante SSH](#)

El archivo de claves no puede ser visible públicamente para SSH. Puede utilizar el comando `chmod 400 filename.pem` para establecer estos permisos. Para obtener más información, consulte [Crear un par de claves](#).

2. (Opcional) Obtener actualizaciones y reiniciar.

```
$ sudo yum -y update
$ sudo reboot
```

3. Tras el reinicio, vuelva a conectarse a su instancia EC2.
4. Instale el cliente NFS.

Si utiliza una AMI de Amazon Linux o una AMI de Red Hat Linux, instale el cliente NFS con el siguiente comando.

```
$ sudo yum -y install nfs-utils
```

Si está utilizando una AMI de Amazon EC2 de Ubuntu, instale el cliente NFS con el siguiente comando.

```
$ sudo apt-get -y install nfs-common
```

5. Inicie el servicio NFS con los siguientes comandos. Para RHEL 7:

```
$ sudo service nfs start
```

Para RHEL 8:

```
$ sudo service nfs-server start
```

6. Compruebe que se inició el servicio NFS, como se indica a continuación.

```
$ sudo service nfs status
Redirecting to /bin/systemctl status nfs.service
# nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled; vendor
   preset: disabled)
   Active: active (exited) since Wed 2019-10-30 16:13:44 UTC; 5s ago
   Process: 29446 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/
   SUCCESS)
   Process: 29441 ExecStartPre=/bin/sh -c /bin/kill -HUP `cat /run/gssproxy.pid`
   (code=exited, status=0/SUCCESS)
   Process: 29439 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
   Main PID: 29446 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/nfs-server.service
```

Si utiliza un kernel personalizado (es decir, si crea una AMI personalizada), debe incluir como mínimo el módulo de kernel del cliente NFSv4.1 y el ayudante de montaje de espacio de usuarios de NFS4 adecuado.

Note

Si elige la AMI de Amazon Linux 2016.03.0 o AMI de Amazon Linux 2016.09.0 al lanzar la instancia de Amazon EC2, no tendrá que instalar `nfs-utils` porque ya está incluido en la AMI de forma predeterminada.

Siguiente: Montaje del sistema de archivos

Utilice uno de los siguientes procedimientos para montar su sistema de archivos.

- [Montaje en Amazon EC2 con un nombre de DNS](#)
- [Montaje con una dirección IP](#)
- [Cómo montar su sistema de archivos de Amazon EFS automáticamente](#)

Opciones recomendadas de montaje NFS

Le recomendamos los siguientes valores de opciones de montaje de Linux:

- `noresvport`: indica al cliente NFS que utilice un nuevo puerto de origen de protocolo de control de transmisión (TCP) sin privilegios cuando se restablece la conexión a la red. El software cliente NFS incluido en las versiones anteriores del kernel de Linux (versiones 5.4 y anteriores) presenta un comportamiento que provoca que los clientes NFS, al desconectarse, intenten volver a conectarse al mismo puerto de origen TCP. Este comportamiento no cumple con la RFC de TCP y puede impedir que estos clientes restablezcan rápidamente las conexiones con un sistema de archivos EFS.

El uso de la opción `noresvport` ayuda a garantizar que los clientes NFS se vuelvan a conectar de forma transparente al sistema de archivos EFS, manteniendo una disponibilidad ininterrumpida al volver a conectarse después de un evento de recuperación de la red.

Important

Recomendamos encarecidamente utilizar la opción de montaje `noresvport` para garantizar que el sistema de archivos EFS tenga una disponibilidad ininterrumpida tras un evento de reconexión o recuperación de la red.

Plantéese utilizar el [ayudante de montaje de EFS](#) para montar sus sistemas de archivos. El asistente de montaje de EFS utiliza opciones de montaje de NFS optimizadas para los sistemas de archivos de Amazon EFS.

- `rsize=1048576`: establece el número máximo de bytes de datos que el cliente NFS puede recibir para cada solicitud de red READ. Este valor se aplica al leer los datos desde un archivo en un sistema de archivos de EFS. Le recomendamos que utilice el mayor tamaño posible (hasta 1048576) para evitar un rendimiento reducido.
- `wsize=1048576`: establece el número máximo de bytes de datos que el cliente NFS puede enviar para cada solicitud de red WRITE. Este valor se aplica al escribir datos en un archivo en un sistema de archivos de EFS. Le recomendamos que utilice el mayor tamaño posible (hasta 1048576) para evitar un rendimiento reducido.
- `hard`: establece el comportamiento de recuperación del cliente NFS después de que se agote el tiempo de espera de una solicitud NFS, de modo que las solicitudes de NFS se vuelven a intentar indefinidamente hasta que el servidor responda. Le recomendamos que utilice la opción de montaje forzado (`hard`) para garantizar la integridad de los datos. Si utiliza un montaje `soft`, establezca el parámetro `timeo` en al menos 150 décimas de segundo (15 segundos). De esta forma, ayuda a reducir el riesgo de daño en los datos que es inherente con montajes flexibles.
- `timeo=600`: establece el valor de tiempo de espera que utiliza el cliente NFS para esperar una respuesta antes de volver a intentar una solicitud NFS en 600 décimas de segundo (60 segundos).

Si debe cambiar el parámetro de tiempo de espera (`timeo`), le recomendamos que utilice un valor de al menos 150, lo que equivale a 15 segundos. De esta forma, se evita una reducción del rendimiento.

- `retrans=2`: establece en 2 el número de veces que el cliente de NFS reintenta una solicitud antes de intentar una acción de recuperación adicional.
- `_netdev`: cuando está presente en `/etc/fstab`, impide que el cliente intente montar el sistema de archivos de EFS hasta que se haya habilitado la red.
- `nofail`: si su instancia de EC2 tiene que iniciarse independientemente del estado de su sistema de archivos de EFS montado, añada la opción `nofail` a la entrada de su sistema de archivos en el archivo `/etc/fstab`.

Si no utiliza los valores predeterminados anteriores, tenga en cuenta lo siguiente:

- En general, evite configurar otras opciones de montaje que sean diferentes de los valores predeterminados, lo que puede provocar una reducción del rendimiento y otros problemas. Por ejemplo, cambiar el tamaño del búfer de lectura o escritura, o deshabilitar el almacenamiento en caché de atributos puede reducir el rendimiento.
- Amazon EFS ignora los puertos de origen. Si cambia los puertos de origen de Amazon EFS, no tiene ningún efecto.
- Amazon EFS no es compatible con la opción de montaje `nconnect`.
- Amazon EFS no es compatible con ninguna de las variantes de seguridad de Kerberos. Por ejemplo, el siguiente comando de montaje devuelve un error.

```
$ mount -t nfs4 -o krb5p <DNS_NAME>:/ /efs/
```

- Le recomendamos que monte el sistema de archivos utilizando su nombre de DNS. Este nombre se resuelve en una dirección IP del destino de montaje de Amazon EFS en la misma zona de disponibilidad que su instancia de Amazon EC2. Si utiliza el destino de montaje en una zona de disponibilidad distinta de la de su instancia de Amazon EC2, incurre en cargos de EC2 estándar para datos enviados entre zonas de disponibilidad. También podría ver latencias más elevadas para las operaciones del sistema de archivos.
- Para más opciones de montaje y explicaciones detalladas de las opciones predeterminadas, consulte las páginas [man fstab](#) y [man nfs](#) en la documentación de Linux.

Montaje en Amazon EC2 con un nombre de DNS

Note

Antes de montar el sistema de archivos, debe añadir una regla al grupo de seguridad de destino de montaje que permita el acceso entrante a NFS desde el grupo de seguridad de EC2. Para obtener más información, consulte [Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje](#).

- Nombre de DNS del sistema de archivos: utilizar el nombre de DNS del sistema de archivos es la opción de montaje más sencilla. El nombre de DNS del sistema de archivos resuelve automáticamente la dirección IP de un destino de montaje en la zona de disponibilidad de la instancia de Amazon EC2 que se conecta. Puede obtener el nombre de DNS desde la consola o, si tiene el ID del sistema de archivos, puede construirlo mediante la siguiente convención.

```
file-system-id.efs.aws-region.amazonaws.com
```

Note

La resolución de DNS para nombres del DNS del sistema de archivos requiere que el sistema de archivos de Amazon EFS tenga un destino de montaje en la misma zona de disponibilidad que la instancia del cliente.

- Con el nombre de DNS del sistema de archivos, puede montar un sistema de archivos en su instancia de Linux de Amazon EC2 con el siguiente comando.

```
sudo mount -t nfs -o  
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport file-  
system-id.efs.aws-region.amazonaws.com:/ /efs-mount-point
```

- Con el nombre de DNS del sistema de archivos, puede montar un sistema de archivos en su instancia de Mac de Amazon EC2 que ejecute una versión de macOS compatible (Big Sur, Monterey, Ventura) con el siguiente comando.

```
sudo mount -t nfs -o  
nfsvers=4.0,rsiz=65536,wsiz=65536,hard,timeo=600,retrans=2,noresvport,mountport=2049  
system-id.efs.aws-region.amazonaws.com:/ /efs
```

Important

Debe usar `mountport=2049` para conectarse correctamente al sistema de archivos de EFS cuando lo monte en instancias de Mac EC2 que ejecuten versiones compatibles con macOS.

- Nombre de DNS de destino de montaje: en diciembre de 2016, presentamos los nombres de DNS de sistemas de archivos. Seguimos proporcionando un nombre DNS para cada destino de montaje de las zonas de disponibilidad para compatibilidad con versiones anteriores. La forma genérica de un nombre DNS de destino de montaje es la siguiente.

```
availability-zone.file-system-id.efs.aws-region.amazonaws.com
```

Note

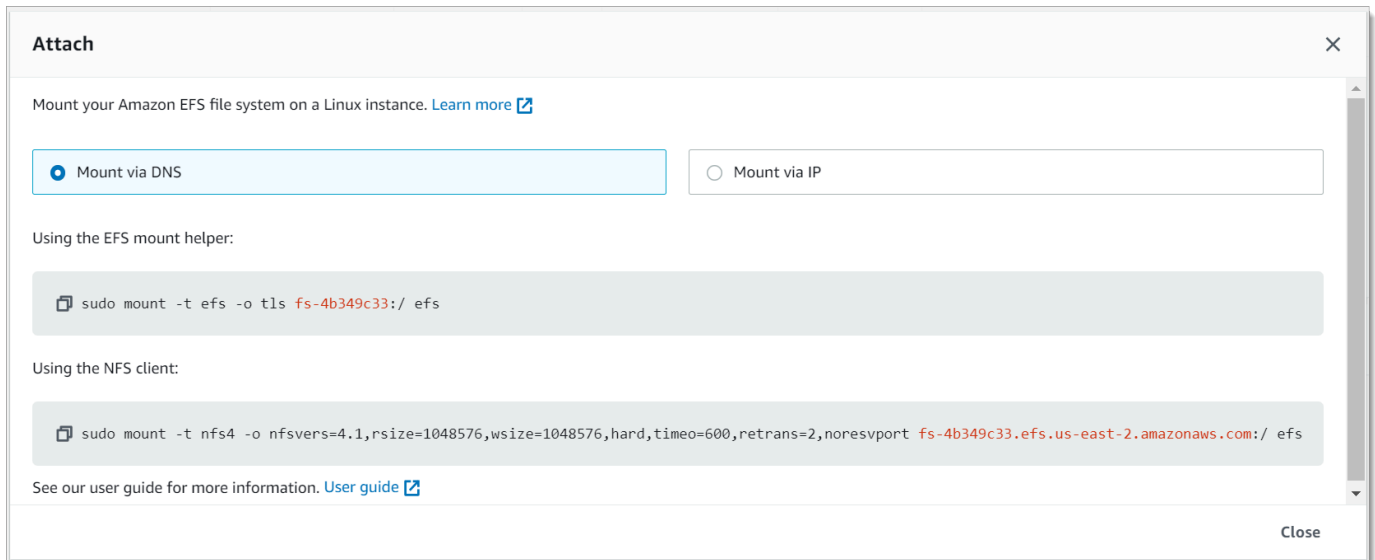
Se admite la resolución de nombres de DNS de destino de montaje en todas las zonas de disponibilidad.

En algunos casos, es posible que elimine un destino de montaje y que cree otro nuevo en la misma zona de disponibilidad. En este caso, el nombre DNS para ese nuevo destino de montaje en dicha zona de disponibilidad es el mismo que el nombre DNS del antiguo destino de montaje.

Puede ver y copiar los comandos exactos para montar el sistema de archivos en el cuadro de diálogo Adjuntar.

Para ver los comandos de montaje de su sistema de archivos

1. En la consola de Amazon EFS, elija el sistema de archivos que desee montar para que aparezca su página de detalles.
2. Para ver los comandos de montaje que se van a utilizar en este sistema de archivos, seleccione Adjuntar en la esquina superior derecha.



La pantalla Adjuntar muestra los comandos exactos que se utilizarán para montar el sistema de archivos.

3. La vista predeterminada Montar mediante DNS muestra el comando para montar el sistema de archivos con el nombre de DNS del sistema de archivos cuando se monta con el asistente de montaje de EFS o un cliente NFS.

Para obtener una lista de Región de AWS los dispositivos compatibles con Amazon EFS, consulte [Amazon Elastic File System](#) en el Referencia general de AWS.

Para poder utilizar un nombre DNS en el comando mount, se debe cumplir lo siguiente:

- La instancia EC2 que se conecta debe estar dentro de una VPC y se debe configurar para utilizar el servidor DNS proporcionado por Amazon. Para obtener información sobre el servidor DNS de Amazon, consulte [Conjuntos de opciones de DHCP](#) en la Guía del usuario de Amazon VPC.
- La VPC de la instancia EC2 de conexión debe tener habilitados la resolución de DNS y los nombres de host DNS. Para obtener más información, consulte [Visualización de nombres de host DNS de la instancia de EC2](#) en la Guía del usuario de VPC de Amazon.
- La instancia EC2 que se conecta debe estar dentro de la misma VPC que el sistema de archivos de EFS. Para obtener más información acerca del acceso a y del montaje de un sistema de archivos desde otra ubicación o desde una VPC diferente, consulte [Tutorial: Crear y montar un sistema de archivos en las instalaciones con AWS Direct Connect y una VPN](#) y [Tutorial: Montar un sistema de archivos desde una VPC distinta](#) .

Note

Le recomendamos que espere 90 segundos después de crear un destino de montaje antes de montar el sistema de archivos. Esta espera permite que los registros DNS se propaguen completamente en el Región de AWS lugar donde se encuentra el sistema de archivos.

Montaje con una dirección IP

Como alternativa al montaje de su sistema de archivos de Amazon EFS con el nombre de DNS, las instancias de Amazon EC2 pueden montar un sistema de archivos mediante una dirección IP del montaje de destino. El montaje por dirección IP funciona en entornos donde el DNS está deshabilitado, tales como VPC con nombres de host DNS deshabilitados.

También puede configurar el montaje de un sistema de archivos mediante la dirección IP de destino de montaje como una opción de reserva para aplicaciones configuradas para montar el sistema de archivos utilizando su nombre de DNS de forma predeterminada. Al conectar a una dirección IP de destino de montaje, las instancias EC2 deben montar utilizando la dirección IP del destino de montaje en la misma zona de disponibilidad de la instancia que se conecta.

Puede ver y copiar los comandos exactos para montar el sistema de archivos en el cuadro de diálogo Adjuntar.

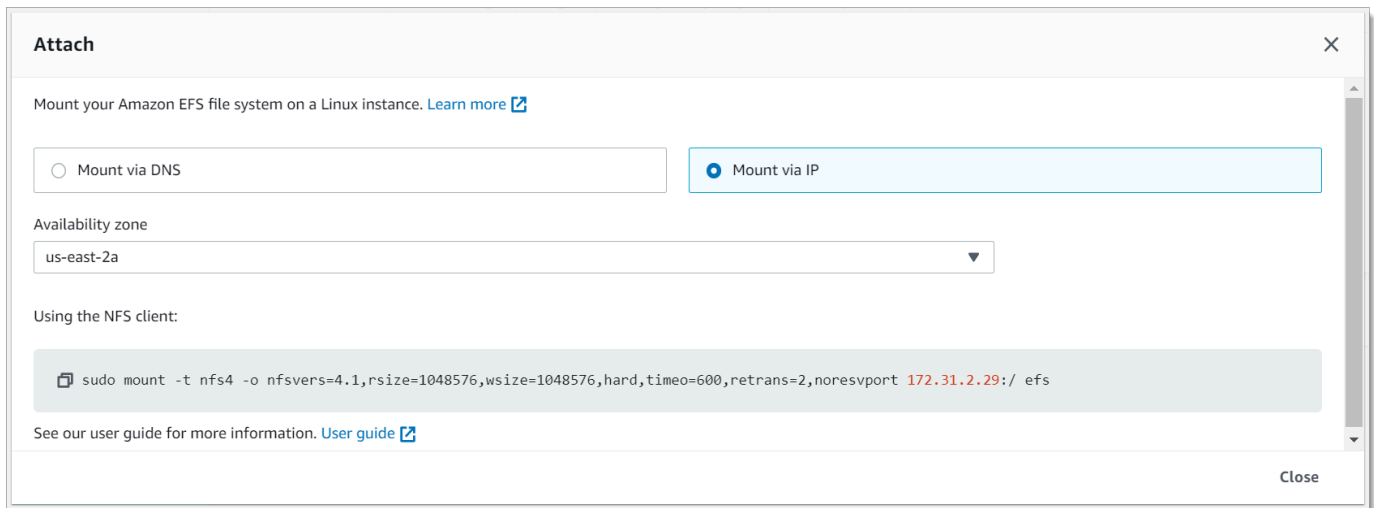
Note

Antes de montar el sistema de archivos, debe añadir una regla para el grupo de seguridad de destino de montaje que permita el acceso entrante a NFS desde el grupo de seguridad de EC2. Para obtener más información, consulte [Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje](#).

Para ver y copiar los comandos exactos para montar el sistema de archivos EFS mediante la dirección IP de destino del montaje

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. En la consola de Amazon EFS, elija el sistema de archivos que desee montar para que aparezca su página de detalles.

- Para ver los comandos de montaje que se van a utilizar en este sistema de archivos, seleccione **Adjuntar** en la esquina superior derecha.



- La pantalla **Adjuntar** muestra los comandos exactos que se utilizarán para montar el sistema de archivos.

Seleccione **Montar mediante IP** para mostrar el comando que permite montar el sistema de archivos mediante la dirección IP de destino del montaje en la zona de disponibilidad seleccionada con un cliente NFS.

- Con la dirección IP de un destino de montaje en el comando `mount`, puede montar un sistema de archivos en su instancia de Linux de Amazon EC2 con el siguiente comando.

```
sudo mount -t nfs -o
nfsvers=4.1,rsz=1048576,wsz=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-IP:/ /efs
```

- Con la dirección IP de un destino de montaje en el comando `mount`, puede montar un sistema de archivos en su instancia de Mac de Amazon EC2 que ejecute macOS Big Sur con el siguiente comando.

```
sudo mount -t nfs -o
nfsvers=4.0,rsz=65536,wsz=65536,hard,timeo=600,retrans=2,noresvport,mountport=2049 mount-
target-IP:/ /efs
```

⚠ Important

Debe usar `mountport=2049` para conectarse correctamente al sistema de archivos de EFS cuando lo monte en instancias de Mac EC2 que ejecuten macOS Big Sur.

Montaje con una dirección IP en AWS CloudFormation

También puede montar su sistema de archivos utilizando una dirección IP en una AWS CloudFormation plantilla. Para obtener más información, consulte [storage-efs-mountfilesystem-ip-addr.config en el repositorio awsdocs/elastic-beanstalk-samples para ver los archivos](#) de configuración proporcionados por la comunidad. GitHub

Consideraciones de montaje adicionales

Le recomendamos los siguientes valores de opciones de montaje de Linux:

- `rsize=1048576`: establece el número máximo de bytes de datos que el cliente NFS puede recibir para cada solicitud de red READ. Este valor se aplica al leer los datos desde un archivo en un sistema de archivos de EFS. Le recomendamos que utilice el mayor tamaño posible (hasta 1048576) para evitar un rendimiento reducido.
- `wsize=1048576`: establece el número máximo de bytes de datos que el cliente NFS puede enviar para cada solicitud de red WRITE. Este valor se aplica al escribir datos en un archivo en un sistema de archivos de EFS. Le recomendamos que utilice el mayor tamaño posible (hasta 1048576) para evitar un rendimiento reducido.
- `hard`: establece el comportamiento de recuperación del cliente NFS después de que se agote el tiempo de espera de una solicitud NFS, de modo que las solicitudes de NFS se vuelven a intentar indefinidamente hasta que el servidor responda. Le recomendamos que utilice la opción de montaje forzado (`hard`) para garantizar la integridad de los datos. Si utiliza un montaje `soft`, establezca el parámetro `timeo` en al menos 150 décimas de segundo (15 segundos). De esta forma, ayuda a reducir el riesgo de daño en los datos que es inherente con montajes flexibles.
- `timeo=600`: establece el valor de tiempo de espera que utiliza el cliente NFS para esperar una respuesta antes de volver a intentar una solicitud NFS en 600 décimas de segundo (60 segundos). Si debe cambiar el parámetro de tiempo de espera (`timeo`), le recomendamos que utilice un valor de al menos 150, lo que equivale a 15 segundos. De esta forma, se evita una reducción del rendimiento.

- `retrans=2`: establece en 2 el número de veces que el cliente de NFS reintenta una solicitud antes de intentar una acción de recuperación adicional.
- `noresvport`: indica al cliente NFS que utilice un nuevo puerto de origen de protocolo de control de transmisión (TCP) sin privilegios cuando se restablece la conexión a la red. Esto ayuda a garantizar que el sistema de archivos de EFS tiene una disponibilidad ininterrumpida después de un evento de recuperación de red.
- `_netdev`: cuando está presente en `/etc/fstab`, impide que el cliente intente montar el sistema de archivos de EFS hasta que se haya habilitado la red.

En general, evite configurar otras opciones de montaje que sean diferentes de los valores predeterminados, lo que puede provocar una reducción del rendimiento y otros problemas. Si no utiliza los valores predeterminados anteriores, tenga en cuenta lo siguiente:

- Cambiar el tamaño del búfer de lectura o escritura, o deshabilitar el almacenamiento en caché de atributos puede reducir el rendimiento.
- Amazon EFS ignora los puertos de origen. Si cambia los puertos de origen de Amazon EFS, no tiene ningún efecto.
- Amazon EFS no es compatible con ninguna de las variantes de seguridad de Kerberos. Por ejemplo, el siguiente comando de montaje devuelve un error.

```
$ mount -t nfs4 -o krb5p <DNS_NAME>:/ /efs/
```

- Le recomendamos que monte el sistema de archivos utilizando su nombre de DNS. Amazon EFS resuelve este nombre en una dirección IP del destino de montaje de Amazon EFS en la misma zona de disponibilidad que su instancia de Amazon EC2 sin llamar a recursos externos. Si utiliza el destino de montaje en una zona de disponibilidad distinta de la de su instancia de Amazon EC2, incurre en cargos de EC2 estándar para datos enviados entre zonas de disponibilidad. También podría ver latencias más elevadas para las operaciones del sistema de archivos.
- Para más opciones de montaje y explicaciones detalladas de las opciones predeterminadas, consulte las páginas [man fstab](#) y [man nfs](#) en la documentación de Linux.

Note

Si su instancia EC2 tiene que iniciarse independientemente del estado de su sistema de archivos de EFS montado, añada la opción `nofail` a la entrada de su sistema de archivos en el archivo `/etc/fstab`.

Desmontaje de sistemas de archivos

Antes de eliminar un sistema de archivos, le recomendamos que lo desmonte de todas las instancias de Amazon EC2 a las que esté conectado. Puede desmontar un sistema de archivos en su instancia de Amazon EC2 ejecutando el comando `umount` de la propia instancia. No puede desmontar un sistema de archivos Amazon EFS a través del AWS CLI, AWS Management Console, el o a través de ninguno de los AWS SDK. Para desmontar un sistema de archivos de Amazon EC2 conectado a una instancia de Amazon EC2 que ejecuta Linux, utilice el comando `umount` como se muestra a continuación:

```
umount /mnt/efs
```

Le recomendamos que no especifique las demás opciones `umount`. Evite la configuración de otras opciones `umount` que sean diferentes de los valores predeterminados.

Puede comprobar que el sistema de archivos de Amazon EFS se haya desmontado ejecutando el comando `df`. Este comando muestra las estadísticas de uso del disco de los sistemas de archivos actualmente montados en la instancia de Amazon EC2 basada en Linux. Si el sistema de archivos de Amazon EFS que desea desmontar no aparece en la salida del comando `df`, esto significa que el sistema de archivos está desmontado.

Example – Identifique el estado de montaje de un sistema de archivos de Amazon EFS y desmóntelo

```
$ df -T
Filesystem Type 1K-blocks Used Available Use% Mounted on
/dev/sda1 ext4 8123812 1138920 6884644 15% /
availability-zone.file-system-id.efs.aws-region.amazonaws.com :/ nfs4 9007199254740992
0 9007199254740992 0% /mnt/efs
```

```
$ umount /mnt/efs
```

```
$ df -T
```

```
Filesystem Type 1K-blocks Used Available Use% Mounted on  
/dev/sda1 ext4 8123812 1138920 6884644 15% /
```

Solución de problemas montaje

A continuación, encontrará información sobre la solución de problemas relacionados con el montaje de sistemas de archivos de Amazon EFS.

- [El montaje del sistema de archivos en la instancia de Windows falla](#)
- [Acceso denegado por el servidor](#)
- [Se produce un error de montaje automático y la instancia no responde](#)
- [Se produce un error de montaje de varios sistemas de archivos de Amazon EFS en /etc/fstab](#)
- [El comando de montaje falla con el mensaje de error "wrong fs type"](#)
- [El comando de montaje falla con el mensaje de error "incorrect mount option"](#)
- [El montaje con un punto de acceso falla](#)
- [El montaje del sistema de archivos falla de inmediato después de la creación del sistema de archivos](#)
- [El montaje del sistema de archivos deja de responder y, a continuación, falla con un error de tiempo de espera agotado](#)
- [El montaje del sistema de archivos con NFS que utiliza el nombre de DNS falla](#)
- [El montaje del sistema de archivos falla y emite el mensaje "nfs not responding \(nfs no responde\)"](#)
- [El estado de ciclo de vida de destino de montaje está atascado](#)
- [El estado del ciclo de vida objetivo del montaje muestra un error](#)
- [El montaje no responde](#)
- [El cliente montado se desconecta](#)
- [Las operaciones en el sistema de archivos recién montado devuelven el error "bad file handle"](#)
- [Error de desmontaje de un sistema de archivos](#)

El montaje del sistema de archivos en la instancia de Windows falla

Se produce un error en el montaje de un sistema de archivos en una instancia de Amazon EC2 en Microsoft Windows.

Acción que debe ejecutarse

No utilice Amazon EFS con instancias EC2 de Windows, pues no es compatible.

Acceso denegado por el servidor

Se produce un error en el montaje del sistema de archivos con el siguiente mensaje:

```
/efs mount.nfs4: access denied by server while mounting 127.0.0.1:/
```

Este problema puede producirse si el cliente NFS no tiene permiso para montar el sistema de archivos.

Acción que debe ejecutarse

Si está intentando montar el sistema de archivos mediante IAM, asegúrese de que está utilizando la opción `-o iam` del comando `mount`. Esto indica al ayudante de montaje de EFS que pase sus credenciales al destino de montaje de EFS. Si sigue sin tener acceso, compruebe la política del sistema de archivos y la política de identidad para asegurarse de que no existen cláusulas DENY que se apliquen a la conexión y de que haya al menos una cláusula ALLOW que se aplique a la conexión. Para obtener más información, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#) y [Creación de políticas de sistema de archivos](#).

Se produce un error de montaje automático y la instancia no responde

Este problema puede ocurrir si el sistema de archivos se monta automáticamente en una instancia y la opción `_netdev` no se ha declarado. Si falta `_netdev`, la instancia EC2 puede dejar de responder. Este resultado se debe a que los sistemas de archivos de red se deben inicializar después de que la instancia de procesamiento inicia sus redes.

Acción que se debe ejecutar

Si se produce este problema, póngase en contacto con AWS Support.

Se produce un error de montaje de varios sistemas de archivos de Amazon EFS en /etc/fstab

En el caso de instancias que utilizan el sistema systemd init con dos o más entradas de Amazon EFS en /etc/fstab, puede haber ocasiones en que algunas o todas las entradas no se monten. En este caso, el resultado dmesg muestra una o varias líneas parecidas a lo siguiente.

```
NFS: nfs4_discover_server_trunking unhandled error -512. Exiting with error EIO
```

Acción que debe ejecutarse

En este caso, le recomendamos que cree un nuevo archivo de servicio systemd en /etc/systemd/system/mount-nfs-sequentially.service. El código que se debe incluir en el archivo depende de si monta los sistemas de archivos manualmente o utiliza el asistente de montaje de Amazon EFS.

- Si va a montar los sistemas de archivos manualmente, el comando ExecStart debe apuntar al Sistema de archivos de red (NFS4). Incluya el código siguiente en el archivo:

```
[Unit]
Description=Workaround for mounting NFS file systems sequentially at boot time
After=remote-fs.target

[Service]
Type=oneshot
ExecStart=/bin/mount -avt nfs4
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

- Si utiliza el asistente de montaje de Amazon EFS, el comando ExecStart debe apuntar a EFS en lugar de a NFS4 para usar seguridad de la capa de transporte (TLS) (TLS). Incluya el código siguiente en el archivo:

```
[Unit]
Description=Workaround for mounting NFS file systems sequentially at boot time
After=remote-fs.target

[Service]
```

```
Type=oneshot
ExecStart=/bin/mount -avt efs
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

Después de crear el archivo, ejecute los dos comandos siguientes:

1. `sudo systemctl daemon-reload`
2. `sudo systemctl enable mount-nfs-sequentially.service`

A continuación, reinicie la instancia de Amazon EC2. Los sistemas de archivos se montan bajo demanda, por lo general, en un plazo de un segundo.

El comando de montaje falla con el mensaje de error "wrong fs type"

El comando de montaje falla con el siguiente mensaje de error.

```
mount: wrong fs type, bad option, bad superblock on 10.1.25.30:/,
missing codepage or helper program, or other error (for several filesystems
(e.g. nfs, cifs) you might need a /sbin/mount.<type> helper program)
In some cases useful info is found in syslog - try dmesg | tail or so.
```

Acción que debe ejecutarse

Si recibe este mensaje, instale el paquete `nfs-utils` (o `nfs-common` en Ubuntu). Para obtener más información, consulte [Instalación del cliente NFS](#).

El comando de montaje falla con el mensaje de error "incorrect mount option"

El comando de montaje falla con el siguiente mensaje de error.

```
mount.nfs: an incorrect mount option was specified
```

Acción que debe ejecutarse

Este mensaje de error lo más probable es que signifique que su distribución de Linux no admite las versiones 4.0 y 4.1 de Network File System (NFSv4). Para confirmar si es el caso, puede ejecutar el siguiente comando.

```
$ grep CONFIG_NFS_V4_1 /boot/config*
```

Si el comando anterior devuelve `# CONFIG_NFS_V4_1 is not set`, NFSv4.1 no se admite en su distribución de Linux. Para obtener una lista de las Imágenes de máquina de Amazon (AMI) de Amazon Elastic Compute Cloud (Amazon EC2) que admiten NFSv4.1, consulte [Compatibilidad con NFS](#).

El montaje con un punto de acceso falla

El comando `mount` falla cuando se monta con un punto de acceso y aparece el siguiente mensaje de error:

```
mount.nfs4: mounting access_point failed, reason given by server: No such file or directory
```

Acción que debe ejecutarse

Este mensaje de error indica que la ruta EFS especificada no existe. Asegúrese de proporcionar la propiedad y los permisos del directorio raíz del punto de acceso. EFS no creará el directorio raíz sin esta información. Para obtener más información, consulte [Trabajo con puntos de acceso de Amazon EFS](#).

Si no especifica la propiedad ni los permisos del directorio raíz, y el directorio raíz aún no existe, EFS no creará el directorio raíz. Cuando esto suceda, los intentos de montar el sistema de archivos utilizando el punto de acceso producirán un error.

El montaje del sistema de archivos falla de inmediato después de la creación del sistema de archivos

Puede llevar hasta 90 segundos después de crear un destino de montaje hasta que los registros del servicio de nombres de dominio (DNS) se propaguen totalmente en una Región de AWS.

Acción que debe ejecutarse

Si va a crear y montar sistemas de archivos mediante programación, por ejemplo, con una AWS CloudFormation plantilla, le recomendamos que implemente una condición de espera.

El montaje del sistema de archivos deja de responder y, a continuación, falla con un error de tiempo de espera agotado

El comando de montaje del sistema de archivos deja de responder durante un minuto o dos y, a continuación, falla con un error de tiempo de espera agotado. En el siguiente código se muestra un ejemplo.

```
$ sudo mount -t nfs -o
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-ip:/ mnt

[2+ minute wait here]
mount.nfs: Connection timed out
$
```

Acción que ejecutar

Este error puede producirse porque la instancia de Amazon EC2 o los grupos de seguridad del destino de montaje no están configurados correctamente. Asegúrese de que el grupo de seguridad de destino de montaje tenga una regla de entrada que permita el acceso NFS desde el grupo de seguridad de EC2.

Type	Protocol	Port Range	Source	Description
NFS	TCP	2049	Custom	sg- XXXXXXXXXXXX e.g. SSH for Admin Desktop

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel **Save**

Para obtener más información, consulte [Creación de grupos de seguridad](#).

Compruebe que la dirección IP del destino de montaje que ha especificado es válida. Si especifica una dirección IP incorrecta y no hay nada más en esa dirección IP para rechazar el montaje, podría experimentar este problema.

El montaje del sistema de archivos con NFS que utiliza el nombre de DNS falla

Los intentos de montar un sistema de archivos mediante un cliente de NFS (no utilizando el cliente `amazon-efs-utils`) utilizando el nombre de DNS del sistema de archivos fallan, como se muestra en el siguiente ejemplo:

```
$ sudo mount -t nfs -o
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport file-
system-id.efs.aws-region.amazonaws.com:/ mnt
mount.nfs: Failed to resolve server file-system-id.efs.aws-region.amazonaws.com:
Name or service not known.

$
```

Acción que ejecutar

Compruebe la configuración de VPC. Si utiliza una VPC personalizada, asegúrese de que la configuración de DNS esté habilitada. Para obtener más información, consulte [Atributos de DNS para su VPC](#) en la Guía del usuario de Amazon VPC. Además, los nombres DNS del sistema de archivos y del destino del montaje no se pueden resolver desde fuera de la VPC donde se encuentran.

Antes de montar un sistema de archivos utilizando su nombre de DNS en el comando `mount`, debe hacer lo siguiente:

- Asegúrese de que haya un destino de montaje de Amazon EFS en la misma zona de disponibilidad que la instancia de Amazon EC2.
- Asegúrese de que haya un destino de montaje en la misma VPC que la instancia de Amazon EC2. De lo contrario, no se puede utilizar la resolución de nombres de DNS para los destinos de montaje de EFS que están en otra VPC. Para obtener más información, consulte [Montaje de sistemas de archivos EFS desde otro Cuenta de AWS o desde una VPC](#).
- Conecte su instancia de Amazon EC2 dentro de una Amazon VPC configurada para utilizar el servidor DNS proporcionado por Amazon. Para obtener más información, consulte [Conjuntos de opciones de DHCP](#) en la Guía del usuario de Amazon VPC.
- Asegúrese de que la Amazon VPC de la instancia de Amazon EC2 de conexión tiene los nombres de host DNS habilitados. Para obtener más información, consulte [Atributos de DNS para su VPC](#) en la Guía del usuario de Amazon VPC.

El montaje del sistema de archivos falla y emite el mensaje "nfs not responding (nfs no responde)"

Un montaje del sistema de archivos de Amazon EFS falla en un evento de reconexión del protocolo de control de transmisión (TCP) con "nfs: server_name still not responding".

Acción que ejecutar

Utilice la opción de montaje `noresvport` para asegurarse de que el cliente NFS utiliza un nuevo puerto de origen de TCP cuando se restablece la conexión a la red. Esto ayuda a garantizar la disponibilidad ininterrumpida después de un evento de recuperación de red.

El estado de ciclo de vida de destino de montaje está atascado

El estado del ciclo de vida del destino de montaje está bloqueado en el estado `creating` (creación) o `deleting` (eliminación).

Acción que debe ejecutarse

Vuelva a intentar la llamada `CreateMountTarget` o `DeleteMountTarget`.

El estado del ciclo de vida objetivo del montaje muestra un error

El estado del ciclo de vida del destino de montaje se muestra como error.

Acción que ejecutar

Amazon EFS no puede crear los registros del Sistema de nombres de dominio (DNS) necesarios para los nuevos destinos de montaje del sistema de archivos si la nube privada virtual (VPC) tiene zonas alojadas en conflicto. Amazon EFS no puede crear nuevos registros en una zona alojada propiedad del cliente. Si necesita mantener una zona alojada con un rango de DNS de `efs.<region>.amazonaws.com` conflictivo, cree la zona alojada en una VPC independiente. Para obtener más información sobre las consideraciones de DNS para la VPC, consulte [Atributos de DNS para su VPC](#).

Para solucionar este problema, elimine el host de `efs.<region>.amazonaws.com` en conflicto de la VPC y vuelva a crear el destino de montaje. Para obtener más información sobre la creación de destinos de montaje, consulte [Administrar destinos de montaje](#).

El montaje no responde

Parece que un montaje de Amazon EFS deja de responder. Por ejemplo, comandos como `ls` dejan de responder.

Acción que ejecutar

Este error se produce si otra aplicación está escribiendo grandes cantidades de datos en el sistema de archivos. El acceso a los archivos que se están escribiendo podría bloquearse hasta que se haya completado la operación. En general, cualquier comando o aplicación que intenta acceder a archivos que se están escribiendo podría parecer que ha dejado de responder. Por ejemplo, el comando `ls` podría dejar de responder cuando llega al archivo que se está escribiendo. Este resultado se debe a que algunas distribuciones de Linux especifican como alias el comando `ls` para que recupere atributos de archivos, además de mostrar el contenido del directorio.

Para solucionar este problema, compruebe que otra aplicación está escribiendo archivos en el montaje de Amazon EFS y que está en el estado `Uninterruptible sleep (D)`, como en el siguiente ejemplo:

```
$ ps aux | grep large_io.py
root 33253 0.5 0.0 126652 5020 pts/3 D+ 18:22 0:00 python large_io.py /efs/large_file
```

Una vez que haya verificado que este es el caso, puede tratar la cuestión esperando a que la otra operación de escritura se complete o implementando una alternativa. En el ejemplo de `ls`, puede utilizar el comando `/bin/ls` directamente, en lugar de un alias. Esto permite que el comando continúe sin que el archivo que se está escribiendo deje de responder. En general, si la aplicación que escribe los datos puede forzar un vaciado de datos de forma periódica, quizás el uso de `fsync(2)` podría ayudar a mejorar la capacidad de respuesta del sistema de archivos para otras aplicaciones. No obstante, esta mejora podría ser a costa de desempeño cuando la aplicación escribe datos.

El cliente montado se desconecta

En ocasiones, un cliente montado en un sistema de archivos de Amazon EFS puede desconectarse debido a diversas causas. Los clientes NFS están diseñados para volver a conectarse automáticamente en caso de interrupción a fin de minimizar el impacto de las desconexiones rutinarias en el rendimiento y la disponibilidad de las aplicaciones. En la mayoría de los casos, los clientes se vuelven a conectar de forma transparente en cuestión de segundos.

Sin embargo, el software de cliente NFS incluido en las versiones anteriores del núcleo de Linux (versiones 5.4 y anteriores) presenta un comportamiento que provoca que los clientes NFS, al desconectarse, intenten volver a conectarse en el mismo puerto de origen TCP. Este comportamiento no cumple con la RFC de TCP y puede impedir que estos clientes restablezcan rápidamente las conexiones con su servidor NFS (en este caso, un sistema de archivos EFS).

Para resolver este problema, le recomendamos encarecidamente que utilice el asistente de montaje de Amazon EFS para montar los sistemas de archivos EFS. El asistente de montaje de EFS utiliza una configuración de montaje optimizada para los sistemas de archivos de Amazon EFS. Para obtener más información sobre el ayudante de montaje y el cliente de EFS, consulte [Instalación de las herramientas de Amazon EFS](#).

Si no puede utilizar el asistente de montaje de EFS, le recomendamos encarecidamente que utilice la opción de montaje `noresvport` de NFS, que indica a los clientes NFS que restablezcan las conexiones mediante nuevos puertos de origen TCP para evitar este problema. Para obtener más información, consulte [Opciones recomendadas de montaje NFS](#).

Las operaciones en el sistema de archivos recién montado devuelven el error "bad file handle"

Las operaciones realizadas en un sistema de archivos recién montado devuelven un error `bad file handle`.

Este error puede ocurrir si una instancia de Amazon EC2 se ha conectado a un sistema de archivos y un destino de montaje con una dirección IP especificada y, a continuación, dicho sistema de archivos y el destino de montaje se han eliminado. Si crea un nuevo sistema de archivos y destino de montaje para conectarse a esa instancia de Amazon EC2 con la misma dirección IP del destino de montaje, puede producirse este problema.

Acción que debe ejecutarse

Puede resolver este error desmontando el sistema de archivos y, a continuación, volviendo a montar el sistema de archivos en la instancia de Amazon EC2. Para obtener más información sobre el desmontaje de su sistema de archivos de Amazon EFS, consulte [Desmontaje de sistemas de archivos](#).

Error de desmontaje de un sistema de archivos

Si el sistema de archivos está ocupado, no puede desmontarlo.

Acción que debe ejecutarse

Puede resolver este problema de las siguientes maneras:

- Utilice el modo lazy unmount, `umount -l` que separa el sistema de archivos de la jerarquía del sistema de archivos al ejecutarlo y, a continuación, limpia todas las referencias al sistema de archivos en cuanto deja de estar ocupado.
- Espere a que todas las operaciones de lectura y escritura terminen y, a continuación, intente de nuevo el comando `umount`.
- Fuerce un desmontaje con el comando `umount -f`.

Warning

Si se fuerza un desmontaje se interrumpen las operaciones de lectura o escritura de datos que se encuentran actualmente en curso para el sistema de archivos. Consulte la [página de `umount man`](#) para obtener más información y orientación sobre el uso de esta opción.

Transferencia de datos a Amazon EFS

Puede usar AWS Transfer Family y transferir datos AWS DataSync a sus sistemas de archivos Amazon EFS. AWS DataSync es un servicio de transferencia de datos en línea que puede copiar datos entre el Network File System (NFS), los servidores de archivos Server Message Block (SMB), el almacenamiento de objetos autogestionado y también entre servicios. AWS Para obtener más información sobre el uso DataSync con Amazon EFS, consulte [AWS DataSync Utilización para transferir datos a Amazon EFS](#).

AWS Transfer Family es un AWS servicio totalmente gestionado que puede utilizar para transferir archivos a y desde los sistemas de archivos de Amazon EFS a través del Protocolo seguro de transferencia de archivos (SFTP), el Protocolo de transferencia de archivos (FTP) y el FTP a través del protocolo Secure Sockets Layer (FTPS). Con Transfer Family, puede proporcionar a sus socios comerciales acceso a los archivos almacenados en sus sistemas de archivos de Amazon EFS para casos de uso como la distribución de datos, la cadena de suministro, la administración de contenido y las aplicaciones de servidor web. Para obtener más información acerca del uso de Transfer Family con Amazon EFS, consulte [AWS Transfer Family Utilización para transferir datos a Amazon EFS](#).

Temas

- [AWS DataSync Utilización para transferir datos a Amazon EFS](#)
- [AWS Transfer Family Utilización para transferir datos a Amazon EFS](#)

AWS DataSync Utilización para transferir datos a Amazon EFS

AWS DataSync es un servicio de transferencia de datos en línea que simplifica, automatiza y acelera el traslado y la replicación de datos entre sistemas de almacenamiento locales y también entre servicios de almacenamiento. AWS DataSync puede copiar datos entre el Network File System (NFS), los servidores de archivos Server Message Block (SMB), el almacenamiento de objetos autogestionado, los buckets de Amazon AWS Snowcone S3, los sistemas de archivos Amazon EFS y los sistemas de archivos FSx for Windows File Server.

También se puede utilizar DataSync para transferir archivos entre dos sistemas de archivos EFS, incluidos los sistemas de archivos de diferentes sistemas de archivos y Región de AWS los sistemas de archivos que pertenecen a diferentes Cuenta de AWS sistemas de archivos. Al DataSync copiar datos entre sistemas de archivos EFS, puede realizar migraciones de datos únicas, ingesta

periódica de datos para cargas de trabajo distribuidas y automatizar la replicación para la protección y recuperación de datos.

Para obtener más información, consulte [Introducción a Amazon Elastic File System](#) y la [Guía del usuario de AWS DataSync](#).

AWS Transfer Family Utilización para transferir datos a Amazon EFS

AWS Transfer Family es un AWS servicio totalmente gestionado que puede utilizar para transferir archivos a y desde los sistemas de archivos de Amazon EFS mediante los siguientes protocolos:

- Secure Shell (SSH) File Transfer Protocol (SFTP) (AWS Transfer for SFTP)
- Protocolo seguro de transferencia de archivos (FTPS) (AWS Transfer for FTPS)
- Protocolo de File Transfer (FTP) (AWS Transfer for FTP)

Con Transfer Family, puede permitir de forma segura que terceros, como sus proveedores, socios o clientes, accedan a sus archivos a través de los protocolos compatibles a escala mundial, sin necesidad de administrar ninguna infraestructura. Además, ahora puede acceder fácilmente a sus sistemas de archivos de EFS desde entornos Windows, macOS y Linux mediante clientes SFTP, FTPS y FTP. Esto ayuda a ampliar la accesibilidad de sus datos más allá de los clientes y puntos de acceso NFS, a los usuarios de varios entornos.

El uso de Transfer Family para transferir datos en los sistemas de archivos de Amazon EFS se contabiliza de la misma manera que el uso de otros clientes. Para obtener más información, consulte [Modos de rendimiento](#) y [Cuotas de Amazon EFS](#).

Para obtener más información AWS Transfer Family, consulte la [Guía AWS Transfer Family del usuario](#).

Note

El uso de Transfer Family con Amazon Cuenta de AWS EFS está desactivado de forma predeterminada para los sistemas de archivos Amazon EFS con políticas que permiten el acceso público que se crearon antes del 6 de enero de 2021. Para permitir el uso de Transfer Family para acceder a su sistema de archivos, póngase en contacto con AWS Support.

Temas

- [Requisitos previos para su uso AWS Transfer Family con Amazon EFS](#)
- [Configuración del sistema de archivos Amazon EFS para que funcione con AWS Transfer Family](#)

Requisitos previos para su uso AWS Transfer Family con Amazon EFS

Para utilizar Transfer Family para acceder a los archivos de su sistema de archivos Amazon EFS, la configuración debe cumplir las siguientes condiciones:

- El servidor Transfer Family y su sistema de archivos de Amazon EFS se encuentran en la misma Región de AWS.
- Las políticas de IAM se configuran para permitir el acceso al rol de IAM utilizado por Transfer Family. Para obtener más información, consulte [Creación de un rol y política de IAM](#) en la AWS Transfer Family Guía del usuario de .
- (Opcional) Si el servidor Transfer Family es propiedad de una cuenta diferente, habilite el acceso entre cuentas.
 - Asegúrese de que la política de su sistema de archivos no permita el acceso público. Para obtener más información, consulte [Bloqueo del acceso público a los sistemas de archivos de Amazon EFS](#).
 - Modifique la política del sistema de archivos para permitir el acceso entre cuentas. Para obtener más información, consulte [Configuración del acceso entre cuentas para Transfer Family](#).

Configuración del sistema de archivos Amazon EFS para que funcione con AWS Transfer Family

La configuración de un sistema de archivos de Amazon EFS para que funcione con Transfer Family requiere los siguientes pasos:

- Paso 1. Obtenga la lista de ID POSIX que se asignan a los usuarios de Transfer Family.
- Paso 2. Asegúrese de que los usuarios de Transfer Family puedan acceder a los directorios de su sistema de archivos mediante los ID POSIX asignados a los usuarios de Transfer Family.
- Paso 3. Configure IAM para permitir el acceso al rol de IAM utilizado por Transfer Family.

Configuración de permisos de archivos y directorios para los usuarios de Transfer Family

Asegúrese de que los usuarios de Transfer Family tengan acceso a los archivos y directorios necesarios del sistema de archivos EFS. Asigne permisos de acceso al directorio utilizando la lista de ID POSIX asignada a los usuarios de Transfer Family. En este ejemplo, un usuario crea un directorio denominado `transferFam` bajo el punto de montaje de EFS. La creación de un directorio es opcional en función de su caso de uso. Si es necesario, puede elegir su nombre y ubicación en el sistema de archivos EFS.

Para asignar permisos de archivos y directorios a los usuarios de POSIX para Transfer Family

1. Conéctese a la instancia de Amazon EC2. Amazon EFS solo admite el montaje mediante instancias de EC2 basadas en Linux.
2. Monte el sistema de archivos de EFS si aún no está montado en la instancia de EC2. Para obtener más información, consulte [Montaje de sistemas de archivos de EFS](#).
3. El siguiente ejemplo crea el directorio en el sistema de archivos de EFS y cambia su grupo por el ID de grupo POSIX para los usuarios de Transfer Family, que es 1101 en este ejemplo.
 - a. Ejecute los siguientes comandos para crear el directorio `efs/transferFam`. En la práctica, puede utilizar un nombre y una ubicación en el sistema de archivos que desee.

```
[ec2-user@ip-192-0-2-0 ~]$ ls
efs  efs-mount-point  efs-mount-point2
[ec2-user@ip-192-0-2-0 ~]$ ls efs
[ec2-user@ip-192-0-2-0 ~]$ sudo mkdir efs/transferFam
[ec2-user@ip-192-0-2-0 ~]$ ls -l efs
total 0
drwxr-xr-x 2 root root 6 Jan  6 15:58 transferFam
```

- b. Utilice el siguiente comando para cambiar el grupo de `efs/transferFam` al GID POSIX asignado a los usuarios de Transfer Family.

```
[ec2-user@ip-192-0-2-0 ~]$ sudo chown :1101 efs/transferFam/
```

- c. Confirme el cambio.

```
[ec2-user@ip-192-0-2-0 ~]$ ls -l efs
total 0
```

```
drwxr-xr-x 2 root 1101 6 Jan  6 15:58 transferFam
```

Habilitar el acceso al rol de IAM utilizado por Transfer Family

En Transfer Family, se crea una política de IAM basada en recursos y un rol de IAM que define el acceso de los usuarios al sistema de archivos de EFS. Para obtener más información, consulte [Creación de un rol y política de IAM](#) en la Guía del usuario de AWS Transfer Family . Debe conceder a ese rol de IAM de Transfer Family acceso a su sistema de archivos de EFS mediante una política de identidad de IAM o una política de sistema de archivos.

A continuación se muestra un ejemplo de una política del sistema de archivos que concede ClientMount (lectura) y ClientWrite accede al rol de IAM EFS-role-for-transfer.

```
{
  "Version": "2012-10-17",
  "Id": "efs-policy-wizard-8698b356-4212-4d30-901e-ad2030b57762",
  "Statement": [
    {
      "Sid": "Grant-transfer-role-access",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/EFS-role-for-transfer"
      },
      "Action": [
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientMount"
      ]
    }
  ]
}
```

Para obtener más información sobre la creación de una política de sistema de archivos, consulte [Creación de políticas de sistema de archivos](#). Para obtener más información acerca del uso de las políticas de IAM basadas en identidades para administrar el acceso a recursos de EFS, consulte [Políticas de Amazon EFS basadas en identidades](#).

Configuración del acceso entre cuentas para Transfer Family

Si el servidor Transfer Family utilizado para acceder a su sistema de archivos pertenece a otro Cuenta de AWS, debe conceder a esa cuenta acceso a su sistema de archivos. Además, la política

del sistema de archivos no debe ser pública. Para obtener más información acerca del bloqueo del acceso público al sistema de archivos, consulte [Bloqueo del acceso público a los sistemas de archivos de Amazon EFS](#).

Puede conceder un Cuenta de AWS acceso diferente a su sistema de archivos en la política del sistema de archivos. En la consola de Amazon EFS, utilice la sección Otorgar permisos adicionales del editor de políticas del sistema de archivos para especificar el Cuenta de AWS nivel de acceso al sistema de archivos que va a conceder. Para obtener más información sobre la creación o edición de una política de sistema de archivos, consulte [Creación de políticas de sistema de archivos](#).

Puede especificar la cuenta mediante el ID de cuenta o el Nombre de recurso de Amazon (ARN) de la cuenta. Para obtener más información sobre los ARN, consulte [ARN de IAM](#) en la Guía del usuario de IAM.

El siguiente ejemplo es una política de sistema de archivos no pública que permite el acceso entre cuentas al sistema de archivos. Tiene las dos instrucciones siguientes:

1. La primera instrucción, `NFS-client-read-write-via-fsmt`, otorga privilegios de lectura, escritura y raíz a los clientes NFS que acceden al sistema de archivos mediante un destino de montaje del sistema de archivos.
2. La segunda declaración, `Grant-cross-account-access`, solo otorga privilegios de lectura y escritura a Cuenta de AWS 111122223333, que es la cuenta propietaria del servidor Transfer Family que necesita acceder al sistema de archivos EFS de su cuenta.

```
{
  "Statement": [
    {
      "Sid": "NFS-client-read-write-via-fsmt",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientMount"
      ],
      "Condition": {
        "Bool": {
          "elasticfilesystem:AccessedViaMountTarget": "true"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "Grant-cross-account-access",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
      "elasticfilesystem:ClientWrite",
      "elasticfilesystem:ClientMount"
    ]
  }
]
}

```

La siguiente política del sistema de archivos añade una declaración que concede el acceso al rol de IAM utilizado por Transfer Family.

```

{
  "Statement": [
    {
      "Sid": "NFS-client-read-write-via-fsmt",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientMount"
      ],
      "Condition": {
        "Bool": {
          "elasticfilesystem:AccessedViaMountTarget": "true"
        }
      }
    },
    {
      "Sid": "Grant-cross-account-access",
      "Effect": "Allow",
      "Principal": {

```

```
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientMount"
    ]
},
{
    "Sid": "Grant-transfer-role-access",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/EFS-role-for-transfer"
    },
    "Action": [
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientMount"
    ]
}
]
```

Gestión de sistemas de archivos de Amazon EFS

Las tareas de gestión de sistema de archivos hacen referencia a la creación y la eliminación de sistemas de archivos, a la gestión de etiquetas, y a la gestión de la accesibilidad de la red, el acceso y las copias de seguridad de un sistema de archivos.

Puede realizar estas tareas de administración del sistema de archivos mediante AWS Command Line Interface (AWS CLI) o la API AWS Management Console, o mediante programación, como se explica en las siguientes secciones.

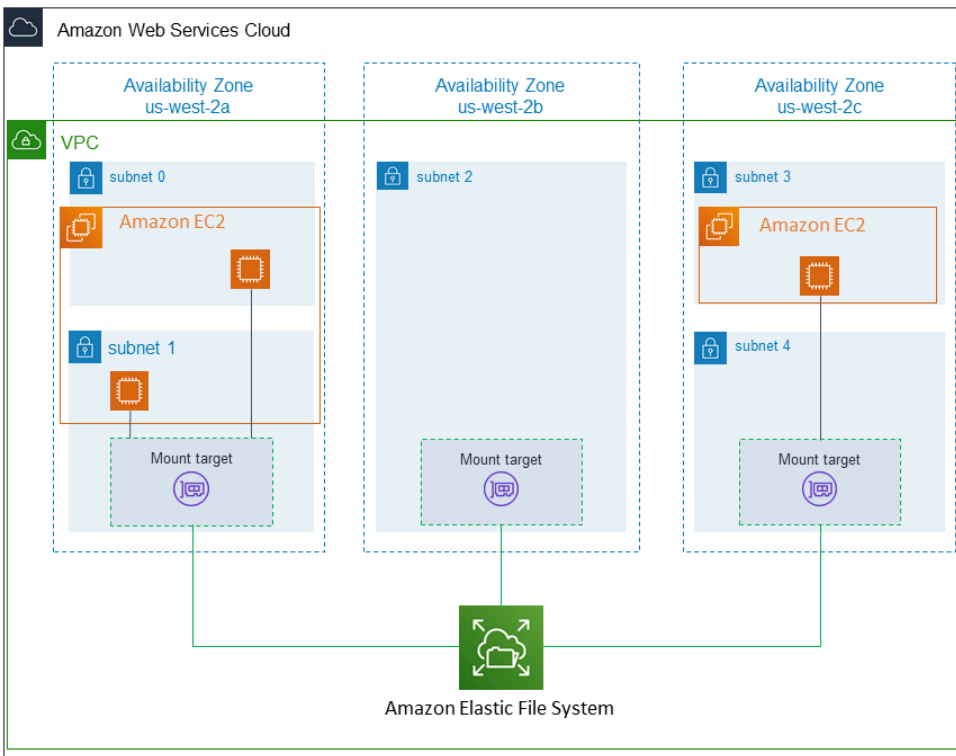
Temas

- [Gestión de la accesibilidad de red del sistema de archivos](#)
- [Administrar el rendimiento del sistema de archivos](#)
- [Administrar el almacenamiento del sistema de archivos](#)
- [Administración del acceso a los sistemas de archivos cifrados](#)
- [Medición: cómo Amazon EFS registra el tamaño del sistema de archivos y el tamaño de los objetos](#)
- [Administración de los costos del sistema de archivos Amazon EFS mediante AWS Budgets](#)
- [Estado del sistema de archivos](#)

Gestión de la accesibilidad de red del sistema de archivos

El sistema de archivos se monta en Amazon EC2 o en otra instancia AWS informática de la nube privada virtual (VPC) mediante un destino de montaje que se crea para el sistema de archivos. La gestión de la accesibilidad de red del sistema de archivos se refiere a la gestión de los destinos de montaje de un sistema de archivos.

La siguiente ilustración muestra cómo las instancias de EC2 en una VPC acceden a un sistema de archivos de Amazon EFS mediante un destino de montaje.



La ilustración muestra tres instancias de EC2 lanzadas en diferentes subredes de VPC que acceden a un sistema de archivos de Amazon EFS. El ejemplo también muestra un destino de montaje en cada una de las zonas de disponibilidad (independientemente del número de subredes en cada zona de disponibilidad).

Puede crear solo un destino de montaje por zona de disponibilidad. Si una zona de disponibilidad tiene varias subredes, tal y como se muestra en una de las zonas de la ilustración, puede crear un destino de montaje en tan solo una de las subredes. Siempre que tenga un destino de montaje en una zona de disponibilidad, las instancias EC2 lanzadas en cualquiera de sus subredes pueden compartir el mismo destino de montaje.

La gestión de destinos de montaje hace referencia a estas actividades:

- Creación y eliminación de destinos de montaje en una VPC: como mínimo, debe crear un destino de montaje en cada zona de disponibilidad desde la que desea acceder al sistema de archivos.
- Actualización de la configuración de destino de montaje: al crear un destino de montaje, asocia los grupos de seguridad con el destino de montaje. Un grupo de seguridad funciona como un firewall virtual que controla el tráfico hacia y desde el destino de montaje. Puede añadir reglas de entrada para controlar el acceso al destino de montaje y, por lo tanto, al sistema de archivos. Después de

crear un destino de montaje, es posible que desee modificar los grupos de seguridad asignados a ellos.

En las secciones siguientes se incluye información sobre la gestión de la accesibilidad de red de su sistema de archivos.

Temas

- [Creación o eliminación de destinos de montaje en una VPC](#)
- [Cambio de la VPC para el destino de montaje](#)
- [Actualización de la configuración de destinos de montaje](#)

Creación o eliminación de destinos de montaje en una VPC

Para acceder a un sistema de archivos de Amazon EFS en una VPC, necesita destinos de montaje. En el caso de un sistema de archivos de Amazon EFS, se cumple lo siguiente:

- Puede crear un destino de montaje en cada zona de disponibilidad.
- Si la VPC tiene varias subredes en una zona de disponibilidad, puede crear un destino de montaje en tan solo una de las subredes. Todas las instancias EC2 en la zona de disponibilidad pueden compartir el destino de montaje.

Note

Le recomendamos crear un destino de montaje en cada una de las zonas de disponibilidad. Existen consideraciones de costos para montar un sistema de archivos en una instancia EC2 en una zona de disponibilidad a través de un destino de montaje creado en otra zona de disponibilidad. Para obtener más información, consulte [Amazon EFS](#). Además, usando siempre un destino de montaje local en la zona de disponibilidad de la instancia, elimina un escenario de error parcial. Si la zona del destino de montaje deja de funcionar, no tendrá acceso a su sistema de archivos a través de dicho destino de montaje.

Si elimina un destino de montaje, la operación rompe de manera forzada los montajes del sistema de archivos, lo que podría afectar a las instancias o a las aplicaciones que utilizan dichos montajes. Para evitar la interrupción de la aplicación, detenga las aplicaciones y desmonte el sistema de

archivos antes de eliminar el destino de montaje. Para obtener más información, consulte [Administrar destinos de montaje](#).

Note

Antes de eliminar un destino de montaje, desmonte primero el sistema de archivos. Para obtener más información, consulte [Desmontaje de sistemas de archivos](#).

Puede utilizar un sistema de archivos solo en una VPC a la vez. Es decir, puede crear destinos de montaje para el sistema de archivos en una VPC a la vez. Si desea acceder al sistema de archivos desde otra VPC, elimine en primer lugar los destinos de montaje de la VPC actual. A continuación, cree nuevos destinos de montaje en otra VPC.

Con la AWS Management Console AWS CLI, la y la API, puede crear y gestionar los objetivos de montaje en los sistemas de archivos. Para los destinos de montaje existentes, puede añadir y eliminar grupos de seguridad o eliminar el destino de montaje. Para obtener más información, consulte [Administrar destinos de montaje](#).

Cambio de la VPC para el destino de montaje

Puede utilizar un sistema de archivos de Amazon EFS en una VPC basada en el servicio de Amazon VPC a la vez. Es decir, que puede crear destinos de montaje en una VPC para su sistema de archivos y utilizar dichos destinos de montaje para proporcionar acceso al sistema de archivos.

Puede montar el sistema de archivos de Amazon EFS desde estos destinos:

- Las instancias de Amazon EC2 de la misma VPC
- Instancias EC2 en una VPC conectada por interconexión con VPC
- Servidores locales mediante AWS Direct Connect
- Servidores locales a través de una red privada AWS virtual (VPN) mediante Amazon VPC

Una interconexión de VPC es una conexión de redes entre dos VPC que permite direccionar el tráfico entre ellas. La conexión puede utilizar direcciones Internet Protocol versión 4 (IPv4) o versión 6 (IPv6). Para obtener más información sobre el funcionamiento de Amazon EFS y la interconexión con VPC, consulte [Montaje de sistemas de archivos EFS desde otro Cuenta de AWS o desde una VPC](#).

Para acceder al sistema de archivos desde instancias de EC2 en otra VPC, debe:

- Eliminar los destinos de montaje actuales.
- Cambiar la VPC.
- Crear nuevos destinos de montaje.

Para obtener más información sobre cómo realizar estos pasos en el AWS Management Console, consulte [Para cambiar la VPC de un sistema de archivos de Amazon EFS \(consola\)](#)

Uso de la CLI

Para utilizar un sistema de archivos en otra VPC, elimine primero todos los destinos de montaje que haya creado anteriormente en la VPC. A continuación, cree nuevos destinos de montaje en otra VPC. Para comandos de la AWS CLI de ejemplo, consulte [Administrar los objetivos de montaje \(CLI\)](#).

Actualización de la configuración de destinos de montaje

Después de crear un destino de montaje para su sistema de archivos, puede que desee actualizar los grupos de seguridad que están en vigor. No puede cambiar la dirección IP de un destino de montaje existente. Para cambiar la dirección IP, elimine el destino de montaje y cree uno nuevo con la nueva dirección. La eliminación de un destino de montaje rompe todos los montajes existentes del sistema de archivos.

Note

Antes de eliminar un destino de montaje, desmonte primero el sistema de archivos.

Cada destino de montaje también tiene una dirección IP. Al crear un destino de montaje, puede elegir una dirección IP desde la subred donde coloca el destino de montaje. Si omite un valor, Amazon EFS selecciona una dirección IP no utilizada desde dicha subred.

No hay ninguna operación de Amazon EFS para cambiar la dirección IP después de crear un destino de montaje. Por lo tanto, no puede cambiar la dirección IP mediante programación ni utilizando la AWS CLI. Sin embargo, la consola le permite cambiar la dirección IP. Entre bambalinas, la consola elimina el destino de montaje y vuelve a crearlo de nuevo.

⚠ Warning

Si cambia la dirección IP de un destino de montaje, se rompen los montajes de sistema de archivos existentes y tendrá que volver a montar el sistema de archivos.

Ninguno de los cambios de configuración en la accesibilidad de red al sistema de archivos afecta al propio sistema de archivos. El sistema de archivos y los datos se conservan.

Modificación de un grupo de seguridad

Los grupos de seguridad definen el acceso de entrada y salida. Al cambiar los grupos de seguridad asociados a un destino de montaje, asegúrese de autorizar el acceso de entrada y salida necesario. Esto permite que la instancia EC2 se comunice con el sistema de archivos.

Para obtener más información sobre los grupos de seguridad, consulte los [grupos de seguridad de Amazon EC2 para instancias de Linux](#) en la Guía del usuario de Amazon EC2.

Para modificar el grupo de seguridad de un destino de montaje, consulte [Administrar destinos de montaje](#).


Administrar el rendimiento del sistema de archivos

Elastic es el modo de rendimiento predeterminado y se recomienda para la mayoría de los casos de uso. Con rendimiento elástico, este se escala hacia arriba o hacia abajo para satisfacer las necesidades de la actividad de la carga de trabajo. Sin embargo, si conoce los patrones de acceso específicos de sus cargas de trabajo (incluidas las necesidades de rendimiento, latencia y almacenamiento), puede optar por cambiar el modo de rendimiento.

Otros modos de rendimiento que puede elegir incluyen:

- Rendimiento provisionado: se especifica un nivel de rendimiento que el sistema de archivos puede impulsar independientemente del tamaño del sistema de archivos o del saldo de crédito de ráfaga.
- Rendimiento por ráfagas: el rendimiento se amplía con la cantidad de almacenamiento del sistema de archivos y permite ráfagas a niveles superiores durante un máximo de 12 horas al día.

Para obtener más información sobre los modos de rendimiento de Amazon EFS, consulte [Modos de rendimiento](#).

 Note


Puede cambiar el modo de rendimiento y la cantidad de rendimiento aprovisionada una vez que el sistema de archivos esté disponible. Sin embargo, cada vez que cambie el sistema de archivos a rendimiento aprovisionado o aumente la cantidad de rendimiento aprovisionada, debe esperar al menos 24 horas antes de poder volver a cambiar el modo de rendimiento o reducir la cantidad aprovisionada.

Puede administrar el modo de rendimiento del sistema de archivos mediante la consola de Amazon EFS, AWS Command Line Interface (AWS CLI) y la API de Amazon EFS.

Para administrar el rendimiento del sistema de archivos (consola)

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. En el panel de navegación izquierdo, elija Sistemas de archivos para ver la lista de sistemas de archivos de EFS de su cuenta.
3. Elija el sistema de archivos cuyo modo de rendimiento desea cambiar.
4. En la página de detalles del sistema de archivos, en la sección General, elija Editar. Aparece la página Editar.
5. Modifique el ajuste del modo de rendimiento.
 - Para usar rendimiento elástico o aprovisionado, seleccione Mejorado y luego seleccione Elástico o Aprovisionado.

Si elige el modo Aprovisionado, en Rendimiento aprovisionado (MIB/s), introduzca la cantidad de rendimiento que se va a aprovisionar para las solicitudes del sistema de archivos. La cantidad de Rendimiento máximo de lectura se muestra tres veces mayor que la cantidad de rendimiento que introduzca. Los sistemas de archivos de EFS miden las solicitudes de lectura a un tercio de la velocidad de otras solicitudes. Tras entrar en el modo de rendimiento, se muestra una estimación del coste mensual del sistema de archivos.

 Note

Puede cambiar el modo de rendimiento y la cantidad de rendimiento aprovisionada una vez que el sistema de archivos esté disponible. Sin embargo, cada vez que cambie el rendimiento del sistema de archivos a aprovisionado o aumente la cantidad

de rendimiento aprovisionada, debe esperar al menos 24 horas antes de poder volver a cambiar el modo de rendimiento o reducir la cantidad aprovisionada.

- Para utilizar el modo Rendimiento de ráfaga, seleccione Ráfaga.

Para obtener más información sobre cómo elegir el modo de rendimiento correcto para sus necesidades de rendimiento, consulte [Modos de rendimiento](#).

6. Para implementar los cambios, elija Guardar cambios.

Para administrar el rendimiento del sistema de archivos (CLI)

- Utilice el comando [update-file-system](#) de la CLI o la acción [UpdateFileSystem](#) de la API para cambiar el modo de rendimiento de un sistema de archivos.

Administrar el almacenamiento del sistema de archivos

Para administrar sus sistemas de archivos de manera que se almacenen de forma rentable durante todo su ciclo de vida, utilice la administración del ciclo de vida para transferir automáticamente los datos entre las clases de almacenamiento de acuerdo con la configuración del ciclo de vida definida para el sistema de archivos. La configuración del ciclo de vida es un conjunto de políticas de ciclo de vida que definen cuándo hacer la transición de los datos del sistema de archivos a otra clase de almacenamiento.

Políticas de ciclo de vida

Las políticas de ciclo de vida indican a la administración del ciclo de vida cuándo realizar la transición de los archivos a las clases de almacenamiento EFS Infrequent Access (IA) y EFS Archive. El tiempo de transición se basa en la fecha en que se accedió por última vez a los archivos en la clase de almacenamiento Estándar. Las políticas de ciclo de vida se aplican a todo el sistema de archivos de EFS.

Las políticas del ciclo de vida de EFS son:

- Transición a IA: indica a la administración del ciclo de vida cuándo mover los archivos al almacenamiento de acceso poco frecuente, lo que optimiza los costos para los datos a los que se accede solo unas pocas veces cada trimestre. De forma predeterminada, los archivos a los que no se accede en el almacenamiento Estándar durante 30 días se transfieren a IA.

- **Transición al archivado:** indica a la administración del ciclo de vida cuándo mover los archivos a la clase de almacenamiento archivado, que optimiza los costos para los datos a los que se accede solo unas pocas veces al año o menos. De forma predeterminada, los archivos a los que no se accede en el almacenamiento Estándar durante 90 días se transfieren a Archivado.
- **Transición al estándar:** indica a la administración del ciclo de vida si debe pasar los archivos de IA o archivado y devolverlos al almacenamiento estándar, que proporciona latencias de lectura de menos de milisegundos para los datos a los que se accede con frecuencia. De forma predeterminada, los archivos no se devuelven al almacenamiento Estándar y permanecen en la clase de almacenamiento IA o Archivado. Para los casos de uso sensibles al rendimiento y que exigen el rendimiento de latencia más rápido (como las aplicaciones que funcionan con un gran volumen de archivos pequeños), opte por la transición de los archivos al almacenamiento Estándar en primer acceso.

Para obtener más información sobre configuración de las políticas del ciclo de vida de un sistema de archivos, consulte [Administrar políticas del ciclo de vida de un sistema de archivos](#).

Para determinar la hora de último acceso en la clase de almacenamiento Estándar, un temporizador interno registra el momento del último acceso a un archivo (no los atributos del sistema de archivos POSIX que se pueden ver públicamente). Cada vez que se accede a un archivo en Standard, se restablece el temporizador de administración del ciclo de vida. Una vez que la administración del ciclo de vida traslada un archivo a las clases de almacenamiento IA o Archive, el archivo permanece allí indefinidamente, a menos que se establezca la política de transición a la estándar, que indica a la administración del ciclo de vida que devuelva los archivos a la categoría Estándar cuando se acceda a ella.

Las operaciones de metadatos, como enumerar el contenido de un directorio, no cuentan como acceso a archivos. Durante el proceso de mover el contenido de un archivo al almacenamiento IA o Archivado, el archivo se almacena en la clase de almacenamiento Estándar y se factura a esa tarifa de almacenamiento.

Operaciones del sistema de archivos para la administración del ciclo de vida

Las operaciones del sistema de archivos de administración del ciclo de vida tienen una prioridad menor que las de las cargas de trabajo del sistema de archivos de EFS. El tiempo necesario para mover archivos a la clase de almacenamiento IA y Archivado varía en función del tamaño del archivo y de la carga de trabajo del sistema de archivos.

Los metadatos de archivos, incluidos los nombres de archivo, la información de propiedad y la estructura de directorios del sistema de archivos, se almacenan siempre en Estándar para garantizar un rendimiento coherente de los metadatos. Todas las operaciones de escritura en archivos de las clases de almacenamiento IA o Archivado del sistema de archivos se escriben primero en las clases de almacenamiento Estándar y, después, son aptas para pasar a la clase de almacenamiento correspondiente después de 24 horas.

Administrar políticas del ciclo de vida de un sistema de archivos

Al crear un sistema de archivos Amazon EFS que utiliza la configuración recomendada por el servicio mediante la AWS Management Console, las políticas de ciclo de vida del sistema de archivos utilizan la siguiente configuración predeterminada:

- La transición hacia el IA se establece en 30 días desde el último acceso.
- La transición hacia Archivado se establece en 90 días desde el último acceso.
- Transición a Estándar se establece en Ninguna.

Para obtener más información acerca de cómo crear un sistema de archivos con la configuración de servicio recomendada, consulte [Cree rápidamente un sistema de archivos con la configuración recomendada \(consola\)](#).

Puede configurar las políticas del ciclo de vida una vez creado el sistema de archivos o al crear un sistema de archivos con ajustes personalizados.

Los posibles valores de las políticas de ciclo de vida de transición a IA y transición a Archivado incluyen:

- Ninguna
- 1 día desde el último acceso
- 7 días desde el último acceso
- 14 días desde el último acceso
- 30 días desde el último acceso
- 60 días desde el último acceso
- 90 días desde el último acceso
- 180 días desde el último acceso
- 270 días desde el último acceso

- 365 días desde el último acceso

Los posibles valores de la política de ciclo de vida de transición a Estándar incluyen:

- Ninguna
- En el primer acceso

Puede configurar las políticas de ciclo de vida mediante las AWS Management Console y las AWS CLI, tal y como se describe en los siguientes procedimientos.

Administrar las políticas del ciclo de vida en un sistema de archivos existente (consola)

Puede utilizar el AWS Management Console para establecer las políticas del ciclo de vida de un sistema de archivos existente.

1. Inicie sesión en la consola Amazon EFS AWS Management Console y ábrala en <https://console.aws.amazon.com/efs/>.
2. Seleccione Sistemas de archivos para ver la lista de sistemas de archivos de su cuenta.
3. Elija el sistema de archivos en el que desee modificar las políticas del ciclo de vida.
4. En la página de detalles del sistema de archivos, en la sección General, elija Editar. Aparece la página Editar.
5. Para la administración del ciclo de vida, puede cambiar las siguientes políticas del ciclo de vida:
 - Defina Transición a IA en una de las configuraciones disponibles. Para dejar de mover archivos al almacenamiento de IA, seleccione Ninguno.
 - Defina Transición a Archivado en una de las configuraciones disponibles. Para dejar de mover archivos al almacenamiento Archivado, seleccione Ninguno.
 - Defina Transición a Estándar a En el primer acceso para mover los archivos que se encuentran en el almacenamiento de IA al almacenamiento estándar cuando se accede a ellos para operaciones que no sean de metadatos.

Para dejar de mover archivos de IA Archivado al almacenamiento Estándar en el primer acceso, establézcalos en Ninguno.

6. Elija Guardar cambios para guardar los cambios.

Administrar las políticas del ciclo de vida en un sistema de archivos existente (CLI)

Puede utilizarla AWS CLI para establecer o modificar las políticas de ciclo de vida de un sistema de archivos.

- Ejecute el [put-lifecycle-configuration](#) AWS CLI comando o el comando de la [PutLifecycleConfiguration](#) API y especifique el ID del sistema de archivos para el que está gestionando la gestión del ciclo de vida.

```
$ aws efs put-lifecycle-configuration \  
--file-system-id File-System-ID \  
--lifecycle-policies "[{\"TransitionToIA\": \"AFTER_60_DAYS\"}, \  
{\"TransitionToPrimaryStorageClass\": \"AFTER_1_ACCESS\"}, {\"TransitionToArchive\": \  
\"AFTER_90_DAYS\"}]" \  
--region us-west-2 \  
--profile adminuser
```

Obtendrá la siguiente respuesta.

```
{  
  "LifecyclePolicies": [  
    {  
      "TransitionToIA": "AFTER_60_DAYS"  
    },  
    {  
      "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"  
    },  
    {  
      "TransitionToArchive": "AFTER_90_DAYS"  
    }  
  ]  
}
```

Para detener la administración del ciclo de vida para un sistema de archivos existente (CLI)

- Ejecute el comando `put-lifecycle-configuration` y especifique el ID del sistema de archivos para el que se va a detener la administración del ciclo de vida. Mantenga la propiedad `--lifecycle-policies` vacía.

```
$ aws efs put-lifecycle-configuration \  
--file-system-id File-System-ID \  
--lifecycle-policies \  
--region us-west-2 \  
--profile adminuser
```

Obtendrá la siguiente respuesta.

```
{  
  "LifecyclePolicies": []  
}
```

Administración del acceso a los sistemas de archivos cifrados

Con Amazon EFS puede crear sistemas de archivos cifrados. Amazon EFS admite dos formas de cifrado para sistemas de archivos, el cifrado en tránsito y en reposo. Cualquier administración de claves que tenga que hacer solo está relacionada con el cifrado en reposo. Amazon EFS administra automáticamente las claves del cifrado en tránsito.

Si crea un sistema de archivos que utiliza el cifrado en reposo, los datos y los metadatos se cifran en reposo. Amazon EFS usa AWS Key Management Service (AWS KMS) para la administración de claves. Al crear un sistema de archivos mediante el cifrado en reposo, debe especificar una AWS KMS key. La clave de KMS puede ser `aws/elasticfilesystem` (la Clave administrada de AWS de Amazon EFS) o puede ser una clave administrada por el cliente que usted administre.

Los datos de archivos, el contenido de sus archivos, se cifran en reposo con la clave de CMK que especificó al crear el sistema de archivos. Los metadatos, nombres de archivo, nombres de directorio y contenido del directorio, se cifran con una clave que Amazon EFS administra.

La EFS Clave administrada de AWS del sistema de archivos se utiliza como clave KMS para cifrar los metadatos del sistema de archivos, por ejemplo, los nombres de los archivos, los nombres de los directorios y el contenido de los directorios. Usted es el propietario de la clave gestionada por el usuario que se utiliza para cifrar datos de archivos (el contenido de los archivos) en reposo.

Puede administrar quién tiene acceso a las las claves KMS y al contenido de los sistemas de archivos cifrados. Este acceso está controlado por las políticas AWS Identity and Access Management (de IAM) y. AWS KMS Las políticas de IAM controlan el acceso de los usuarios a las

acciones de la API de Amazon EFS. AWS KMS las políticas clave controlan el acceso de un usuario a la clave de KMS que especificó al crear el sistema de archivos. Para más información, consulte los siguientes temas:

- [Usuarios de IAM](#) en la Guía del usuario de IAM
- [Uso de las políticas de claves en AWS KMS](#) en la Guía para desarrolladores de AWS Key Management Service
- [Uso de concesiones](#) en la Guía del desarrollador de AWS Key Management Service .

Como administrador de claves, puede importar las claves externas. También puede habilitar, deshabilitar o eliminar las claves, modificándolas de este modo. El estado de la clave KMS que especificó (cuando creó el sistema de archivos con cifrado en reposo) afecta al acceso a su contenido. La clave KMS debe estar en ese `enabled` estado para que los usuarios puedan acceder al contenido de un sistema de `encrypted-at-rest` archivos cifrado con esa clave.

Realización de acciones administrativas en las claves KMS de Amazon EFS

A continuación se explica cómo activar, desactivar o eliminar las claves KMS asociadas a un sistema de archivos de Amazon EFS. También puede saber qué comportamiento se espera de un sistema de archivos al realizar estas acciones.

Administrar el acceso a la clave KMS de un sistema de archivos

Puede deshabilitar o eliminar sus claves KMS administradas por el cliente, o también puede revocar el acceso de Amazon EFS a sus claves KMS. Las acciones de deshabilitar y revocar el acceso de Amazon EFS a las claves son reversibles. Tenga mucha precaución cuando elimine las claves KMS. La eliminación de una clave KMS es una acción irreversible.

Si deshabilita o elimina la clave KMS utilizada para su sistema de archivos montado, se cumple lo siguiente:

- Esa clave KMS no se puede usar como clave para nuevos sistemas de `encrypted-at-rest` archivos.
- Los sistemas de `encrypted-at-rest` archivos existentes que utilizan esa clave KMS dejan de funcionar después de un período de tiempo.

Si revoca el acceso de Amazon EFS a una concesión para un sistema de archivos montado, el comportamiento es el mismo que si deshabilitara o eliminara la clave KMS asociada. En otras palabras, el sistema de encrypted-at-rest archivos sigue funcionando, pero deja de funcionar después de un período de tiempo.

Puede impedir el acceso a un sistema de encrypted-at-rest archivos montado que tenga una clave de KMS a la que haya inhabilitado, eliminado o revocado el acceso a Amazon EFS. Para ello, desmonte el sistema de archivos y elimine sus destinos de montaje de Amazon EFS.

No puede eliminar una de forma inmediata AWS KMS key, pero puede programarla para que se elimine en un plazo de 7 a 30 días. Cuando una clave KMS está programada para su eliminación, no puede utilizarla para realizar operaciones criptográficas. También puede cancelar la eliminación programada de una clave KMS.

Para obtener información acerca de cómo deshabilitar y volver a habilitar claves KMS administradas por el cliente, consulte [Habilitación y deshabilitación de claves](#) en la Guía del usuario de AWS Key Management Service . Para obtener información sobre cómo programar la eliminación de las claves de KMS administradas por el cliente, consulte [Eliminar claves de KMS](#) en la Guía para desarrolladores de AWS Key Management Service .

Medición: cómo Amazon EFS registra el tamaño del sistema de archivos y el tamaño de los objetos

En las siguientes secciones se describe cómo Amazon EFS informa sobre los tamaños de los sistemas de archivos y los tamaños de los objetos dentro de un sistema de archivos.

Medición de objetos del sistema de archivos de Amazon EFS

Los objetos que puede ver en un sistema de Amazon EFS pueden ser archivos normales, directorios, enlaces simbólicos y archivos especiales (FIFO y sockets). Cada uno de estos objetos se mide para 2 KiB (KiB) de metadatos (por su inode), y uno o más incrementos de 4 KiB de datos. En la siguiente lista se explica el tamaño de datos medido para distintos tipos de objetos del sistema de archivos.

- Archivos normales: el tamaño de datos medido de un archivo normal es el tamaño lógico del archivo redondeado al incremento de 4 KiB más próximo, salvo que pueda resultar menor para archivos dispersos.

Un archivo disperso es un archivo en que los datos no se escriben en todas las posiciones del archivo antes de alcanzar su tamaño lógico. Para un archivo disperso, en algunos casos el

almacenamiento real utilizado es inferior al tamaño lógico redondeado al incremento de 4 KiB más cercano. En estos casos, Amazon EFS notifica el almacenamiento real utilizado como tamaño de datos medido.

- Directorios: el tamaño de datos medidos de un directorio es el almacenamiento real utilizado para el directorio y las entradas de directorio y la estructura de datos que contiene, redondeado al intervalo de 4 KiB más cercano. El tamaño de datos medido no incluye el almacenamiento real utilizado por los datos de los archivos.
- Enlaces simbólicos y archivos especiales: el tamaño de datos medido para estos objetos es siempre 4 KiB.

Cuando Amazon EFS registra el espacio utilizado de un objeto, a través del atributo `space_used` de NFSv4.1, incluye el tamaño de datos medido actual del objeto, pero no el tamaño de los metadatos. Hay dos utilidades disponibles para medir el uso de disco de un archivo: las utilidades `du` y `stat`. A continuación, se muestra un ejemplo de cómo utilizar la utilidad `du` en un archivo vacío que incluye la opción `-k` para devolver la salida en kilobytes.

```
$ du -k file
4      file
```

El siguiente ejemplo muestra cómo utilizar la utilidad `stat` en un archivo vacío para devolver el uso del disco del archivo.

```
$ /usr/bin/stat --format="%b*%B" file | bc
4096
```

Para medir el tamaño de un directorio, utilice la utilidad `stat`. Busque el valor `Blocks` y, a continuación, multiplique dicho valor por el tamaño del bloque. A continuación, se muestra un ejemplo de cómo utilizar la utilidad `stat` en un directorio vacío:

```
$ /usr/bin/stat --format="%b*%B" . | bc
4096
```

Tamaño medido de un sistema de archivos de Amazon EFS

El tamaño medido de un sistema de archivos de Amazon EFS incluye la suma de los tamaños de todos los objetos actuales de todas las clases de almacenamiento de EFS. El tamaño de cada objeto

se calcula a partir de un muestreo representativo que representa el tamaño del objeto durante la hora medida, por ejemplo, la hora de las 8:00 a las 9:00 de la mañana.

Un archivo vacío contribuye en 6 KiB (2 KiB de metadatos +4 KiB de datos) al tamaño medido de su sistema de archivos. Tras la creación, un sistema de archivos dispone de un único directorio raíz vacío y, por tanto, tiene un tamaño medido de 6 KiB.

Los tamaños medidos de un sistema de archivos particular definen el uso que se facturará en la cuenta del propietario de este sistema de archivos por esa hora.

Note

El tamaño medido calculado no representa una instantánea coherente del sistema de archivos en un momento particular durante esa hora. En lugar de ello, representa los tamaños de los objetos que había en el sistema de archivos en distintos momentos de cada hora o de la hora anterior posiblemente. Estos tamaños se suman para determinar el tamaño medido del sistema de archivos de la hora. El tamaño medido de un sistema de archivos es finalmente coherente con los tamaños medidos de los objetos almacenados cuando no hay escrituras en el sistema de archivos.

Puede ver el tamaño medido para un sistema de archivos de Amazon EFS de las siguientes formas:

- Mediante el [describe-file-systems](#) AWS CLI comando y la operación de [DescribeFileSystem](#) API, la respuesta incluye lo siguiente:

```
"SizeInBytes":{
  "Timestamp": 1403301078,
  "Value": 29313744866,
  "ValueInIA": 675432,
  "ValueInStandard": 29312741784
  "ValueInArchive": 327650
}
```

Cuando tamaño medido de ValueInStandard también se utiliza para determinar su punto de referencia de rendimiento de E/S y las tasas de ráfaga para los sistemas de archivos que utilizan el [rendimiento por ráfaga](#).

- Vea la StorageBytes CloudWatch métrica, que muestra el tamaño total medido de los datos en cada clase de almacenamiento. Para obtener más información acerca de la métrica StorageBytes, consulte [CloudWatch Métricas de Amazon para Amazon EFS](#).
- Ejecute el comando `df` en Linux en el símbolo del terminal de una instancia EC2.

No utilice el comando `du` de la raíz del sistema de archivos para medir el almacenamiento, ya que la respuesta no refleja el conjunto completo de datos que se utilizan para medir el sistema de archivos.

Note

El tamaño medido de `ValueInStandard` también se utiliza para determinar su punto de referencia de rendimiento de E/S y las tasas de ráfaga. Para obtener más información, consulte [Rendimiento por ráfagas](#).

Medición de las clases de almacenamiento Archivado y Acceso poco frecuente

Las clases de almacenamiento EFS Infrequent Access (IA) y Archive se miden en incrementos de 4 KiB y tienen un cargo mínimo de facturación por archivo de 128 KiB. Los metadatos de los archivos de IA y Archivado (2 KiB por archivo) se almacenan y se miden siempre en la clase de almacenamiento Estándar. La compatibilidad con archivos de menos de 128 KiB solo está disponible para las políticas de ciclo de vida actualizadas a partir de las 12:00 PM PT del 26 de noviembre de 2023. El acceso a los datos de almacenamiento IA y Archivado se mide en incrementos de 128 KiB.

Puede utilizar la StorageBytes CloudWatch métrica para ver el tamaño medido de los datos en cada una de las clases de almacenamiento. La métrica también muestra el número total de bytes que se consumen al redondear archivos pequeños en las clases de almacenamiento IA y Archive. Para obtener más información sobre la visualización de CloudWatch las métricas, consulte [Acceder a CloudWatch las métricas](#) Para obtener más información acerca de la métrica StorageBytes, consulte [CloudWatch Métricas de Amazon para Amazon EFS](#).

Medición del rendimiento

Amazon EFS mide el rendimiento de las solicitudes de lectura a un tercio de la velocidad de las demás operaciones de E/S del sistema de archivos. Por ejemplo, si utiliza 30 mebibytes por segundo (MiBps) del rendimiento de lectura y escritura, la parte de lectura cuenta como el 10% MiBps del rendimiento efectivo, la parte de escritura cuenta como 30 MiBps y el rendimiento medido combinado

es 40. MiBps Este rendimiento combinado ajustado a las tasas de consumo se refleja en la métrica. `MeteredIOBytes` CloudWatch

Medición de rendimiento elástico

Cuando el modo de rendimiento elástico está habilitado para un sistema de archivos, solo pagas por la cantidad de metadatos y datos leídos o escritos en el sistema de archivos. Los sistemas de archivos Amazon EFS que utilizan el modo de rendimiento elástico miden y facturan los metadatos leen como operaciones de lectura y escriben los metadatos como operaciones de escritura. Las operaciones de metadatos se miden en incrementos de 4 KiB y las operaciones de datos se miden en incrementos de 32 KiB.

Medición de rendimiento aprovisionado

En el caso de los sistemas de archivos que utilizan el modo de rendimiento aprovisionado, solo se paga por el tiempo que el rendimiento esté activado. Amazon EFS mide los sistemas de archivos con el modo de rendimiento aprovisionado habilitado una vez cada hora. Para la medición cuando el modo de rendimiento aprovisionado está configurado en menos de una hora, Amazon EFS calcula el promedio de tiempo con una precisión de milisegundos.

Administración de los costos del sistema de archivos Amazon EFS mediante AWS Budgets

Puede planificar y gestionar los costes del sistema de archivos Amazon EFS mediante AWS Budgets.

Puede trabajar con AWS Budgets desde la AWS Billing and Cost Management consola. Para usar AWS Budgets, debe crear un presupuesto de costos mensual para sus sistemas de archivos EFS. Puede configurar el presupuesto de tal forma que le avise si se prevé que los costos van a superar el importe presupuestado y, a continuación, realizar ajustes para mantener el presupuesto según sea necesario.

El uso AWS de Budgets conlleva costos. De forma regular Cuentas de AWS, los dos primeros presupuestos son gratuitos. Para obtener más información sobre AWS los presupuestos, incluidos los costes, [consulte Gestión de los costes con presupuestos](#) en la Guía del AWS Billing usuario.

Puede establecer presupuestos personalizados para los costes y el uso de Amazon EFS a nivel de cuenta Región de AWS, servicio o etiqueta mediante los parámetros del presupuesto. En la siguiente

sección, encontrará una descripción detallada de cómo configurar un presupuesto de costes en un sistema de archivos EFS con AWS Budgets. Para ello, utilice las etiquetas de asignación de costos.

Requisitos previos

Para realizar los procedimientos que se mencionan en las secciones siguientes, asegúrese de que dispone de lo siguiente:

- Un sistema de archivos de EFS
- Una política AWS Identity and Access Management (IAM) con los siguientes permisos:
 - Acceso a la AWS Billing and Cost Management consola.
 - Capacidad para realizar las acciones `elasticfilesystem:DescribeTags` y `elasticfilesystem:CreateTags`.

Creación de un presupuesto de costes mensual para un sistema de archivos de EFS

Para crear un presupuesto de costes mensual para su sistema de archivos de Amazon EFS mediante etiquetas se requieren tres pasos.

Para crear un presupuesto de costos mensual para el sistema de archivos de EFS mediante etiquetas

1. Cree una etiqueta que se utilizará para identificar el sistema de archivos cuyo seguimiento de costos desea realizar. Para saber cómo hacerlo, consulte [Etiquetado de los recursos de Amazon EFS](#).
2. Active la etiqueta como etiqueta de asignación de costes en la consola de Facturación y administración de costes. Para obtener un procedimiento detallado, consulte [Activación de etiquetas de asignación de costes definidas por el usuario](#) en la Guía del usuario de AWS Billing .
3. En la consola Billing and Cost Management, en Presupuestos, cree un presupuesto de costes mensuales en AWS Presupuestos. Para obtener un procedimiento detallado, consulte [Crear un presupuesto de costes](#) en la .Guía del usuario de AWS Billing .

Después de crear el presupuesto de costos mensual de EFS, puede verlo en el panel Budgets (Presupuestos) que muestra los siguientes datos presupuestarios:

- Los costos actuales y el uso realizado para un presupuesto durante el periodo presupuestario.
- Costos presupuestados para el periodo presupuestario.
- Costos previstos para el periodo presupuestario.
- Un porcentaje que muestra los costos comparados con la cantidad presupuestada.
- Un porcentaje que muestra los costos previstos comparados con la cantidad presupuestada

Para obtener más información acerca de la visualización del presupuesto de costes de EFS, consulte [Visualización de presupuestos](#) en la Guía del usuario de AWS Billing .

Estado del sistema de archivos

Puede ver el estado de los sistemas de archivos de Amazon EFS mediante la consola de Amazon EFS o la AWS CLI. Un sistema de archivos de Amazon EFS puede tener uno de los valores de estado que se describen en la siguiente tabla.

Estado del sistema de archivos	Descripción
DISPONIBLE	El sistema de archivos se encuentra en buen estado y está accesible y disponible para su uso.
EN CREACIÓN	Amazon EFS está creando el nuevo sistema de archivos.
ELIMINANDO	Amazon EFS está eliminando el sistema de archivos en respuesta a una solicitud de eliminación iniciada por el usuario. Para obtener más información, consulte Eliminar los sistemas de archivos Amazon EFS .
DELETED	Amazon EFS ha eliminado el sistema de archivos en respuesta a una solicitud de eliminación iniciada por el usuario. Para obtener más información, consulte Eliminar los sistemas de archivos Amazon EFS .
ACTUALIZANDO	El sistema de archivos se está actualizando en respuesta a una solicitud de actualización iniciada por el usuario.
ERROR	Aplicable a los sistemas de archivos One Zone, incluidos los sistemas de archivos en una configuración de replicación.

Estado del sistema de archivos	Descripción
	<p>El sistema de archivos está en un estado de fallo y no se puede recuperar . Para acceder a los datos del sistema de archivos, restaure una copia de seguridad de este sistema de archivos en un sistema de archivos nuevo. Para obtener más información, consulte .</p> <ul style="list-style-type: none">• Restauración de un punto de recuperación.• Clases de almacenamiento de EFS• Replicación de sistemas de archivos

Monitoreo de Amazon EFS

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon EFS y sus AWS soluciones. Le recomendamos que recopile datos de monitoreo de todas las partes de la AWS solución para poder depurar más fácilmente un error multipunto en caso de que se produzca. No obstante, antes de comenzar a monitorizar Amazon EFS, debe crear un plan de monitorización que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de monitoreo va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del rendimiento normal de Amazon EFS en su entorno. Para ello, se debe medir el rendimiento en distintos momentos y bajo distintas condiciones de carga. Cuando monitoree Amazon EFS, debe tener en cuenta el almacenamiento de los datos de monitoreo históricos. Estos datos almacenados le darán un punto de referencia para compararlos con los datos de desempeño actual, identificar los patrones de desempeño normales y las anomalías del desempeño e idear métodos para solucionar problemas.

Por ejemplo, con Amazon EFS, puede supervisar el desempeño de red, E/S para operaciones de lectura, escritura o metadatos, conexiones de clientes y saldos de ráfagas de crédito de sus sistemas de archivos. Cuando el desempeño se sitúa fuera de la referencia establecida, es posible que necesite cambiar el tamaño del sistema de archivos o el número de clientes conectados para optimizar el sistema de archivos para su carga de trabajo.

Para establecer un punto de referencia debe, como mínimo, monitorizar los elementos siguientes:

- El desempeño de red del sistema de archivos.
- El número de conexiones cliente a un sistema de archivos.
- El número de bytes de cada operación del sistema de archivos, incluida las operaciones de lectura de datos, escritura de datos y metadatos.

Temas

- [Herramientas de monitoreo](#)
- [Supervisión de las métricas de Amazon EFS con Amazon CloudWatch](#)
- [Registro de llamadas a la API de Amazon EFS con AWS CloudTrail](#)

Herramientas de monitoreo

AWS proporciona varias herramientas que puede utilizar para supervisar Amazon EFS. Puede configurar algunas de estas herramientas para que monitoreen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de supervisión en la medida de lo posible.

Herramientas de monitoreo automatizadas

Puede utilizar las siguientes herramientas de monitoreo automatizadas para vigilar Amazon EFS e informar cuando haya algún problema:

- Amazon CloudWatch Alarms: observe una sola métrica durante un período de tiempo que especifique y realice una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo. La acción es una notificación enviada a un tema del Servicio de Notificación Simple (Amazon SNS) o a una política de Auto Scaling de Amazon EC2. CloudWatch las alarmas no invocan acciones solo porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener más información, consulte [Supervisión de las métricas de Amazon EFS con Amazon CloudWatch](#).
- Amazon CloudWatch Logs: supervise, almacene y acceda a sus archivos de registro desde AWS CloudTrail u otras fuentes. Para obtener más información, consulte [Supervisión de archivos de registro](#) en la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Events: haga coincidir los eventos y diríjalos a una o más funciones o transmisiones de destino para realizar cambios, capturar información de estado y tomar medidas correctivas. Para obtener más información, consulta [Qué es Amazon CloudWatch Events](#) en la Guía del CloudWatch usuario de Amazon.
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas, supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs, cree aplicaciones de procesamiento de registros en Java y valide que sus archivos de registro no hayan

cambiado después de su entrega CloudTrail. Para obtener más información, consulte [Trabajar con archivos de CloudTrail registro](#) en la Guía del AWS CloudTrail usuario.

Herramientas de monitoreo manuales

Otra parte importante de la supervisión de Amazon EFS implica la supervisión manual de los elementos que las CloudWatch alarmas de Amazon no cubren. Amazon EFS y otros AWS Management Console paneles proporcionan una at-a-glance vista del estado de su AWS entorno. CloudWatch Le recomendamos que también compruebe los archivos de registro en el sistema de archivos.

- Desde la consola de Amazon EFS, puede encontrar los siguientes elementos para sus sistemas de archivos:
 - El tamaño medido actual
 - El número de destinos de montaje
 - El estado del ciclo de vida
- CloudWatch la página de inicio muestra:
 - Alarmas y estado actual
 - Gráficos de alarmas y recursos
 - Estado de los servicios

Además, puede CloudWatch hacer lo siguiente:

- Cree [paneles personalizados](#) para monitorizar los servicios que utiliza.
- Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias.
- Busca y examina todas las métricas AWS de tus recursos.
- Crear y editar las alarmas de notificación de problemas.

Supervisión de las métricas de Amazon EFS con Amazon CloudWatch

Puede supervisar los sistemas de archivos con Amazon CloudWatch, que recopila y procesa datos sin procesar de Amazon EFS para convertirlos en métricas legibles prácticamente en tiempo real.

Estas estadísticas se registran durante un periodo de 15 meses, de forma que pueda obtener una mejor perspectiva acerca del desempeño de su aplicación web o servicio.

De forma predeterminada, los datos de las métricas de Amazon EFS se envían automáticamente CloudWatch en periodos de 1 minuto, a menos que se indique lo contrario para algunas métricas individuales. La consola Amazon EFS muestra una serie de gráficos basados en los datos sin procesar de Amazon CloudWatch. Según sus necesidades, es posible que prefiera obtener los datos de sus sistemas de archivos en CloudWatch lugar de los gráficos de la consola.

Para obtener más información sobre Amazon CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).

CloudWatch Las métricas de Amazon EFS se presentan como bytes sin procesar. Los bytes no se redondean a un decimal o múltiple binario de la unidad.

CloudWatch Métricas de Amazon para Amazon EFS

Las métricas de Amazon EFS utilizan el espacio de nombres de EFS y proporcionan métricas para una sola dimensión, `FileSystemId`. En la consola de Amazon EFS se puede encontrar el ID del sistema de archivos, con el formato `fs-abcdef0123456789a`.

El espacio de nombres de AWS/EFS incluye las siguientes métricas.

TimeSinceLastSync

Muestra el tiempo transcurrido desde la última sincronización correcta con el sistema de archivos de destino en una configuración de replicación. Todos los cambios en los datos del sistema de archivos de origen que se hayan producido antes del valor de `TimeSinceLastSync` se han replicado correctamente. Es posible que cualquier cambio que se haya producido en el origen después de `TimeSinceLastSync` no se haya replicado por completo.

Unidades: segundos

Estadísticas válidas: Minimum, Maximum, Average

PercentIOLimit

Muestra lo que le queda a un sistema de archivos para llegar al límite de E/S del modo de desempeño de uso general predeterminado.

Unidades: porcentaje

Estadísticas válidas: Minimum, Maximum, Average

BurstCreditBalance

El número de créditos de ráfaga de un sistema de archivos. Los créditos de ráfaga permiten que un sistema de archivos se amplíe a niveles de velocidad superiores al nivel de referencia del sistema de archivos durante determinados periodos de tiempo.

La estadística `Minimum` es el saldo de créditos de ráfaga menor para cualquier minuto durante el periodo. La estadística `Maximum` es el saldo de créditos de ráfaga mayor para cualquier minuto durante el periodo. La estadística `Average` es el saldo de créditos de ráfaga medio durante el periodo.

Unidades: bytes

Estadísticas válidas: Minimum, Maximum, Average

PermittedThroughput

Se permite la cantidad máxima de rendimiento de un sistema de archivos.

- Para los sistemas de archivos que utilizan un rendimiento elástico, este valor refleja el rendimiento máximo de escritura del sistema de archivos.
- En el caso de los sistemas de archivos que utilizan un rendimiento aprovisionado, si la cantidad de datos almacenados en la clase de almacenamiento estándar de EFS permite que el sistema de archivos genere un rendimiento superior al aprovisionado, esta métrica refleja el rendimiento superior en lugar de la cantidad aprovisionada.
- En el caso de los sistemas de archivos en modo de rendimiento dinámico, este valor es una función del tamaño del sistema de archivos y `BurstCreditBalance`

La estadística `Minimum` es el desempeño menor permitido para cualquier minuto durante el periodo. La estadística `Maximum` es el desempeño mayor permitido para cualquier minuto durante el periodo. La estadística `Average` es el desempeño medio permitido durante el periodo.

Note

Las operaciones de lectura se miden a un tercio del ritmo de las demás operaciones.

Unidades: bytes por segundo

Estadísticas válidas: Minimum, Maximum, Average

MeteredIOBytes

El número de bytes medidos para cada operación del sistema de archivos, incluidas las operaciones de lectura, escritura de datos y metadatos; las operaciones de lectura se miden a un tercio de la velocidad de las demás operaciones.

Puede crear una [expresión matemática CloudWatch métrica](#) que se compare con `MeteredIOBytes`. `PermittedThroughput` Si estos valores son iguales, entonces está consumiendo toda la cantidad de rendimiento asignada a su sistema de archivos. En esta situación, podría considerar cambiar el modo de rendimiento del sistema de archivos para obtener un rendimiento superior.

La estadística `Sum` es el número total de bytes medidos asociados a todas las operaciones del sistema de archivos. La estadística `Minimum` es el tamaño de la operación más pequeña durante el periodo. La estadística `Maximum` es el tamaño de la operación más grande durante el periodo. La estadística `Average` es el tamaño medio de una operación durante el periodo. La estadística `SampleCount` proporciona el recuento de todas las operaciones.

Unidades:

- Bytes para las estadísticas `Minimum`, `Maximum`, `Average` y `Sum`.
- Recuento de `SampleCount`.

Estadísticas válidas: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

TotalIOBytes

El número de bytes real de cada operación del sistema de archivos, incluida las operaciones de lectura de datos, escritura de datos y metadatos. Esta es la cantidad real que genera su aplicación y no el rendimiento con el que se mide el sistema de archivos. Puede ser superior a los números que se muestran en `PermittedThroughput`.

La estadística `Sum` es el número total de bytes asociados a todas las operaciones del sistema de archivos. La estadística `Minimum` es el tamaño de la operación más pequeña durante el periodo. La estadística `Maximum` es el tamaño de la operación más grande durante el periodo. La estadística `Average` es el tamaño medio de una operación durante el periodo. La estadística `SampleCount` proporciona el recuento de todas las operaciones.

Note

Para calcular el valor medio de las operaciones por segundo durante un periodo, divida la estadística `SampleCount` por el número de segundos del periodo. Para calcular el

rendimiento medio (bytes por segundo) de un periodo, divida la estadística Sum por el número de segundos del periodo.

Unidades:

- Bytes para las estadísticas Minimum, Maximum, Average y Sum.
- Recuento de SampleCount.

Estadísticas válidas: Minimum, Maximum, Average, Sum, SampleCount

DataReadIOBytes

El número real de bytes de cada operación de lectura del sistema de archivos.

La estadística Sum es el número total de bytes asociados a las operaciones de lectura. La estadística Minimum es el tamaño de la operación de lectura más pequeña durante el periodo. La estadística Maximum es el tamaño de la operación de lectura más grande durante el periodo. La estadística Average es el tamaño medio de las operaciones de lectura durante el periodo. La estadística SampleCount proporciona el recuento de operaciones de lectura.

Unidades:

- Bytes para Minimum, Maximum, Average y Sum.
- Recuento de SampleCount.

Estadísticas válidas: Minimum, Maximum, Average, Sum, SampleCount

DataWriteIOBytes

El número real de bytes de cada operación de escritura del sistema de archivos.

La estadística Sum es el número total de bytes asociados a las operaciones de escritura. La estadística Minimum es el tamaño de la operación de escritura más pequeña durante el periodo. La estadística Maximum es el tamaño de la operación de escritura más grande durante el periodo. La estadística Average es el tamaño medio de las operaciones de escritura durante el periodo. La estadística SampleCount proporciona el recuento de operaciones de escritura.

Unidades:

- Los bytes son las unidades de las estadísticas Minimum, Maximum, Average y Sum.

- Recuento de `SampleCount`.

Estadísticas válidas: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

MetadataIOBytes

El número real de bytes de cada operación de metadatos.

La estadística `Sum` es el número total de bytes asociados a las operaciones de metadatos. La estadística `Minimum` es el tamaño de la operación de metadatos más pequeña durante el periodo. La estadística `Maximum` es el tamaño de la operación de metadatos más grande durante el periodo. La estadística `Average` es el tamaño de la operación de metadatos media durante el periodo. La estadística `SampleCount` proporciona el recuento de operaciones de metadatos.

Unidades:

- Los bytes son las unidades de las estadísticas `Minimum`, `Maximum`, `Average` y `Sum`.
- Recuento de `SampleCount`.

Estadísticas válidas: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

MetadataReadIOBytes

El número real de bytes de cada operación de lectura de metadatos.

La `Sum` estadística es el número total de bytes asociados a las operaciones de lectura de metadatos. La `Minimum` estadística es el tamaño de la operación de lectura de metadatos más pequeña durante el período. La `Maximum` estadística es el tamaño de la mayor operación de lectura de metadatos durante el período. La `Average` estadística es el tamaño medio de las operaciones de lectura de metadatos durante el período. La `SampleCount` estadística proporciona un recuento de las operaciones de lectura de metadatos.

Unidades:

- Los bytes son las unidades de las estadísticas `Minimum`, `Maximum`, `Average` y `Sum`.
- Recuento de `SampleCount`.

Estadísticas válidas: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

MetadataWriteIOBytes

El número real de bytes de cada operación de escritura de metadatos.

La `Sum` estadística es el número total de bytes asociados a las operaciones de escritura de metadatos. La `Minimum` estadística es el tamaño de la operación de escritura de metadatos más pequeña durante el período. La `Maximum` estadística es el tamaño de la mayor operación de escritura de metadatos durante el período. La `Average` estadística es el tamaño medio de las operaciones de escritura de metadatos durante el período. La `SampleCount` estadística proporciona un recuento de las operaciones de escritura de metadatos.

Unidades:

- Los bytes son las unidades de las estadísticas `Minimum`, `Maximum`, `Average` y `Sum`.
- Recuento de `SampleCount`.

Estadísticas válidas: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

ClientConnections

El número de conexiones cliente a un sistema de archivos. Cuando se utiliza un cliente estándar, hay una conexión por instancia de Amazon EC2 montada.

Note

Para calcular el valor medio de `ClientConnections` para períodos superiores a un minuto, divida la estadística `Sum` por el número de minutos del periodo.

Unidades: número de conexiones cliente

Estadísticas válidas: `Sum`

StorageBytes

El tamaño del sistema de archivos en bytes, incluida la cantidad de datos almacenados en las clases de almacenamiento de EFS. Esta métrica se emite CloudWatch cada 15 minutos.

La métrica `StorageBytes` tiene las siguientes dimensiones:

- `Totales` el tamaño medido (en bytes) de los datos almacenados en el sistema de archivos, en todas las clases de almacenamiento. Para las clases de almacenamiento EFS Infrequent Access (IA) y EFS Archive, los archivos de menos de 128 KB se redondean a 128 KB.
- `Standardes` el tamaño medido (en bytes) de los datos almacenados en la clase de almacenamiento EFS Standard.

- `IAes` el tamaño real (en bytes) de los datos almacenados en la clase de almacenamiento EFS Infrequent Access.
- `IASizeOverheades` la diferencia (en bytes) entre el tamaño real de los datos de la clase de almacenamiento de acceso poco frecuente de EFS (indicado en la `IA` dimensión) y el tamaño medido de la clase de almacenamiento, tras redondear los archivos pequeños a 128 KB.
- `Archivees` el tamaño real (en bytes) de los datos almacenados en la clase de almacenamiento EFS Archive.
- `ArchiveSizeOverheades` la diferencia (en bytes) entre el tamaño real de los datos de la clase de almacenamiento EFS Archive (indicado en la `Archive` dimensión) y el tamaño medido de la clase de almacenamiento, tras redondear los archivos pequeños a 128 KB.

Unidades: bytes

Estadísticas válidas: Minimum, Maximum, Average

Note

`StorageBytes` se muestra en la página de métricas del sistema de archivos de la consola de Amazon EFS utilizando unidades base 1024 (kibibytes, mebibytes, gibibytes y tebibytes).

¿Cómo utilizo las métricas de Amazon EFS?

Las métricas mostradas por Amazon EFS proporcionan información que puede analizar de diferentes maneras. En la siguiente lista se indican algunos usos frecuentes de las métricas. Se trata de sugerencias que puede usar como punto de partida y no de una lista completa.

¿Cómo?	Métricas relevantes
¿Cómo puedo determinar mi desempeño?	Puede monitorizar la estadística <code>Sum</code> diaria de la métrica <code>TotalIOBytes</code> para ver el desempeño.
¿Cómo se puede supervisar el número de instancias de	Puede monitorizar la estadística <code>Sum</code> de la métrica <code>ClientConnections</code> . Para calcular el valor medio de <code>ClientConnections</code>

¿Cómo?	Métricas relevantes
Amazon EC2 que se conectan a un sistema de archivos?	para períodos superiores a un minuto, divida la suma por el número de minutos en el periodo.
¿Cómo puedo ver mis saldo de crédito de ráfagas?	Puede ver su saldo monitorizando la métrica <code>BurstCreditBalance</code> para su sistema de archivos. Para obtener más información sobre la transmisión por ráfaga y los créditos de ráfaga, consulte Rendimiento por ráfagas .

Uso de CloudWatch métricas para monitorear el rendimiento

Las CloudWatch métricas de la supervisión del rendimiento (`TotalIOBytes`, `ReadIOBytesWriteIOBytes`, y `MetadataIOBytes` —) representan el rendimiento real que se está generando en el sistema de archivos. La métrica `MeteredIOBytes` representa el cálculo del rendimiento medido total que está impulsando. Puede utilizar el gráfico de utilización del rendimiento (%) de la sección Supervisión de la consola de Amazon EFS para supervisar el uso del rendimiento. Si utiliza CloudWatch paneles personalizados u otra herramienta de supervisión, puede crear una [expresión matemática CloudWatch métrica](#) que se compare con `MeteredIOBytes` `PermittedThroughput`

`PermittedThroughput` mide la cantidad de rendimiento permitido para el sistema de archivos. Este valor se basa en uno de los métodos siguientes:

- Para los sistemas de archivos con un rendimiento de Elastic, este valor refleja el rendimiento máximo de escritura del sistema de archivos.
- En el caso de los sistemas de archivos que utilizan un rendimiento aprovisionado, si la cantidad de datos almacenados en la clase de almacenamiento estándar de EFS permite que el sistema de archivos genere un rendimiento superior al aprovisionado, esta métrica refleja el rendimiento superior en lugar de la cantidad aprovisionada.
- En el caso de los sistemas de archivos que utilizan un rendimiento rápido, este valor es una función del tamaño del sistema de archivos y `BurstCreditBalance`. Supervise `BurstCreditBalance` para asegurarse de que su sistema de archivos funcione a su velocidad de ráfaga y no a su velocidad base. Si el saldo se mantiene constante en cero o cerca de cero, considere la posibilidad de cambiar a Elastic Throughput o Provisioned Throughput para obtener un rendimiento adicional.

Cuando los valores de `MeteredIOBytes` y `PermittedThroughput` son iguales, el sistema de archivos consume todo el rendimiento disponible. En el caso de los sistemas de archivos que utilizan un rendimiento aprovisionado, puedes aprovisionar un rendimiento adicional.

Uso de cálculos de métricas con Amazon EFS

Con la matemática métrica, puede consultar varias CloudWatch métricas y utilizar expresiones matemáticas para crear nuevas series temporales basadas en estas métricas. Puede visualizar las series temporales resultantes en la CloudWatch consola y añadirlas a los paneles. Por ejemplo, puede utilizar métricas de Amazon EFS para realizar el recuento de muestra de operaciones `DataRead` dividido por 60. El resultado es el número medio de lecturas por segundo en su sistema de archivos para un determinado periodo de 1 minuto. Para obtener más información sobre las matemáticas métricas, consulte [Use Metric Math](#) en la Guía del CloudWatch usuario de Amazon.

A continuación, hay algunas expresiones matemáticas de métricas útiles para Amazon EFS.

Temas

- [Matemáticas métricas: rendimiento en MiBps](#)
- [Cálculos de métricas: Rendimiento porcentual](#)
- [Cálculos de métricas: porcentaje de utilización de rendimiento permitido](#)
- [Cálculos de métricas: rendimiento de IOPS](#)
- [Cálculos de métricas: Porcentaje de IOPS](#)
- [Cálculos de métricas: Tamaño medio de E/S en KiB](#)
- [Uso de cálculos de métricas a través de una plantilla de AWS CloudFormation para Amazon EFS](#)

Matemáticas métricas: rendimiento en MiBps

Para calcular el rendimiento promedio (en MiBps) durante un período de tiempo, primero elija una estadística de suma (`DataReadIOBytes`, `DataWriteIOBytes`, `MetadataIOBytes`, o `TotalIOBytes`). A continuación, convierta el valor a MiB y divida por el número de segundos del periodo.

Supongamos que la lógica del ejemplo es la siguiente: (suma de `TotalIOBytes` ÷ 1 048 576 (para convertir en MiB)) ÷ segundos en el periodo

A continuación, la información CloudWatch métrica es la siguiente.

ID	Métricas usables	Estadística	Período
m1	<ul style="list-style-type: none"> DataReadIOBytes DataWriteIOBytes MetadataIOBytes TotalIOBytes 	sum	1 minuto

Su ID de cálculo de métrica y expresión son los siguientes.

ID	Expression
e1	$(m1/1048576)/PERIOD(m1)$

Cálculos de métricas: Rendimiento porcentual

Esta expresión matemática métrica calcula el porcentaje del rendimiento total utilizado para los distintos tipos de E/S, por ejemplo, el porcentaje del rendimiento total que se basa en las solicitudes de lectura. Para calcular el porcentaje del rendimiento total utilizado por uno de los distintos tipos de E/S (DataReadIOBytes, DataWriteIOBytes o MetadataIOBytes) para un periodo de tiempo, en primer lugar, multiplique las respectivas estadísticas de sumas por 100. A continuación, divida el resultado por la estadística de suma de TotalIOBytes para el mismo periodo.

Supongamos que la lógica del ejemplo es la siguiente: (suma de DataReadIOBytes x 100 (para convertir a porcentaje)) ÷ suma de TotalIOBytes

Entonces, su información CloudWatch métrica es la siguiente.

ID	Métricas o métrica usable	Estadística	Período
m1	<ul style="list-style-type: none"> TotalIOBytes 	sum	1 minuto

ID	Métricas o métrica usable	Estadística	Período
m2	• DataReadI 0Bytes	sum	1 minuto

Su ID de cálculo de métrica y expresión son los siguientes.

ID	Expression
e1	$(m2 * 100) / m1$

Cálculos de métricas: porcentaje de utilización de rendimiento permitido

Para calcular el porcentaje de utilización del rendimiento permitido (MeteredIOBytes) durante un período de tiempo, primero multiplique el rendimiento por 100. MiBps A continuación, divida el resultado por la estadística media de PermittedThroughput convertida a MiB del mismo periodo.

Supongamos que la lógica de ejemplo es la siguiente: (expresión matemática métrica para el rendimiento en MiBps x 100 (para convertir en porcentaje)) ÷ (suma de PermittedThroughput ÷ 1.048.576 (para convertir bytes a MiB))

A continuación, la información CloudWatch métrica es la siguiente.

ID	Métricas o métrica usable	Estadística	Período
m1	MeteredIOBytes	sum	1 minuto
m2	Permitted Throughput	average	1 minuto

Su ID de cálculo de métrica y expresión son los siguientes.

ID	Expression
e1	(m1/1048576)/PERIOD(m1)
e2	m2/1048576
e3	((e1)*100)/(e2)

Cálculos de métricas: rendimiento de IOPS

Para calcular el valor medio de las operaciones por segundo (IOPS) durante un periodo de tiempo, divida la estadística de recuento de muestra (DataReadIOBytes, DataWriteIOBytes, MetadataIOBytes o TotalIOBytes) por el número de segundos en el periodo.

Supongamos que la lógica del ejemplo es la siguiente: recuento de muestra de DataWriteIOBytes ÷ segundos en el periodo

Entonces, la información de su CloudWatch métrica es la siguiente.

ID	Métricas usables	Estadística	Período
m1	<ul style="list-style-type: none"> DataReadIOBytes DataWriteIOBytes MetadataIOBytes TotalIOBytes 	recuento de muestra	1 minuto

Su ID de cálculo de métrica y expresión son los siguientes.

ID	Expression
e1	m1/PERIOD(m1)

Cálculos de métricas: Porcentaje de IOPS

Para calcular el porcentaje de IOPS por segundo de los distintos tipos de E/S (`DataReadIOBytes`, `DataWriteIOBytes` o `MetadataIOBytes`) para un periodo de tiempo, en primer lugar, multiplique las respectivas estadísticas de recuento de muestra por 100. A continuación, divida el valor por la estadística de recuento de muestra de `TotalIOBytes` para el mismo periodo.

Supongamos que la lógica del ejemplo es la siguiente: (recuento de muestra de `MetadataIOBytes` x 100 (para convertir a porcentaje)) ÷ recuento de muestra de `TotalIOBytes`

Entonces, la información de su CloudWatch métrica es la siguiente.

ID	Métricas usables	Estadística	Período
m1	<ul style="list-style-type: none"> <code>TotalIOBytes</code> 	recuento de muestra	1 minuto
m2	<ul style="list-style-type: none"> <code>DataReadIOBytes</code> <code>DataWriteIOBytes</code> <code>MetadataIOBytes</code> 	recuento de muestra	1 minuto

Su ID de cálculo de métrica y expresión son los siguientes.

ID	Expression
e1	$(m2*100)/m1$

Cálculos de métricas: Tamaño medio de E/S en KiB

Para calcular el tamaño medio de E/S (en KiB) durante un periodo, divida las respectivas estadísticas de suma para la métrica `DataReadIOBytes`, `DataWriteIOBytes` o `MetadataIOBytes` por la misma estadística de recuento de muestra de esa métrica.

Supongamos que la lógica del ejemplo es la siguiente: (suma de `DataReadIOBytes` ÷ 1024 (para convertir a KiB)) ÷ recuento de muestra de `DataReadIOBytes`

Entonces, la información CloudWatch métrica es la siguiente.

ID	Métricas usables	Estadística	Período
m1	<ul style="list-style-type: none"> DataReadI OBytes DataWrite IOBytes MetadataI OBytes 	sum	1 minuto
m2	<ul style="list-style-type: none"> DataReadI OBytes DataWrite IOBytes MetadataI OBytes 	recuento de muestra	1 minuto

Su ID de cálculo de métrica y expresión son los siguientes.

ID	Expression
e1	$(m1/1024)/m2$

Uso de cálculos de métricas a través de una plantilla de AWS CloudFormation para Amazon EFS

También puede crear expresiones matemáticas métricas mediante AWS CloudFormation plantillas. Puede descargar y personalizar una de estas plantillas para utilizarla en los [tutoriales de Amazon EFS](#) GitHub. Para obtener más información sobre el uso de AWS CloudFormation plantillas, consulte [Trabajar con AWS CloudFormation plantillas](#) en la Guía del AWS CloudFormation usuario.

Supervisión del estado exitoso o fallido del intento de montaje

Puede utilizar Amazon CloudWatch Logs para supervisar e informar del éxito o el fracaso de los intentos de montaje de sus sistemas de archivos EFS de forma remota sin tener que iniciar sesión en

los clientes. Utilice el siguiente procedimiento para configurar la instancia EC2 de manera que utilice CloudWatch los registros para supervisar el éxito o el fracaso de los intentos de montaje del sistema de archivos.

Para habilitar la notificación de intentos de montaje correctos o fallidos en los registros CloudWatch

1. Instale `amazon-efs-utils` en la instancia de EC2 que monta el sistema de archivos. Para obtener más información, consulte [Utilización AWS Systems Manager para instalar o actualizar automáticamente el cliente Amazon EFS](#) o [Instalación manual del cliente de Amazon EFS](#).
2. Instale `botocore` en la instancia de EC2 que montará el sistema de archivos. Para obtener más información, consulte [Instalación y actualización botocore](#).
3. Habilite la función de CloudWatch registros en `amazon-efs-utils`. Al AWS Systems Manager instalar y configuraramazon-efs-utils, el CloudWatch registro se realiza automáticamente. Al instalar manualmente el paquete `amazon-efs-utils`, debe actualizar manualmente el archivo de configuración `/etc/amazon/efs/efs-utils.conf` quitando los comentarios de la línea `# enabled = true` de la sección `cloudwatch-log`. Use uno de los siguientes comandos para habilitar CloudWatch los registros manualmente.

En instancias de Linux:

```
sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/}' /etc/amazon/efs/efs-utils.conf
```

Para instancias de macOS:

```
EFS_UTILS_VERSION= efs-utils-version
sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/;}' /usr/local/Cellar/amazon-efs-utils/${EFS_UTILS_VERSION}/libexec/etc/amazon/efs/efs-utils.conf
```

Para instancias de mac2:

```
EFS_UTILS_VERSION= efs-utils-version
sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/;}' /opt/homebrew/Cellar/amazon-efs-utils/${EFS_UTILS_VERSION}/libexec/etc/amazon/efs/efs-utils.conf
```

4. Si lo desea, puede configurar CloudWatch los nombres de los grupos de registros y establecer los días de retención de registros en el `efs-utils.conf` archivo. Si desea tener grupos de

registros independientes CloudWatch para cada sistema de archivos montado, `{fs_id}` agréguelos al final del `log_group_name` campo del `efs-utils.conf` archivo de la siguiente manera:

```
[cloudwatch-log]
log_group_name = /aws/efs/utils/{fs_id}
```

5. Adjunte la política `AmazonElasticFileSystemsUtils` AWS administrada a la función de IAM que ha asociado a la instancia EC2 o a AWS las credenciales configuradas en la instancia. Puede utilizar Systems Manager para ello. Para obtener más información, consulte [Paso 1: Configure un perfil de instancia de IAM con los permisos necesarios.](#)

A continuación, se muestran ejemplos de entradas de registro de estado de intentos de montaje:

```
Successfully mounted fs-12345678.efs.us-east-1.amazonaws.com at /home/ec2-user/efs
Mount failed, Failed to resolve "fs-01234567.efs.us-east-1.amazonaws.com"
```

Para ver el estado del montaje en los registros CloudWatch

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En la barra de navegación izquierda, elija Grupos de registro.
3. Elija el grupo de registros `/aws/efs/utils`. Verá un flujo de registro para cada combinación de instancia de Amazon EC2 y sistema de archivos de EFS.
4. Elija un flujo de registro para ver eventos de registro específicos, incluido el estado del intento de montaje exitoso o fallido.

Acceder a CloudWatch las métricas

Puede ver las métricas de Amazon EFS CloudWatch de varias maneras:


- En la consola de Amazon EFS
- En la CloudWatch consola
- Uso de la CloudWatch CLI
- Uso de la CloudWatch API

Los siguientes procedimientos le muestran cómo obtener acceso a las métricas a través de estas herramientas.

Para ver CloudWatch las métricas y las alarmas en la consola de Amazon EFS

1. Inicie sesión en la consola Amazon EFS AWS Management Console y ábrala en <https://console.aws.amazon.com/efs/>.
2. Elija Sistemas de archivos.
3. Elija el sistema de archivos cuyas CloudWatch métricas desee ver.
4. Seleccione Supervisión para mostrar la página de métricas del sistema de archivos.

La página de métricas del sistema de archivos muestra un conjunto predeterminado de CloudWatch métricas para el sistema de archivos. Todas CloudWatch las alarmas que haya configurado también se muestran con estas métricas. Para los sistemas de archivos que utilizan el modo de rendimiento máximo de E/S, el conjunto predeterminado de métricas incluye el saldo de crédito de ráfaga en lugar del límite porcentual de E/S. Puede anular la configuración predeterminada mediante el cuadro de diálogo de configuración de métricas, al que se accede abriendo la configuración.

 Note

La métrica de utilización del rendimiento (%) no es una CloudWatch métrica; se obtiene mediante cálculos CloudWatch métricos.

5. Puede ajustar la forma en que se muestran las métricas y las alarmas con los controles de la página de métricas del sistema de archivos, de la siguiente manera.
 - Cambia el modo de visualización entre series temporales o valores únicos.
 - Muestra u oculta CloudWatch las alarmas configuradas para el sistema de archivos.
 - Seleccione Ver más en CloudWatch para ver las métricas en CloudWatch.
 - Selecciona Añadir al panel de control para abrir el CloudWatch panel y añadir las métricas que se muestran.
 - Ajuste el intervalo de tiempo de la métrica que se muestra de 1 hora a 1 semana.

Para ver las métricas mediante la CloudWatch consola

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.

2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de EFS.
4. (Opcional) Para ver una métrica, escriba su nombre en el campo de búsqueda.
5. (Opcional) Para filtrar por dimensión, seleccione FileSystemID.

Para acceder a las métricas desde AWS CLI

- Utilice el comando [list-metrics](#) con el espacio de nombres de `--namespace "AWS/EFS"`. Para obtener más información, consulte [Referencia de comandos de la AWS CLI](#).

Para acceder a las métricas desde la CloudWatch API

- Llamar a [GetMetricStatistics](#). Para obtener más información, consulta [Amazon CloudWatch API Reference](#).

Creación de CloudWatch alarmas para supervisar Amazon EFS

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una métrica determinada durante el periodo especificado. A continuación, la alarma realiza una o varias acciones según el valor de la métrica con respecto a un umbral determinado durante varios periodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de escalado automático.

Las alarmas invocan acciones únicamente en caso de cambios de estado sostenidos. CloudWatch las alarmas no invocan acciones solo porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de periodos.

Un uso importante de CloudWatch las alarmas en Amazon EFS es aplicar el cifrado en reposo del sistema de archivos. Puede habilitar el cifrado en reposo para sistema de archivos de Amazon EFS al crear el sistema. Para hacer cumplir `encryption-at-rest` las políticas de datos de los sistemas de archivos Amazon EFS, puede utilizar Amazon CloudWatch y AWS CloudTrail detectar la creación de un sistema de archivos y comprobar que el cifrado en reposo está activado. Para obtener más información, consulte [Tutorial: Aplicar cifrado en reposo a un sistema de archivos de Amazon EFS](#).

Note

En la actualidad, no puede forzar el cifrado en tránsito.

Los siguientes procedimientos describen cómo crear alarmas para Amazon EFS.

Para configurar las alarmas mediante la CloudWatch consola

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en <https://console.aws.amazon.com/cloudwatch/>.
2. Elija Crear alarma. Esto lanza el Asistente de creación de alarmas.
3. Elija Métricas de EFS y desplácese a través de las métricas de para localizar la métrica donde desea colocar una alarma. Para mostrar solo las métricas de Amazon EFS en este cuadro de diálogo, busque el ID del sistema de archivos de su sistema de archivos. Seleccione la métrica para crear una alarma y elija Siguiente.
4. Rellene los valores de Name (Nombre), Description (Descripción) y Whenever (Siempre que) para la métrica.
5. Si CloudWatch quiere enviarte un correo electrónico cuando se alcance el estado de alarma, en el campo Siempre que aparezca esta alarma:, selecciona State is ALARM. En el campo Send notification to: (Enviar notificación a:), elija un tema de SNS. Si selecciona Crear tema, puede definir el nombre y las direcciones de correo electrónico de una nueva lista de suscripción de correo electrónico. Esta lista se guarda y aparece en el campo para futuras alarmas.

Note

Si utiliza Crear tema para crear un nuevo tema de Amazon SNS, debe verificar las direcciones de correo electrónico para que reciban notificaciones. Los correos electrónicos solo se envían cuando la alarma entra en estado de alarma. Si este cambio en el estado de la alarma se produce antes de que se verifiquen las direcciones de correo electrónico, no reciben una notificación.

6. En este momento, el área Alarm Preview le ofrece la oportunidad de previsualizar la alarma que está a punto de crear. Seleccione Crear alarma.

Para configurar una alarma mediante el AWS CLI

- Llamar a [put-metric-alarm](#). Para obtener más información, consulte [Referencia de comandos de la AWS CLI](#).

Para configurar una alarma mediante la CloudWatch API

- Llamar a [PutMetricAlarm](#). Para obtener más información, consulta la [referencia de la CloudWatch API de Amazon](#).

Registro de llamadas a la API de Amazon EFS con AWS CloudTrail

Amazon EFS está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon EFS. CloudTrail captura todas las llamadas a las API de Amazon EFS como eventos, incluidas las llamadas desde la consola de Amazon EFS y las llamadas en código a las operaciones de la API de Amazon EFS.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon EFS. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon EFS, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información, consulte la [Guía del usuario de AWS CloudTrail](#).

Información de Amazon EFS en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Amazon EFS, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para obtener un registro continuo de sus eventos Cuenta de AWS, incluidos los eventos de Amazon EFS, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todos los Región de AWS s. La ruta registra los eventos de toda Regiones de AWS la AWS partición y entrega los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar

otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail :

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail Integraciones y servicios compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas las [llamadas a la API](#) de Amazon EFS las registra CloudTrail. Por ejemplo, las llamadas a `CreateMountTarget` y `CreateTags` las operaciones generan entradas en los archivos de CloudTrail registro. `CreateFileSystem`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario raíz o de usuario AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento [CloudTrail UserIdentity en la Guía del usuario](#).AWS CloudTrail

Descripción de las entradas de archivos de registro de Amazon EFS

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra el CreateTags funcionamiento cuando se crea una etiqueta para un sistema de archivos desde la consola.

```
{
  "eventVersion": "1.06",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-03-01T18:02:37Z"
      }
    }
  },
  "eventTime": "2017-03-01T19:25:47Z",
  "eventSource": "elasticfilesystem.amazonaws.com",
  "eventName": "CreateTags",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "fileSystemId": "fs-00112233",
    "tags": [{
      "key": "TagName",
      "value": "AnotherNewTag"
    }
  ]
},
  "responseElements": null,
  "requestID": "dEXAMPLE-feb4-11e6-85f0-736EXAMPLE75",
  "eventID": "eEXAMPLE-2d32-4619-bd00-657EXAMPLEe4",
  "eventType": "AwsApiCall",
  "apiVersion": "2015-02-01",
  "recipientAccountId": "111122223333"
}
```

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra la DeleteTags acción que se produce cuando se elimina de la consola una etiqueta de un sistema de archivos.

```
{
  "eventVersion": "1.06",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-03-01T18:02:37Z"
      }
    }
  },
  "eventTime": "2017-03-01T19:25:47Z",
  "eventSource": "elasticfilesystem.amazonaws.com",
  "eventName": "DeleteTags",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "fileSystemId": "fs-00112233",
    "tagKeys": []
  },
  "responseElements": null,
  "requestID": "dEXAMPLE-feb4-11e6-85f0-736EXAMPLE75",
  "eventID": "eEXAMPLE-2d32-4619-bd00-657EXAMPLEe4",
  "eventType": "AwsApiCall",
  "apiVersion": "2015-02-01",
  "recipientAccountId": "111122223333"
}
```

Entradas de registro para roles vinculados al servicio EFS

La función vinculada al servicio de Amazon EFS realiza llamadas de API a los AWS recursos. Verá las entradas de CloudTrail registro de las username :

AWSServiceRoleForAmazonElasticFileSystem llamadas realizadas por el rol vinculado

al servicio de EFS. Para obtener más información acerca de EFS y roles vinculados a servicios, consulte [Uso de roles vinculados a servicios para Amazon EFS](#).

El siguiente ejemplo muestra una entrada de CloudTrail registro que muestra una `CreateServiceLinkedRole` acción cuando Amazon EFS crea el rol `AWSServiceRoleForAmazonElasticFileSystem` vinculado al servicio.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:user/user1",
    "accountId": "111122223333",
    "accessKeyId": "A111122223333",
    "userName": "user1",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-10-23T22:45:41Z"
      }
    },
    "invokedBy": "elasticfilesystem.amazonaws.com"
  },
  "eventTime": "2019-10-23T22:45:41Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "CreateServiceLinkedRole",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "user_agent",
  "requestParameters": {
    "awsServiceName": "elasticfilesystem.amazonaws.com"
  },
  "responseElements": {
    "role": {
      "assumeRolePolicyDocument":
"111122223333-10-111122223333Statement111122223333Action111122223333AssumeRole111122223333Effe
%22%3A%20%22Allow%22%2C%20%22Principal%22%3A%20%7B%22Service%22%3A%20%5B%22
elasticfilesystem.amazonaws.com%22%5D%7D%7D%5D%7D",
      "arn": "arn:aws:iam::111122223333:role/aws-service-role/
elasticfilesystem.amazonaws.com/AWSServiceRoleForAmazonElasticFileSystem",
      "roleId": "111122223333",
      "createDate": "Oct 23, 2019 10:45:41 PM",

```



```

        "roleName": "AWSServiceRoleForAmazonElasticFileSystem",
        "path": "/aws-service-role/elasticfilesystem.amazonaws.com/"
    }
},
"requestID": "11111111-2222-3333-4444-abcdef123456",
"eventID": "11111111-2222-3333-4444-abcdef123456",
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que muestra una `CreateNetworkInterface` acción realizada por el rol `AWSServiceRoleForAmazonElasticFileSystem` vinculado al servicio, tal como se indica en `sessionContext`

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::0123456789ab:assumed-role/AWSServiceRoleForAmazonElasticFileSystem/0123456789ab",
    "accountId": "0123456789ab",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::0123456789ab:role/aws-service-role/elasticfilesystem.amazonaws.com/AWSServiceRoleForAmazonElasticFileSystem",
        "accountId": "0123456789ab",
        "userName": "AWSServiceRoleForAmazonElasticFileSystem"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-10-23T22:50:05Z"
      }
    },
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2019-10-23T22:50:05Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CreateNetworkInterface",

```

```
"awsRegion": "us-east-1",
"sourceIPAddress": "elasticfilesystem.amazonaws.com",
"userAgent": "elasticfilesystem.amazonaws.com",
"requestParameters": {
  "subnetId": "subnet-71e2f83a",
  "description": "EFS mount target for fs-1234567 (fsmt-1234567)",
  "groupSet": {},
  "privateIpAddressesSet": {}
},
"responseElements": {
  "requestId": "0708e4ad-03f6-4802-b4ce-4ba987d94b8d",
  "networkInterface": {
    "networkInterfaceId": "eni-0123456789abcdef0",
    "subnetId": "subnet-12345678",
    "vpcId": "vpc-01234567",
    "availabilityZone": "us-east-1b",
    "description": "EFS mount target for fs-1234567 (fsmt-1234567)",
    "ownerId": "666051418590",
    "requesterId": "0123456789ab",
    "requesterManaged": true,
    "status": "pending",
    "macAddress": "00:bb:ee:ff:aa:cc",
    "privateIpAddress": "192.0.2.0",
    "privateDnsName": "ip-192-0-2-0.ec2.internal",
    "sourceDestCheck": true,
    "groupSet": {
      "items": [
        {
          "groupId": "sg-c16d65b6",
          "groupName": "default"
        }
      ]
    },
    "privateIpAddressesSet": {
      "item": [
        {
          "privateIpAddress": "192.0.2.0",
          "primary": true
        }
      ]
    },
    "tagSet": {}
  }
},
}
```

```

"requestID": "11112222-3333-4444-5555-666666777777",
"eventID": "aaaabbbb-1111-2222-3333-444444555555",
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

Entradas de registro para la autenticación de EFS

NewClientConnectionEmisiones y eventos de autorización de Amazon EFS para clientes de NFS. UpdateClientConnection CloudTrail Se emite un evento NewClientConnection cuando se autoriza una conexión inmediatamente después de una conexión inicial e inmediatamente después de una reconexión. Se emite un UpdateClientConnection cuando se vuelve a autorizar una conexión y se modifica la lista de acciones permitidas. El evento también se emite cuando la nueva lista de acciones permitidas no incluye ClientMount. Para obtener más información acerca de la autorización de EFS, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#).

El siguiente ejemplo muestra una entrada de CloudTrail registro que muestra un NewClientConnection evento.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::0123456789ab:assumed-role/abcdef0123456789",
    "accountId": "0123456789ab",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE ",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::0123456789ab:role/us-east-2",
        "accountId": "0123456789ab",
        "userName": "username"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-12-23T17:50:16Z"
      },
      "ec2RoleDelivery": "1.0"
    }
  }
}

```

```
    }
  },
  "eventTime": "2019-12-23T18:02:12Z",
  "eventSource": "elasticfilesystem.amazonaws.com",
  "eventName": "NewClientConnection",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "elasticfilesystem",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "27859ac9-053c-4112-ae3-f3429719d460",
  "readOnly": true,
  "resources": [
    {
      "accountId": "0123456789ab",
      "type": "AWS::EFS::FileSystem",
      "ARN": "arn:aws:elasticfilesystem:us-east-2:0123456789ab:file-system/
fs-01234567"
    },
    {
      "accountId": "0123456789ab",
      "type": "AWS::EFS::AccessPoint",
      "ARN": "arn:aws:elasticfilesystem:us-east-2:0123456789ab:access-point/
fsap-0123456789abcdef0"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "0123456789ab",
  "serviceEventDetails": {
    "permissions": {
      "ClientRootAccess": true,
      "ClientMount": true,
      "ClientWrite": true
    },
    "sourceIpAddress": "10.7.3.72"
  }
}
```

Entradas de archivos de registro de Amazon EFS para sistemas de encrypted-at-rest archivos

Amazon EFS brinda la opción de utilizar el cifrado en reposo, en tránsito o ambos para los sistemas de archivos. Para obtener más información, consulte [Cifrado de datos en Amazon EFS](#).

Amazon EFS envía [el contexto de cifrado](#) al realizar solicitudes a la AWS KMS API para generar claves de datos y descifrar datos de Amazon EFS. El ID del sistema de archivos es el contexto de cifrado para todos los sistemas de archivos que se cifran en reposo. En el `requestParameters` campo de una entrada de CloudTrail registro, el contexto de cifrado es similar al siguiente.

```
"EncryptionContextEquals": {}  
"aws:elasticfilesystem:filesystem:id" : "fs-4EXAMPLE"
```

Rendimiento de Amazon EFS

En las siguientes secciones, se proporciona una descripción general del rendimiento de Amazon EFS y cómo la configuración de su sistema de archivos afecta a las dimensiones clave de rendimiento. También ofrecemos algunos consejos y recomendaciones importantes para optimizar el rendimiento de su sistema de archivos.

Temas

- [Resumen de rendimiento](#)
- [Clases de almacenamiento](#)
- [Modos de rendimiento](#)
- [Modos de rendimiento](#)
- [Consejos de rendimiento de Amazon EFS](#)
- [Solución de problemas de Amazon EFS: problemas de rendimiento](#)
- [Solución de problemas de AML y de kernel](#)

Resumen de rendimiento

Por lo general, el rendimiento del sistema de archivos se mide por la latencia, el rendimiento y las operaciones de entrada/salida por segundo (IOPS). El rendimiento de Amazon EFS en estas dimensiones depende de la configuración del sistema de archivos. Las siguientes configuraciones afectan al rendimiento de un sistema de archivos de Amazon EFS:

- Tipo de sistema de archivos: regional o One Zone
- Modo de rendimiento: uso general o E/S máxima

Important


El modo de rendimiento máximo de E/S tiene latencias por operación más altas que el modo de rendimiento de uso general. Para un rendimiento más rápido, recomendamos utilizar siempre el modo de rendimiento de uso general. Para obtener más información, consulte [Modos de rendimiento](#).

- Modo de rendimiento: elástico, aprovisionado o en ráfaga

En la siguiente tabla se describen las especificaciones de rendimiento de los sistemas de archivos que utilizan el modo de rendimiento de uso general y las diferentes combinaciones posibles de tipo de sistema de archivos y modo de rendimiento.

Especificaciones de rendimiento para los sistemas de archivos que utilizan el modo de rendimiento de uso general

Configuración de almacenamiento y rendimiento		Latencia		IOPS máximo		Rendimiento máximo		
Tipo de sistema de archivos	Modo de rendimiento	Operación de lectura	Operación de escritura	Operación de lectura	Operación de escritura	Lectura por sistema de archivos ¹	Escritura por sistema de archivos ¹	Lectura/escritura por cliente
Regional	Elastic	Tan solo 250 microsegundos (µs)	Tan solo 2,7 milisegundos (ms)	90.000 a 250.000 ²	50 000	De 3 a 20 gibibytes por segundo () GiBps	DE 1 A 5 GiBps	1500 mebibytes por segundo (3) MiBps
Regional	Aprovisionado	Tan solo 250 µs	Tan solo 2,7 ms	55 000	25 000	3—10 GiBps	1—3.33 GiBps	500 MiBps
Regional	Transmisión por ráfagas	Tan solo 250 µs	Tan bajo como 2,7 ms	35 000	7000	3—5 GiBps	1—3 GiBps	500 MiBps
One Zone	Elástico, provisionado, explosivo	Tan solo 250 µs	Tan solo 1,6 ms	35 000	7000	3 GiBps ⁴	1 GiBps ⁴	500 MiBps

 Note

Notas a pie de página:

1. El rendimiento máximo de lectura y escritura depende de la Región de AWS. Un rendimiento superior al rendimiento máximo de Región de AWS de un requiere un aumento de la cuota de rendimiento. El equipo de servicio de Amazon EFS considerará cualquier solicitud de rendimiento adicional. case-by-case La aprobación puede depender del tipo de carga de trabajo. Para obtener más información sobre cómo solicitar una revisión, consulte [Cuotas de Amazon EFS](#).
2. Los sistemas de archivos que utilizan un rendimiento elástico pueden generar un máximo de 90 000 IOPS de lectura para los datos a los que se accede con poca frecuencia y 250 000 IOPS de lectura para los datos a los que se accede con frecuencia. Se aplican recomendaciones adicionales para lograr el máximo de IOPS. Para obtener más información, consulte [the section called “Optimizar las cargas de trabajo que exigen un alto rendimiento e IOPS”](#).
3. El rendimiento máximo combinado de lectura y escritura es de 1500 MiBps para los sistemas de archivos que utilizan Elastic Throughput y se montan con la versión 2.0 o posterior del cliente Amazon EFS (amazon-efs-utils versión) o el controlador CSI de Amazon EFS (aws-efs-csi-driver). Para todos los demás sistemas de archivos, el límite de rendimiento es de 500. MiBps Para obtener más información sobre el cliente Amazon EFS, consulte [Instalación de las herramientas de Amazon EFS](#)
4. Los sistemas de archivos One Zone que utilizan un rendimiento de ráfaga pueden generar los mismos niveles de rendimiento de per-file-system lectura y escritura que los sistemas de archivos regionales que utilizan un rendimiento de ráfaga (lectura máxima de 5 GiBps para lectura y 3 para escritura). GiBps

Clases de almacenamiento

Las clases de almacenamiento de Amazon EFS están diseñadas para ofrecer el almacenamiento más eficaz en función de los casos de uso.

- La clase de almacenamiento EFS Estándar utiliza almacenamiento en unidades de estado sólido (SSD) para ofrecer los niveles más bajos de latencia para los archivos a los que se accede con frecuencia. Esta clase de almacenamiento proporciona latencias de primer byte de tan solo 250 microsegundos para lecturas y 2,7 milisegundos para escrituras.

- Las clases de almacenamiento EFS Infrequent Access (IA) y EFS Archive almacenan los datos a los que se accede con menos frecuencia y que no requieren el rendimiento de latencia que requieren los datos a los que se accede con frecuencia. Estas clases de almacenamiento proporcionan latencias de primer byte de decenas de milisegundos.

Para obtener más información acerca de las clases de almacenamiento de EFS, consulte [the section called “Clases de almacenamiento de EFS”](#).

Modos de rendimiento

Amazon EFS ofrece dos modos de rendimiento: Uso general y E/S máx.

- El modo de uso general tiene la latencia por operación más baja y es modo predeterminado para los sistemas de archivos. Los sistemas de archivos One Zone siempre utilizan el modo de rendimiento de uso general. Para un rendimiento más rápido, recomendamos utilizar siempre el modo de rendimiento de uso general.
- El modo de E/S máx. es un tipo de rendimiento de generación anterior que está diseñado para cargas de trabajo altamente paralelizadas que pueden tolerar latencias más altas que el modo de uso general. El modo de E/S máx. no es compatible con los sistemas de archivos One Zone ni con los sistemas de archivos que utilizan rendimiento elástico.

Important

Debido a las latencias por operación más altas con una E/S máx., recomendamos utilizar el modo de rendimiento de uso general para todos los sistemas de archivos.

Para garantizar que su carga de trabajo se mantenga dentro del límite de IOPS disponible para los sistemas de archivos que utilizan el modo de rendimiento de uso general, puede supervisar la `PercentIOLimit` CloudWatch métrica. Para obtener más información, consulte [CloudWatch Métricas de Amazon para Amazon EFS](#).

Las aplicaciones pueden escalar sus IOPS de forma elástica hasta el límite asociado al modo de rendimiento. Las IOPS no se facturan por separado, sino que se incluyen en la contabilidad de rendimiento del sistema de archivos. Cada solicitud del Network File System (NFS) se contabiliza como un rendimiento de 4 kilobytes (KB) o su tamaño real de solicitud y respuesta, lo que sea mayor.

Modos de rendimiento

El modo de rendimiento de un sistema de archivos determina el rendimiento disponible para el sistema de archivos. Amazon EFS ofrece tres modos de rendimiento: elástico, aprovisionado y ráfaga. Se ofrece un descuento en el rendimiento de lectura para que pueda obtener un rendimiento de lectura superior al de escritura. El rendimiento máximo disponible con cada modo de rendimiento depende de la Región de AWS. Para obtener más información sobre el rendimiento máximo del sistema de archivos en las distintas regiones, consulte [Cuotas de Amazon EFS](#).

Su sistema de archivos puede alcanzar un rendimiento combinado de lectura y escritura del 100 %. Por ejemplo, si el sistema de archivos utiliza el 33 % de su límite de rendimiento de lectura, el sistema de archivos puede alcanzar simultáneamente hasta el 67 % de su límite de rendimiento de escritura. Puede supervisar el uso del rendimiento del sistema de archivos en el gráfico de utilización del rendimiento (%) que aparece en la página de detalles del sistema de archivos de la consola. Para obtener más información, consulte [Uso de CloudWatch métricas para monitorear el rendimiento](#).

Elección del modo de rendimiento correcto para un sistema de archivos.

La elección del modo de rendimiento correcto para el sistema de archivos depende de los requisitos de rendimiento de la carga de trabajo.

- Rendimiento elástico (recomendado): utilice el rendimiento elástico predeterminado cuando tenga cargas de trabajo puntuales o impredecibles y requisitos de rendimiento difíciles de pronosticar, o cuando su aplicación aumente el rendimiento en una average-to-peak proporción del 5% o menos. Para obtener más información, consulte [Rendimiento elástico](#).
- Rendimiento aprovisionado: utilice el rendimiento aprovisionado si conoce los requisitos de rendimiento de su carga de trabajo o si su aplicación impulsa el rendimiento en una proporción del 5% o más. average-to-peak Para obtener más información, consulte [Rendimiento aprovisionado](#).
- Rendimiento rápido: utilice el rendimiento rápido cuando desee un rendimiento que se adapte a la cantidad de almacenamiento de su sistema de archivos.

Si, después de usar el rendimiento en ráfaga, descubre que su aplicación tiene un rendimiento limitado (por ejemplo, utiliza más del 80% del rendimiento permitido o usted ha utilizado todos los créditos de ráfaga), debe utilizar un rendimiento elástico o Provisioned. Para obtener más información, consulte [Rendimiento por ráfagas](#).

Puedes usar Amazon CloudWatch para determinar el average-to-peak ratio de tu carga de trabajo comparando la MeteredIOBytes métrica con la PermittedThroughput métrica. Para obtener más información acerca de las métricas de Amazon EFS, consulte [CloudWatch Métricas de Amazon para Amazon EFS](#).

Rendimiento elástico

En el caso de los sistemas de archivos que utilizan Elastic Throughput, Amazon EFS escala automáticamente el rendimiento hacia arriba o hacia abajo para satisfacer las necesidades de la actividad de la carga de trabajo. El rendimiento elástico es el mejor modo de rendimiento para cargas de trabajo con picos de actividad o impredecibles con requisitos de rendimiento difíciles de pronosticar, o para aplicaciones que impulsan el rendimiento a una velocidad media del 5% o menos del rendimiento máximo (la relación). average-to-peak

Como el rendimiento de los sistemas de archivos con Elastic Throughput se amplía automáticamente, no necesitas especificar ni aprovisionar la capacidad de rendimiento para satisfacer las necesidades de tus aplicaciones. Solo pagas por la cantidad de metadatos y datos leídos o escritos, y no acumulas ni consumes créditos por ráfaga mientras usas Elastic throughput.

Note

El rendimiento elástico solo está disponible para los sistemas de archivos que utilizan el modo de rendimiento de uso general.

Para obtener información sobre los límites de rendimiento de Elastic por región, consulte. [Cuotas de Amazon EFS que puede incrementar](#)

Rendimiento aprovisionado

Con el rendimiento aprovisionado, se especifica un nivel de rendimiento que el sistema de archivos puede impulsar independientemente del tamaño del sistema de archivos o del saldo acumulado. Utilice el rendimiento aprovisionado si conoce los requisitos de rendimiento de su carga de trabajo o si su aplicación impulsa el rendimiento al 5% o más de la relación. average-to-peak

En el caso de los sistemas de archivos que utilizan el rendimiento aprovisionado, se le cobrará por el rendimiento habilitado para el sistema de archivos. El importe de rendimiento facturado en un mes se basa en el rendimiento aprovisionado que supere el rendimiento base incluido en el sistema de

archivos en el almacenamiento estándar, hasta los límites de rendimiento base de ráfaga vigentes en la Región de AWS.

Si el rendimiento de referencia del sistema de archivos supera el rendimiento aprovisionado, utilizará automáticamente el rendimiento en ráfagas permitido para el sistema de archivos (hasta los límites de rendimiento de referencia de Bursting vigentes en ese momento). Región de AWS

Para obtener información sobre los límites de rendimiento por rendimiento, consulte.

RegionProvisioned [Cuotas de Amazon EFS que puede incrementar](#)

Rendimiento por ráfagas.

Se recomienda aumentar el rendimiento para las cargas de trabajo que requieren un rendimiento que se amplíe en función de la cantidad de almacenamiento del sistema de archivos. Con el rendimiento en ráfagas, el rendimiento base es proporcional al tamaño del sistema de archivos en la clase de almacenamiento estándar, a una velocidad de 50 por KiBps cada GiB de almacenamiento. Los créditos de ráfaga se acumulan cuando el sistema de archivos consume menos de su tasa de rendimiento base y se deducen cuando el rendimiento supera la tasa base.

Cuando hay créditos de ráfaga disponibles, un sistema de archivos puede generar un rendimiento de hasta 100 MiBps por TiB de almacenamiento, hasta Región de AWS el límite, con un mínimo de 100. MiBps Si no hay créditos de ráfaga disponibles, un sistema de archivos puede generar hasta 50 MiBps por TiB de almacenamiento, con un mínimo de 1. MiBps

Para obtener información sobre el rendimiento de ráfagas por región, consulte. [General resource quotas that cannot be changed](#)

Descripción de los créditos de ráfaga de Amazon EFS

Con el rendimiento en ráfagas, cada sistema de archivos gana créditos de ráfaga a lo largo del tiempo a una velocidad de referencia que viene determinada por el tamaño del sistema de archivos que se almacena en la clase de almacenamiento estándar EFS. La velocidad de referencia es de 50 MiBps por tebibyte [TiB] de almacenamiento (equivalente a 50 por KiBps GiB de almacenamiento). Amazon EFS mide las operaciones de lectura hasta un tercio de la velocidad de las operaciones de escritura, lo que permite al sistema de archivos alcanzar una tasa de referencia de hasta 150 KiBps por GiB de rendimiento de lectura o 50 KiBps por GiB de rendimiento de escritura.

Un sistema de archivos puede impulsar el rendimiento a su velocidad medida de referencia de forma continua. Un sistema de archivos acumula créditos de ráfaga siempre que esté inactivo o reduzca el rendimiento por debajo de su tasa medida de referencia. Los créditos de ráfaga acumulados ofrecen al sistema de archivos la capacidad para incrementar el desempeño por encima de su tasa inicial.

Por ejemplo, un sistema de archivos con 100 GiB de datos medidos en la clase de almacenamiento estándar tiene un rendimiento de referencia de 5. MiBps Durante un período de inactividad de 24 horas, el sistema de archivos obtiene un crédito de 432 000 MiB ($5 \text{ MiB} \times 86\,400 \text{ segundos} = 432\,000 \text{ MiB}$), que se pueden utilizar para ráfagas de 100 MiB durante 72 minutos ($432\,000 \text{ MiB} \div 100 = 4320 \text{ minutos}$). MiBps

Los sistemas de archivos mayores de 1 TiB siempre puedan transmitir por ráfagas hasta un 50 por ciento del tiempo si están inactivos el 50 por ciento restante.

La siguiente tabla ofrece ejemplos de comportamiento de transmisión por ráfagas.

Tamaño del sistema de archivos	Rendimiento por ráfagas	Rendimiento de referencia
100 GiB de datos medidos en almacenamiento estándar	<ul style="list-style-type: none"> Ráfaga a 300 (MiBps) en modo de solo lectura durante un máximo de 72 minutos al día, o Ráfaga a 100 unidades de MiBps solo escritura durante un máximo de 72 minutos al día 	<ul style="list-style-type: none"> Conduzca hasta 15 MiBps minutos de forma continua en modo de solo lectura Conduce hasta 5 MiBps unidades de forma continua con solo escritura
100 GiB de datos medidos en almacenamiento estándar	<ul style="list-style-type: none"> Aumente a 300 en modo de MiBps solo lectura durante 12 horas al día, o Ráfaga a 100 unidades con MiBps solo escritura durante 12 horas al día 	<ul style="list-style-type: none"> Conduzca 150 unidades de solo lectura de forma continua MiBps Conduce 50 MiBps unidades de solo escritura de forma continua
10 TiB de datos medidos en almacenamiento estándar	<ul style="list-style-type: none"> Ráfaga a 3 en GiBps modo de solo lectura durante 12 horas al día, o Ráfaga a 1 GiBps solo escritura durante 12 horas al día 	<ul style="list-style-type: none"> Conduzca 1.5 de solo lectura de forma continua GiBps Drive 500 solo de escritura continua MiBps
Por lo general, sistemas de archivos más grandes	<ul style="list-style-type: none"> Alcanza 300 unidades de almacenamiento de MiBps solo lectura por TiB durante 12 horas al día, o 	<ul style="list-style-type: none"> Impulse 150 unidades de MiBps almacenamiento de solo lectura por TiB de forma continua

Tamaño del sistema de archivos	Rendimiento por ráfagas	Rendimiento de referencia
	<ul style="list-style-type: none"> Ráfaga a 100 MiBps unidades de solo escritura por TiB de almacenamiento durante 12 horas al día 	<ul style="list-style-type: none"> Impulse 50 unidades de almacenamiento de MiBps solo escritura por TiB de forma continua

Note

Amazon EFS proporciona un rendimiento medido de 1 MiBps a todos los sistemas de archivos, incluso si la tasa de referencia es inferior.

El tamaño del sistema de archivos utilizado a la hora de determinar la tasa inicial y la tasa de ráfaga es el mismo que el tamaño medido `ValueInStandard` disponible a través de la operación de la API [DescribeFileSystems](#).

Los sistemas de archivos pueden obtener hasta un saldo de crédito máximo de 2,1 TiB para sistemas de archivos de tamaño inferior a 1 TiB o de 2,1 TiB por TiB almacenado para sistemas de archivos mayores de 1 TiB. Este comportamiento significa que los sistemas de archivos pueden acumular créditos suficientes para transmitir por ráfagas de forma continua durante un máximo de 12 horas.

Restricciones a la hora de cambiar el rendimiento y cambiar la cantidad aprovisionada

Puede cambiar el modo de rendimiento de un sistema de archivos existente y cambiar la cantidad de rendimiento. Sin embargo, tras cambiar el modo de rendimiento a rendimiento aprovisionado o cambiar la cantidad de rendimiento aprovisionada, las siguientes acciones están restringidas durante un período de 24 horas:

- Cambiar del modo de rendimiento aprovisionado al modo de rendimiento elástico o en ráfaga.
- Disminuir la cantidad de rendimiento aprovisionada.

Consejos de rendimiento de Amazon EFS

Cuando se utiliza Amazon EFS tenga en cuenta los siguientes consejos de rendimiento.

Tamaño medio de E/S

La naturaleza distribuida de Amazon EFS permite obtener altos niveles de disponibilidad, durabilidad y escalabilidad. Esta arquitectura distribuida da lugar a un costo de latencia pequeño por cada operación con archivos. Debido a esta latencia por operación, el desempeño global suele aumentar a la par que el tamaño medio de E/S, porque el costo se amortiza con la mayor cantidad de datos.

Optimizar las cargas de trabajo que exigen un alto rendimiento e IOPS

Para las cargas de trabajo que requieren un alto rendimiento e IOPS, utilice sistemas de archivos regionales configurados con el modo de rendimiento de uso general y un rendimiento elástico.

Note

Para alcanzar el máximo de 250 000 IOPS de lectura para los datos a los que se accede con frecuencia, el sistema de archivos debe utilizar Elastic Throughput.

Para lograr los niveles más altos de rendimiento, debe aprovechar la paralelización configurando su aplicación o carga de trabajo de la siguiente manera.

1. Distribuya la carga de trabajo de manera uniforme entre todos los clientes y directorios, con al menos el mismo número de directorios que el número de clientes utilizados.
2. Reduzca al mínimo la contención alineando los subprocesos individuales con conjuntos de datos o archivos distintos.
3. Distribuya la carga de trabajo entre 10 o más clientes NFS, con al menos 64 subprocesos por cliente en un único destino de montaje.

Conexiones simultáneas

Puede montar sistemas de archivos Amazon EFS en hasta miles de instancias de Amazon EC2 y otras instancias AWS informáticas de forma simultánea. Si puede paralelizar su aplicación en más instancias, puede ofrecer niveles de desempeño más altos en su sistema de archivos en general entre las instancias.

Modelo de solicitud

Si activa las escrituras asíncronas en el sistema de archivos, las operaciones de escritura pendientes se almacenan en el búfer de memoria en la instancia de Amazon EC2 antes de escribirse en Amazon FSx para Lustre de forma asíncrona. Las escrituras asíncronas suelen tener latencias menores. Cuando se realizan escrituras asíncronas, el kernel utiliza memoria adicional para el almacenamiento en caché.

Un sistema de archivos que tiene habilitadas escrituras síncronas o uno que abre archivos con una opción que ignora la caché (por ejemplo, `O_DIRECT`), emite solicitudes síncronas a Amazon EFS. Cada operación realizará un recorrido de ida y vuelta entre el cliente y Amazon EFS.

Note

El modelo de solicitud elegido tiene contrapartidas en la coherencia (si utiliza varias instancias de Amazon EC2) y en la velocidad. El uso de escrituras síncronas proporciona una mayor coherencia de datos al completar cada transacción de solicitud de escritura antes de procesar la siguiente solicitud. El uso de escrituras asíncronas proporciona un mayor rendimiento al almacenar en búfer las operaciones de escritura pendientes.

Configuración de montaje del cliente NFS

Compruebe que está utilizando las opciones de montaje recomendadas, tal y como se describe en [Montaje de sistemas de archivos de EFS](#) y en [Consideraciones de montaje adicionales](#).

Amazon EFS es compatible con los protocolos de las versiones 4.0 y 4.1 de Network File System (NFSv4) a la hora de montar los sistemas de archivos en instancias de Amazon EC2. NFSv4.1 proporciona un mejor rendimiento para las operaciones paralelas de lectura de archivos pequeños (más de 10 000 archivos por segundo) en comparación con NFSv4.0 (menos de 1000 archivos por segundo). Las instancias de Mac de Amazon EC2 que ejecutan macOS Big Sur solo son compatibles con NFS v4.0.

No utilice las siguientes opciones de montaje:

- `noac`, `actimeo=0`, `acregmax=0`, `acdirmax=0` — Estas opciones deshabilitan la caché de atributos, lo que tiene un gran impacto en el rendimiento.
- `lookupcache=pos`, `lookupcache=none` – Estas opciones deshabilitan la caché de búsqueda de nombres de archivos, lo que tiene un gran impacto en el rendimiento.

- `fs_c` — Esta opción habilita el almacenamiento en caché de archivos local, pero no cambia la coherencia de la caché de NFS ni reduce las latencias.

Note

Es posible que le interese aumentar el tamaño de los búferes de lectura y escritura de su cliente NFS a 1 MB al montar el sistema de archivos.

Optimización del rendimiento de los archivos pequeños

Puede mejorar el rendimiento de los archivos pequeños minimizando las reaperturas de archivos, aumentando el paralelismo y agrupando los archivos de referencia siempre que sea posible.

- Minimice el número de viajes de ida y vuelta al servidor.

No cierre archivos innecesariamente si los necesitará más adelante en un flujo de trabajo. Al mantener abiertos los descriptores de los archivos, se puede acceder directamente a la copia local de la memoria caché. Por lo general, las operaciones de apertura, cierre y metadatos de archivos no se pueden realizar de forma asíncrona ni mediante una canalización.

Al leer o escribir archivos pequeños, los dos viajes de ida y vuelta adicionales son importantes.

Cada viaje de ida y vuelta (archivo abierto, archivo cerrado) puede llevar tanto tiempo como leer o escribir megabytes de datos masivos. Resulta más eficiente abrir un archivo de entrada o salida una vez, al principio del trabajo de computación, y mantenerlo abierto durante todo el trabajo.

- Utilice el paralelismo para reducir el impacto de los tiempos de ida y vuelta.
- Agrupe los archivos de referencia en un archivo `.zip`. Algunas aplicaciones utilizan un conjunto grande de archivos de referencia pequeños, en su mayoría de solo lectura. Al agruparlos en un archivo `.zip`, podrá leer muchos archivos en un solo proceso de apertura y cierre.

El formato `.zip` permite el acceso aleatorio a archivos individuales.

Optimización del rendimiento de directorio

Al realizar una lista (`ls`) en directorios muy grandes (más de 100 000 archivos) que se están modificando simultáneamente, los clientes de Linux NFS pueden bloquearse y no devolver ninguna

respuesta. Este problema se ha corregido en el kernel 5.11, que se ha migrado a Amazon Linux kernels 4.14, 5.4 y 5.10.

Si es posible, le recomendamos que mantenga el número de directorios del sistema de archivos en menos de 10 000. Utilice subdirectorios anidados en la medida de lo posible.

Cuando publique un directorio, evite obtener los atributos del archivo si no son necesarios, ya que no están almacenados en el propio directorio.

Optimización del tamaño de `read_ahead_kb` de NFS

El atributo `read_ahead_kb` de NFS define el número de kilobytes que el kernel de Linux debe leer o recuperar previamente durante una operación de lectura secuencial.

Para las versiones del kernel de Linux anteriores a la 5.4.*, el valor de `read_ahead_kb` se establece multiplicando por `NFS_MAX_READAHEAD` el valor de `rsize` (el tamaño del búfer de lectura configurado por el cliente establecido en las opciones de montaje). Cuando se utilizan las [opciones de montaje recomendadas](#), esta fórmula establece `read_ahead_kb` en 15 MB.

Note

A partir de las versiones 5.4.* del kernel de Linux, el cliente NFS de Linux utiliza un valor de `read_ahead_kb` predeterminado de 128 KB. Se recomienda aumentar este valor a 15 MB.

El asistente de montaje de Amazon EFS, que está disponible en la versión 1.33.2 de `amazon-efs-utils` y posteriores, modifica automáticamente el valor de `read_ahead_kb` para que sea igual a `15 * rsize`, o 15 MB, después de montar el sistema de archivos.

En el caso de los kernels de Linux 5.4 o posteriores, si no utiliza el asistente de montaje para montar los sistemas de archivos, considere la posibilidad de configurar `read_ahead_kb` manualmente en 15 MB para mejorar el rendimiento. Tras montar el sistema de archivos, puede restablecer el valor de `read_ahead_kb` mediante el siguiente comando. Antes de ejecutar este comando, reemplace los siguientes valores:

- Sustituya `read-ahead-value-kb` por el tamaño deseado en kilobytes.
- Sustituya `efs-mount-point` con el punto de montaje del sistema de archivos.

```
device_number=$(stat -c '%d' efs-mount-point)
```

```
((major = ($device_number & 0xFFF00) >> 8))
((minor = ($device_number & 0xFF) | (($device_number >> 12) & 0xFFF00)))
sudo bash -c "echo read-ahead-value-kb > /sys/class/bdi/$major:$minor/read_ahead_kb"
```

Por ejemplo, el siguiente ejemplo establece el tamaño de `read_ahead_kb` en 15 MB.

```
device_number=$(stat -c '%d' efs)
((major = ($device_number & 0xFFF00) >> 8))
((minor = ($device_number & 0xFF) | (($device_number >> 12) & 0xFFF00)))
sudo bash -c "echo 15000 > /sys/class/bdi/$major:$minor/read_ahead_kb"
```

Solución de problemas de Amazon EFS: problemas de rendimiento

En general, si surge algún problema con Amazon EFS que le resulta difícil resolver, confirme que está utilizando un kernel de Linux reciente. Si utiliza una distribución de Linux empresarial, le recomendamos lo siguiente:

- Amazon Linux 2 con kernel 4.3 o posterior
- Amazon Linux 2015.09 o posterior
- RHEL 7.3 o posterior
- Todas las versiones de Ubuntu 16.04
- Ubuntu 14.04 con kernel 3.13.0-83 o posterior
- SLES 12 Sp2 o posterior

Si utiliza otra distribución o un kernel personalizado, le recomendamos la versión de kernel 4.3 o posterior.

Note

RHEL 6.9 podría ser inadecuado para determinadas cargas de trabajo debido a [Rendimiento bajo al abrir muchos archivos en paralelo](#).

Temas

- [No se puede crear un sistema de archivos de EFS](#)
- [Acceso denegado a los archivos permitidos en el sistema de archivos NFS](#)

- [Errores al acceder a la consola de Amazon EFS](#)
- [La instancia de Amazon EC2 deja de responder](#)
- [La aplicación deja de responder al escribir grandes cantidades de datos](#)
- [Rendimiento bajo al abrir muchos archivos en paralelo](#)
- [La configuración de NFS personalizada provoca retrasos de escritura](#)
- [La creación de copias de seguridad con Oracle Recovery Manager es lenta](#)

No se puede crear un sistema de archivos de EFS

Se produce un error en la solicitud de creación de un sistema de archivos de EFS y aparece el siguiente mensaje:

```
User: arn:aws:iam::111122223333:user/username is not authorized to
perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

Acción que debe ejecutarse

Compruebe su política AWS Identity and Access Management (de IAM) para confirmar que está autorizado a crear sistemas de archivos EFS con las condiciones de recursos especificadas. Para obtener más información, consulte [Administración de identidades y acceso Amazon Elastic File System](#).

Acceso denegado a los archivos permitidos en el sistema de archivos NFS

Cuando un usuario al que se le asignan más de 16 identificadores de grupos de acceso (GID) intenta realizar una operación en un sistema de archivos NFS, se le puede denegar el acceso a los archivos permitidos en el sistema de archivos. Este problema se produce porque el protocolo NFS admite un máximo de 16 GID por usuario y cualquier GID adicional se trunca con respecto a la solicitud del cliente de NFS, tal como se define en el [RFC 5531](#).

Acción que debe ejecutarse

Reestructure las asignaciones de usuarios y grupos de NFS para que a cada usuario no se le asignen más de 16 grupos de acceso (GID).

Errores al acceder a la consola de Amazon EFS

En esta sección se describen los errores que pueden experimentar los usuarios al acceder a la consola de administración de Amazon EFS.

Error al autenticar las credenciales de **ec2:DescribeVPCs**

Al acceder a la consola de Amazon EFS, aparece el siguiente mensaje de error:

```
AuthFailure: An error occurred authenticating your credentials for ec2:DescribeVPCs.
```

Este error indica que sus credenciales de inicio de sesión no se autenticaron correctamente con el servicio de Amazon EC2. La consola de Amazon EFS llama al servicio de Amazon EC2 en su nombre al crear sistemas de archivos de EFS en la VPC que elija.

Acción que debe ejecutarse

Asegúrese de que la hora en que el cliente accede a la consola de Amazon EFS esté configurada correctamente.

La instancia de Amazon EC2 deja de responder

Una instancia de Amazon EC2 puede dejar de responder porque ha eliminado un destino de montaje de sistema de archivos sin desmontar primero el sistema de archivos.

Acción que debe ejecutarse

Antes de eliminar un destino de montaje de sistema de archivos, desmonte el sistema de archivos. Para obtener más información sobre el desmontaje de su sistema de archivos de Amazon EFS, consulte [Desmontaje de sistemas de archivos](#).

La aplicación deja de responder al escribir grandes cantidades de datos

Una aplicación que escribe una gran cantidad de datos en Amazon EFS deja de responder y hace que la instancia se reinicie.

Acción que ejecutar

Si una aplicación tarda demasiado tiempo en escribir todos sus datos en Amazon EFS, Linux podría reiniciarse, ya que parece que el proceso ha dejado de responder. Dos parámetros de configuración de kernel definen este comportamiento, `kernel.hung_task_panic` y `kernel.hung_task_timeout_secs`.

En el ejemplo siguiente, el estado del proceso que ha dejado de responder se notifica mediante el comando `ps` con `D` antes de reiniciar la instancia, lo que indica que el proceso está a la espera de E/S.

```
$ ps aux | grep large_io.py
root 33253 0.5 0.0 126652 5020 pts/3 D+ 18:22 0:00 python large_io.py
/efs/large_file
```

Para evitar un reinicio, aumente el periodo de tiempo de espera o deshabilite el modo de pánico del kernel cuando detecte una tarea que ha dejado de responder. El siguiente comando deshabilita el modo de pánico de kernel de la tarea que ha dejado de responder en la mayoría de los sistemas de Linux.

```
$ sudo sysctl -w kernel.hung_task_panic=0
```

Rendimiento bajo al abrir muchos archivos en paralelo

Las aplicaciones que abren varios archivos en paralelo no experimentan el aumento esperado del rendimiento de paralelización de E/S.

Acción que ejecutar

Este problema se produce en los clientes de la versión 4 de Network File System (NFSv4) y en los clientes RHEL 6 que utilizan NFSv4.1 ya que estos clientes de NFS serializan operaciones de APERTURA y de CIERRE de NFS. Utilice la versión 4.1 del protocolo NFS y una de las [distribuciones de Linux](#) sugeridas que no tiene este problema.

Si no puede utilizar NFSv4.1, tenga en cuenta que el cliente NFSv4.0 de Linux serializa las solicitudes de apertura y cierre por ID de usuario e ID de grupo. Esta serialización sucede incluso si varios procesos o varios subprocesos realizan solicitudes al mismo tiempo. El cliente solo envía una operación de apertura o cierre a un servidor de NFS a la vez, cuando todos los ID coinciden. Para solucionar estos problemas, puede realizar cualquiera de las siguientes acciones:

- Puede ejecutar cada proceso desde un ID de usuario distinto en la misma instancia de Amazon EC2.
- Puede dejar el ID de usuario igual en todas las solicitudes abiertas y modificar el conjunto de ID de grupo en su lugar.
- Puede ejecutar cada proceso desde una instancia de Amazon EC2 independiente.

La configuración de NFS personalizada provoca retrasos de escritura

Dispone de configuración de cliente NFS personalizada y una instancia de Amazon EC2 tarda hasta tres segundos en llevar a cabo una operación de escritura en un sistema de archivos desde otra instancia de Amazon EC2.

Acción que ejecutar

Si detecta este problema, puede resolverlo de una de las siguientes formas:

- Si el cliente NFS en la instancia de Amazon EC2 que está leyendo los datos tiene el almacenamiento en caché de atributos activado, desmonte su sistema de archivos. A continuación, vuelva a montarlo con la opción `noac` para deshabilitar el almacenamiento en caché de atributos. El almacenamiento en caché de atributos en NFSv4.1 está habilitado de forma predeterminada.

Note

Deshabilitar el almacenamiento en caché en el lado del cliente podría reducir el desempeño de la aplicación.

- También puede borrar la caché de atributos bajo demanda a través de un lenguaje de programación compatible con los procedimientos de NFS. Para ello, puede enviar una solicitud de procedimiento `ACCESS` inmediatamente antes de una solicitud de lectura.

Por ejemplo, utilizando el lenguaje de programación Python, puede construir la siguiente llamada.

```
# Does an NFS ACCESS procedure request to clear the attribute cache, given a path to
the file
import os
os.access(path, os.W_OK)
```

La creación de copias de seguridad con Oracle Recovery Manager es lenta

La creación de backup con Oracle Recovery Manager puede ser lenta si Oracle Recovery Manager se detiene durante 120 segundos antes de iniciar un trabajo de backup.

Acción que ejecutar

Si detecta este problema, deshabilite Oracle Direct NFS, tal como se describe en [Enabling and Disabling Direct NFS Client Control of NFS](#) en el centro de ayuda de Oracle.

Note

Amazon EFS no admite Oracle Direct NFS.

Solución de problemas de AMI y de kernel

A continuación, encontrará información sobre la resolución de problemas relacionados con determinadas versiones de imagen de máquina de Amazon (AMI) o de kernel al utilizar Amazon EC2 desde una instancia de Amazon EC2.

Temas

- [No se puede cambiar la propiedad](#)
- [El sistema de archivos sigue realizando operaciones repetidamente debido a un error del cliente](#)
- [Cliente con interbloqueo](#)
- [La enumeración de archivos en un directorio grande tarda mucho tiempo](#)

No se puede cambiar la propiedad

No puede cambiar la propiedad de un archivo o directorio utilizando el comando de Linux `chown`.

Versiones de kernel con este error

2.6.32

Acción que ejecutar

Para resolver el error, ejecute la siguiente operación:

- Si está realizando `chown` para el paso de configuración único necesario para cambiar el propietario del directorio raíz de EFS, puede ejecutar el comando `chown` desde una instancia que esté ejecutando un kernel más reciente. Por ejemplo, utilice la versión más reciente de Amazon Linux.
- Si `chown` forma parte de su flujo de trabajo de producción, debe actualizar la versión del kernel que utiliza `chown`.

El sistema de archivos sigue realizando operaciones repetidamente debido a un error del cliente

Un sistema de archivos se bloquea realizando operaciones repetidas debido a un error del cliente.

Acción que debe ejecutarse

Actualice el software de cliente a la versión más reciente.

Cliente con interbloqueo

Un cliente pasa a tener interbloqueo.

Versiones de kernel con este error

- CentOS-7 con kernel Linux 3.10.0-229.20.1.el7.x86_64
- Ubuntu 15.10 con kernel Linux 4.2.0-18-generic

Acción que debe ejecutarse

Realice una de las siguientes acciones siguientes:

- Actualice a una nueva versión del kernel. Para CentOS-7, la versión de kernel Linux 3.10.0-327 o posterior contiene la solución.
- Cambie a una versión de kernel más antigua.

La enumeración de archivos en un directorio grande tarda mucho tiempo

Esto puede ocurrir si el directorio está cambiando mientras el cliente NFS itera a través del directorio para finalizar la operación de listado. Siempre que el cliente NFS observa que el contenido del directorio cambiado durante esta iteración, el cliente NFS reinicia la iteración desde el principio. Por ello, el comando `ls` puede tardar bastante en completarse en el caso de un directorio grande con archivos que se actualizan con frecuencia.

Versiones de kernel con este error

Versiones de kernel de CentOS y RHEL inferiores a la 2.6.32-696.el6

Acción que debe ejecutarse

Para resolver este problema, actualice a una versión del kernel más nueva.

Copia de seguridad de los sistemas de archivos de Amazon EFS

AWS Backup es una forma sencilla y rentable de proteger sus datos mediante la realización de copias de seguridad de sus sistemas de archivos Amazon EFS. AWS Backup es un servicio de respaldo unificado diseñado para simplificar la creación, migración, restauración y eliminación de copias de seguridad y, al mismo tiempo, proporcionar informes y auditorías mejorados. AWS Backup facilita el desarrollo de una estrategia de respaldo centralizada para garantizar el cumplimiento legal, reglamentario y profesional. AWS Backup también simplifica la protección AWS de sus volúmenes de almacenamiento, bases de datos y sistemas de archivos al proporcionar un lugar central en el que puede hacer lo siguiente:

- Configurar y auditar los recursos de AWS de los que desea hacer una copia de seguridad
- Automatizar la programación de copias de seguridad
- Establecer políticas de retención
- Monitorizar toda la actividad reciente de copias de seguridad y restauración

Amazon EFS está integrado de forma nativa con AWS Backup. Puede usar la consola EFS, la API y AWS Command Line Interface (AWS CLI) para habilitar las copias de seguridad automáticas de su sistema de archivos. Las copias de seguridad automáticas utilizan un plan de copias de seguridad predeterminado con la configuración AWS Backup recomendada para las copias de seguridad automáticas. Para obtener más información, consulte [Copias de seguridad automáticas](#). También puede utilizarlo AWS Backup para [configurar manualmente](#) sus propios planes de copias de seguridad, especificando la frecuencia de las copias de seguridad, cuándo realizar las copias de seguridad, durante cuánto tiempo conservarlas y una política de ciclo de vida para las copias de seguridad. Posteriormente, puede asignar sistemas de archivos de Amazon EFS u otros recursos de AWS a ese plan de copia de seguridad.

Copias de seguridad incrementales

AWS Backup realiza copias de seguridad incrementales de los sistemas de archivos EFS. Durante la copia de seguridad inicial, se crea una copia de la totalidad del sistema de archivos. Durante las copias de seguridad posteriores de ese mismo sistema de archivos, solo se copian los archivos y directorios que se hayan cambiado, añadido o eliminado. Con cada copia de seguridad incremental,

AWS Backup conserva los datos de referencia necesarios para permitir una restauración completa. Este enfoque disminuye el tiempo necesario para completar la copia de seguridad y ahorra costos de almacenamiento, ya que no se duplican los datos.

Coherencia de la copia de seguridad

Amazon EFS está diseñado para tener un alto nivel de disponibilidad. Puede acceder a los sistemas de archivos de Amazon EFS y modificarlos mientras la copia de seguridad se realiza en AWS Backup. Sin embargo, pueden producirse incoherencias, como datos duplicados, sesgados o excluidos si realiza modificaciones en su sistema de archivos mientras se realiza la copia de seguridad. Entre estas modificaciones se incluyen las operaciones de escritura, cambio de nombre, traslado o eliminación. Para garantizar la coherencia entre copias de seguridad, le recomendamos que pause las aplicaciones o procesos que modifiquen el sistema de archivos durante el proceso de copia de seguridad. También puede programar las copias de seguridad para que se produzcan durante los periodos en los que el sistema de archivos no se esté modificando.

Rendimiento de Backup

En general, puede esperar las siguientes tasas de copia de seguridad y restauración AWS Backup. Es posible que las velocidades sean menores para algunas cargas de trabajo, como las que contienen un archivo o directorio grande.

- Velocidad de backup de 1000 archivos por segundo o 300 megabytes por segundo (MBps), lo que sea más lento.
- Velocidad de restauración de 500 archivos por segundo o 150 MBps, lo que sea más lento.

La duración máxima de una operación de copia de seguridad AWS Backup es de 30 días.

Su uso AWS Backup no consume los créditos de ráfaga acumulados y no se tiene en cuenta en los límites de funcionamiento de los archivos en el modo de rendimiento de uso general. Para obtener más información, consulte [Cuotas para sistemas de archivos de Amazon EFS](#).

Intervalo de conclusión de la copia de seguridad

Si lo desea, puede especificar una ventana de finalización para una copia de seguridad. Este intervalo define el periodo de tiempo en el que debe completarse una copia de seguridad. Si

especifica una ventana de finalización, asegúrese de tener en cuenta el rendimiento esperado y el tamaño y la composición de su sistema de archivos. Esto le ayuda a garantizar que su copia de seguridad se pueda completar durante el intervalo.

Las copias de seguridad que no se completan durante el periodo especificado se marcan con el estado incompleto. Durante la siguiente copia de seguridad programada, AWS Backup se reanuda en el punto en el que se detuvo. Puede ver el estado de todas sus copias de seguridad en la [consola de administración de AWS Backup](#).

Clases de almacenamiento de EFS

Se puede utilizar AWS Backup para hacer copias de seguridad de todos los datos de un sistema de archivos EFS, independientemente de la clase de almacenamiento en la que se encuentren los datos. No se le aplicará ningún cargo por el acceso a los datos cuando realice copias de seguridad de un sistema de archivos de EFS que tenga la administración del ciclo de vida habilitada y con datos en la clase de almacenamiento Acceso poco frecuente (IA) o Archivado.

Al restaurar un punto de recuperación, todos los archivos se restauran en la clase de almacenamiento Estándar. Para obtener más información sobre las clases de almacenamiento, consulte [Clases de almacenamiento de EFS](#) y [Administrar el almacenamiento del sistema de archivos](#).

Permisos de IAM para crear y restaurar copias de seguridad

Puede utilizar las acciones `elasticfilesystem:backup` y `elasticfilesystem:restore` para permitir o denegar a una entidad de IAM (como un usuario, grupo o función) la capacidad de crear o restaurar copias de seguridad de un sistema de archivos de EFS. Puede utilizar estas acciones en una política del sistema de archivos o en una política de IAM basada en la identidad. Para obtener más información, consulte [Administración de identidades y acceso Amazon Elastic File System](#) y [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#).

Copias de seguridad bajo demanda

Mediante la [consola de administración de AWS Backup](#) o la CLI, puede guardar un único recurso en un almacén de copias de seguridad bajo demanda. A diferencia de las copias de seguridad programadas, no tiene por qué crear un plan de copia de seguridad para iniciar una copia de seguridad bajo demanda. Puede seguir asignando un ciclo de vida a su copia de seguridad, que

traslada automáticamente el punto de recuperación en el nivel del almacenamiento en frío y crea una nota sobre cuándo eliminarlo.

Copias de seguridad simultáneas

AWS Backup limita las copias de seguridad a una copia de seguridad simultánea por recurso. Por lo tanto, las copias de seguridad programadas o bajo demanda podrían producir un error si ya hay un trabajo de copia de seguridad en proceso. Para obtener más información sobre los límites de AWS Backup, consulte [Límites de AWS Backup](#) en la Guía para desarrolladores de AWS Backup.

Copias de seguridad automáticas

Al crear un sistema de archivos mediante la consola de Amazon EFS, las copias de seguridad automáticas se activan de forma predeterminada. Puede activar las copias de seguridad automáticas después de crear el sistema de archivos mediante la CLI o la API. El plan de copias de seguridad EFS predeterminado utiliza la configuración AWS Backup recomendada para las copias de seguridad automáticas: copias de seguridad diarias con un período de retención de 35 días. Las copias de seguridad creadas con el plan de copias de seguridad de EFS predeterminado se almacenan en un almacén de copias de seguridad de EFS predeterminado, que también crea EFS en su nombre. Por lo general, el plan de copias de seguridad y el almacén de copias de seguridad predeterminados no se pueden eliminar. Puede editar la configuración predeterminada del plan de copias de seguridad mediante la consola. AWS Backup Para obtener más información, consulte [Opción 3: Creación de un plan de copias de seguridad](#) en la Guía para desarrolladores de AWS Backup. Puede ver todas las copias de seguridad automáticas y editar la configuración predeterminada del plan de copias de seguridad de EFS mediante la [consola de AWS Backup](#). Puede desactivar las copias de seguridad automáticas en cualquier momento mediante la consola o la CLI de Amazon EFS, tal y como se describe en la siguiente sección.

Amazon EFS aplica la clave de etiqueta del sistema `aws:elasticfilesystem:default-backup` con un valor de `enabled` a los sistemas de archivos de EFS cuando se habilitan las copias de seguridad automáticas.

Note

Las copias de seguridad automáticas están exentas de la configuración AWS Backup de exclusión del servicio. Para obtener más información, consulte [Introducción a AWS Backup](#) en la Guía para desarrolladores de AWS Backup.

Activación o desactivación de las copias de seguridad automáticas de sistemas de archivos existentes

Tras crear un sistema de archivos, se pueden activar o desactivar las copias de seguridad automáticas mediante la consola, la CLI o la API EFS.

Activar o desactivar las copias de seguridad automáticas de un sistema de archivos existente (consola)

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. En la página Sistemas de archivos, elija el sistema de archivos para el que desee activar o desactivar las copias de seguridad automáticas y muestre la página de Detalles del sistema de archivos.
3. Elija Editar en el panel de configuración General.
4.
 - Para activar las copias de seguridad automáticas, seleccione Habilitar copias de seguridad automáticas.
 - Para desactivar las copias de seguridad automáticas, quite Habilitar copias de seguridad automáticas.
5. Elija Guardar cambios.

Activar o desactivar las copias de seguridad automáticas de un sistema de archivos existente (CLI)

- Utilice el comando CLI `put-backup-policy` (la operación de API correspondiente es [PutBackupPolicy](#)) para activar o desactivar las copias de seguridad automáticas de un sistema de archivos existente.
- Utilice el siguiente comando para activar las copias de seguridad automáticas.

```
$ aws efs put-backup-policy --file-system-id fs-01234567 \  
--backup-policy Status="ENABLED"
```

EFS responde con la nueva política de copias de seguridad.

```
{  
  "BackupPolicy": {  
    "Status": "ENABLING"  
  }  
}
```

```
}
```

- Utilice el siguiente comando para desactivar las copias de seguridad automáticas.

```
$ aws efs put-backup-policy --file-system-id fs-01234567 \  
--backup-policy Status="DISABLED"
```

EFS responde con la nueva política de copias de seguridad.

```
{  
  "BackupPolicy": {  
    "Status": "DISABLING"  
  }  
}
```


Se utiliza AWS Backup para configurar manualmente las copias de seguridad

Al configurar manualmente AWS Backup las copias de seguridad del sistema de archivos, primero se crea un plan de copias de seguridad. El plan de copia de seguridad define la programación y el periodo de creación de copias de seguridad, la política de conservación, la política de ciclo de vida y las etiquetas. Puede crear un plan de respaldo mediante la [consola AWS Backup de administración](#), la AWS CLI, la o la AWS Backup API. Como parte de un plan de copia de seguridad, puede definir lo siguiente:

- Programación: cuándo se realiza la copia de seguridad
- Intervalo de copia de seguridad: el intervalo de tiempo durante el cual se debe iniciar la copia de seguridad
- Ciclo de vida: cuándo se debe mover un punto de recuperación al almacenamiento en frío y cuándo eliminarlo
- Almacén de copia de seguridad: almacén que se usa para organizar los puntos de recuperación creados por la regla de copia de seguridad

Tras crear el plan de copia de seguridad, se asignan los sistemas de archivos Amazon EFS específicos al plan de copia de seguridad utilizando etiquetas o el ID del sistema de archivos de Amazon EFS. Después de asignar un plan, AWS Backup empieza a crear automáticamente una


copia de seguridad del sistema de archivos de Amazon EFS en su nombre, de acuerdo con el plan de copia de seguridad definido. Puede usar la AWS Backup consola para administrar las configuraciones de respaldo o monitorear la actividad de respaldo. Para obtener más información, consulte la [Guía para desarrolladores de AWS Backup](#).

 Note

Los sockets y las canalizaciones con nombres no son compatibles y se omiten de las copias de seguridad.

Restauración de un punto de recuperación

Mediante la [consola de AWS Backup](#) o la CLI, puede restaurar un punto de recuperación en un nuevo sistema de archivos de EFS o en un sistema de archivos existente. Puede realizar una operación de restauración completa, que restaura todo el sistema de archivos. O bien, puede restaurar archivos y directorios específicos mediante una restauración parcial. Para restaurar un archivo o directorio concretos, debe especificar la ruta relativa relacionada con el punto de montaje. Por ejemplo, si el sistema de archivos está montado en `/user/home/myname/efs` y la ruta de archivo es `user/home/myname/efs/file1`, escriba `/file1`. Las rutas distinguen entre mayúsculas y minúsculas y no pueden contener caracteres especiales, caracteres comodín ni cadenas de expresiones (regex) regulares.

 Note

Para restaurar un punto de recuperación, los usuarios deben tener el permiso `backup:StartRestoreJob`.

Cuando realiza una restauración completa o parcial, el punto de recuperación se restaura en el directorio de restauración `aws-backup-restore_`*timestamp-of-restore*. Cuando finalice la restauración, podrá ver el directorio de restauración en la raíz del sistema de archivos. Si intenta realizar varias restauraciones de la misma ruta, es posible que existan varios directorios que contengan los elementos restaurados. Si la restauración no llega a completarse, podrá ver el directorio `aws-backup-failed-restore_`*timestamp-of-restore*. Debe eliminar manualmente los directorios `restore` y `failed-restore` cuando termine de usarlos.

Note

Para las restauraciones parciales en un sistema de archivos EFS existente, AWS Backup restaura los archivos y directorios en un nuevo directorio del directorio raíz del sistema de archivos. La jerarquía completa de los elementos especificados se conserva en el directorio de recuperación. Por ejemplo, si el directorio A contiene los subdirectorios B, C y D, AWS Backup conserva la estructura jerárquica cuando se recuperan A, B, C y D.

Tras restaurar un punto de recuperación, los fragmentos de datos que no se puedan restaurar en el directorio correspondiente se colocan en el directorio `aws-backup-lost+found`. Se podrían mover fragmentos a este directorio si se realizan modificaciones en el sistema de archivos mientras se produce la copia de seguridad.

Eliminación de copias de seguridad

La política de acceso al almacén de copia de seguridad de EFS predeterminada está configurada para denegar la eliminación de puntos de recuperación. Para eliminar las copias de seguridad existentes de sus sistemas de archivos EFS, debe cambiar la política de acceso al almacén. Si intenta eliminar un punto de recuperación de EFS sin modificar la política de acceso al almacén, recibirá el siguiente mensaje de error:

```
"Access Denied: Insufficient privileges to perform this action. Please consult with the account administrator for necessary permissions."
```

Para editar la política de acceso al almacén de la copia de seguridad predeterminada, debe tener permisos para editar las políticas. Para obtener más información, consulte [Permitir todas las acciones de IAM \(acceso de administrador\)](#) en la Guía del usuario de IAM.

Para eliminar un punto de recuperación de EFS en AWS Backup

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación izquierdo, elija Almacenes de copias de seguridad.
3. En la lista Almacenes de copias de seguridad, elija `aws/efs/automatic-backup-vault`.
4. En la página de detalles del almacén, elija Administrar acceso en la esquina superior derecha de la página. Aparece la página Editar política de acceso.

5. Para permitir todas las acciones en el almacén de copias de seguridad de EFS, busque la línea "Effect": "Deny", en el editor JSON y edítela para que se lea "Effect": "Allow",.
6. Elija Guardar política para guardar los cambios.
7. En la página de detalles del almacén, desplácese hacia abajo hasta la sección Copias de seguridad y seleccione los puntos de recuperación que desee eliminar de la lista de Copias de seguridad. A continuación, elija Acciones y, a continuación, Eliminar.
8. Siga las instrucciones para confirmar la eliminación. A continuación, elija Eliminar puntos de recuperación.

Replicación de sistemas de archivos

Puede crear una réplica de su sistema Región de AWS de archivos EFS según sus preferencias. Al habilitar la replicación en un sistema de archivos EFS, Amazon Elastic File System (Amazon EFS) replica de forma automática y transparente los datos y metadatos del sistema de archivos de origen en un sistema de archivos de destino. En caso de producirse una incidencia grave o cuando se realicen ejercicios de simulación de incidencias, puede realizar una conmutación por error a su sistema de archivos de réplica y, a continuación, realizar una conmutación por recuperación al sistema de archivos principal para reanudar las operaciones. Para gestionar el proceso de creación del sistema de archivos de destino y mantenerlo sincronizado con el sistema de archivos de origen, Amazon EFS utiliza una configuración de replicación. Para obtener más información acerca de la creación de una configuración de replicación para un sistema de archivos, consulte [Configuración de replicación](#).

Tras crear una configuración de replicación para un sistema de archivos, Amazon EFS mantiene sincronizados automáticamente los sistemas de archivos de origen y destino. Los cambios realizados en el sistema de archivos de origen no se transfieren al sistema de archivos de destino de manera point-in-time coherente, sino que se transfieren en función de la última hora de sincronización de la replicación. La hora de última sincronización indica cuándo se completó la última sincronización satisfactoria entre el origen y el destino. Los cambios realizados en el sistema de archivos de origen a partir de la hora de última sincronización se replican en el sistema de archivos de destino, y existe la posibilidad de que no se repliquen los cambios realizados en el sistema de archivos de origen después de la hora de última sincronización. Para obtener más información, consulte [Supervisión de estado de replicación](#).

La replicación está disponible en todos los Regiones de AWS lugares en los que EFS esté disponible. Para utilizar la replicación en una Región que está deshabilitada de forma predeterminada, primero debe inscribirse en la Región. Para obtener más información, consulte [Administración de Regiones de AWS](#) en la Guía de referencia general de AWS . Si más adelante decide por no participar en una región, Amazon EFS detiene todas las actividades de replicación de la región. Para reanudar las actividades de replicación en la región, debe volver a inscribirse en la Región de AWS.

Note

La replicación no admite el uso de etiquetas para el control de acceso basado en atributos (ABAC).

Temas

- [Configuración de replicación](#)
- [Crear una configuración de replicación](#)
- [Visualización de las configuraciones de replicación](#)
- [Eliminar configuraciones de replicación](#)
- [Supervisión de estado de replicación](#)

Configuración de replicación

Al crear la configuración de replicación para su sistema de archivos, usted elige la Región de AWS en la que desea crear la replicación y si desea replicarla en un sistema de archivos de destino nuevo o existente.

Note

Un sistema de archivos solo puede formar parte de una configuración de replicación. No puede usar un sistema de archivos de destino como sistema de archivos de origen en otra configuración de replicación.

Replicación en un nuevo sistema de archivos

Amazon EFS crea automáticamente un nuevo sistema de archivos y copia los datos y metadatos del sistema de archivos de origen en un nuevo sistema de archivos de destino de solo lectura Región de AWS que elija. El sistema de archivos de destino se crea con las propiedades siguientes:

- Tipo de sistema de archivos: el tipo de sistema de archivos determina la disponibilidad y durabilidad con las que un sistema de archivos Amazon EFS almacena los datos dentro de una Región de AWS.
 - Elija Regional para crear un sistema de archivos que almacene datos y metadatos de forma redundante en todas las zonas de disponibilidad de la Región de AWS.
 - Elija One Zone para crear un sistema de archivos que almacene datos y metadatos de forma redundante en una única zona de disponibilidad.

Para obtener más información sobre los tipos de sistema de archivos, consulte [Tipos de sistemas de archivos EFS](#).

- **Cifrado:** todos los sistemas de archivos de destino se crean con el cifrado en reposo activado. Puede especificar la clave AWS Key Management Service (AWS KMS) que se utiliza para cifrar el sistema de archivos de destino. Si no especifica una clave KMS, se utiliza la clave KMS administrada por el servicio para Amazon EFS.

 Important

Después de crear el sistema de archivos de destino, no se puede cambiar la clave KMS.

- **Copias de seguridad automáticas:** para los sistemas de archivos de destino que utilizan el almacenamiento One Zone, las copias de seguridad automáticas están habilitadas de forma predeterminada. Después de crear el sistema de archivos, puede cambiar la configuración de copia de seguridad automática. Para obtener más información, consulte [Copias de seguridad automáticas](#).
- **modo de rendimiento:** el modo de rendimiento del sistema de archivos de destino coincide con el del sistema de archivos de origen, a menos que el sistema de archivos de destino utilice el almacenamiento One Zone. En ese caso, se utiliza el modo de rendimiento de uso general. El modo de rendimiento no se puede cambiar.
- **modo de rendimiento:** el modo de rendimiento del sistema de archivos de destino coincide con el del sistema de archivos de origen. Después de crear el sistema de archivos, puede modificar el modo.

Si el modo de rendimiento del sistema de archivos de origen es aprovisionado, la cantidad de rendimiento aprovisionada del sistema de archivos de destino coincide con la del sistema de archivos de origen, a menos que la cantidad aprovisionada del archivo de origen supere el límite de la región del sistema de archivos de destino. Si la cantidad aprovisionada del sistema de archivos de origen supera el límite regional del sistema de archivos de destino, la cantidad de rendimiento aprovisionada del sistema de archivos de destino es el límite de la región. Para obtener más información, consulte [Cuotas de Amazon EFS que puede incrementar](#).

- **administración del ciclo de vida:** la administración del ciclo de vida no está habilitada en el sistema de archivos de destino. Después de crear el sistema de archivos de destino, puede activarlo. Para obtener más información, consulte [Administrar el almacenamiento del sistema de archivos](#).

Replicación en un sistema de archivos existente

EFS replica los datos y los metadatos del sistema de archivos de origen en el sistema de archivos de destino Región de AWS que usted elija. Durante la replicación, EFS identifica las diferencias de datos entre los sistemas de archivos y las aplica al sistema de archivos de destino.

Al replicar en un sistema de archivos existente, se aplican los siguientes requisitos.

- La protección de sobrescritura de replicación del sistema de archivos de destino debe estar deshabilitada. La protección contra sobrescritura de la replicación evita que los sistemas de archivos se utilicen como destino en una configuración de replicación. Para obtener más información acerca de deshabilitar la protección, consulte [Protección del sistema de archivos](#).

Para deshabilitar la protección contra la sobrescritura de la replicación, se requieren permisos para el `elasticfilesystem:action.UpdateFileSystemProtection`. Para obtener más información, consulte [política administrada por AWS: AmazonElasticfilesystemAccess](#).

- Si el sistema de archivos de origen está cifrado, el sistema de archivos de destino también debe estar cifrado. Además, si el archivo de origen no está cifrado y el sistema de archivos de destino está cifrado, no podrá volver al destino de origen tras realizar una conmutación por error. Para obtener más información sobre el cifrado, consulte [Cifrado de datos en Amazon EFS](#).

Protección del sistema de archivos

Al crear un sistema de archivos de Amazon EFS, su protección de sobrescritura de replicación se habilita de forma predeterminada. La protección contra sobrescritura de la replicación evita que el sistema de archivos se utilice como destino en una configuración de replicación. Para poder usar el sistema de archivos como destino en una configuración de replicación, debe deshabilitar la protección. Si elimina la configuración de replicación, se vuelve a activar la protección contra sobrescritura de la replicación del sistema de archivos y se puede escribir en el sistema de archivos.

Para deshabilitar la protección contra sobrescritura de la replicación se requieren permisos para la acción `elasticfilesystem:UpdateFileSystemProtection`. Para obtener más información, consulte [política administrada por AWS: AmazonElasticfilesystemAccess](#).

El estado de la protección contra sobrescritura de la replicación de un sistema de archivos de Amazon EFS puede tener uno de los valores que se describen en la siguiente tabla.

Estado del sistema de archivos	Descripción
ENABLED	El sistema de archivos no puede utilizarse como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos se puede escribir. La protección contra sobrescritura de la replicación es ENABLED de forma predeterminada.
DISABLED	El sistema de archivos puede utilizarse como el sistema de archivos de destino en una configuración de replicación.
REPLICATING	El sistema de archivos se utiliza como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos es de solo lectura y solo Amazon EFS lo modifica durante la replicación.

Para deshabilitar la protección contra sobrescritura de la replicación (consola)

1. Inicie sesión en la consola Amazon EFS AWS Management Console y ábrala en <https://console.aws.amazon.com/efs/>.
2. En el panel de navegación izquierdo, elija Sistemas de archivos.
3. En la lista Sistemas de archivos, elija el sistema de archivos Amazon EFS que desee utilizar como sistema de archivos de destino en un configuración de replicación.
4. En la sección Protección del sistema de archivos, desactive la Protección contra sobrescritura de la replicación.

Permisos necesarios

Amazon EFS utiliza la función vinculada al servicio de EFS denominada `AWSServiceRoleForAmazonElasticFileSystem` para sincronizar el estado de la replicación entre los sistemas de archivos de origen y destino. Para utilizar la replicación de EFS, debe configurar los siguientes permisos para permitir a una entidad de IAM (como un usuario, un grupo o un rol) crear un rol vinculado al servicio, una configuración de replicación y un sistema de archivos.

- `elasticfilesystem:CreateReplicationConfiguration*`
- `elasticfilesystem>DeleteReplicationConfiguration*`

- `elasticfilesystem:DescribeFileSystem`
- `elasticfilesystem:DescribeReplicationConfigurations`*
- `elasticfilesystem:CreateFileSystem`*
- `iam:CreateServiceLinkedRole` — consulte el ejemplo en [Uso de roles vinculados a servicios para Amazon EFS](#).

Note

* En su lugar, puede usar la política administrada por `AmazonElasticFileSystemFullAccess` para obtener automáticamente todos los permisos de EFS necesarios. Para obtener más información, consulte [política administrada por AWS: AmazonElasticfilesystemAccess](#).

Costos

Para facilitar la replicación, Amazon EFS crea directorios y metadatos ocultos en el sistema de archivos de destino. Esto equivale a aproximadamente 12 MiB de datos medidos por los que se le factura. Para obtener más información acerca de la medición del almacenamiento del sistema de archivos, consulte [Medición: cómo Amazon EFS registra el tamaño del sistema de archivos y el tamaño de los objetos](#).

Rendimiento

Cuando crea nuevas replicaciones o invierte la dirección de las replicaciones existentes durante el proceso de conmutación por recuperación, Amazon EFS realiza una sincronización inicial, que incluye una serie de acciones de configuración únicas para admitir la replicación. La cantidad de tiempo que la sincronización inicial necesita para realizarse depende de factores como el tamaño del sistema de archivos de origen y el número de archivos que contiene.

Una vez finalizada la replicación inicial, Amazon EFS mantiene un objetivo de punto de recuperación (RPO) de 15 minutos para la mayoría de los sistemas de archivos. Sin embargo, si el sistema de archivos de origen tiene archivos que cambian con mucha frecuencia y tiene más de 100 millones de archivos o archivos que ocupan más de 100 GB, la replicación puede tardar más de 15 minutos. Para obtener información sobre cómo supervisar cuándo finalizó correctamente la última replicación, consulte [Supervisión de estado de replicación](#).

Puedes monitorizar cuándo se produjo la última sincronización correcta mediante la consola, AWS Command Line Interface (AWS CLI), la API y Amazon CloudWatch. En CloudWatch, utilice la métrica [TimeSinceLastSyncEFS](#). Para obtener más información, consulte [Supervisión de estado de replicación](#).

Montaje de un sistema de archivos de destino

Amazon EFS no crea ningún destino de montaje cuando crea el sistema de archivos de destino. Para montar un sistema de archivos de destino, debe crear uno o más destinos de montaje. Para obtener más información, consulte [Montaje del sistema de archivos de EFS mediante el ayudante de montaje de EFS](#).

Como un sistema de archivos de destino es de solo lectura cuando es miembro de una configuración de replicación, cualquier operación de escritura en él fallará. Sin embargo, puede usar el sistema de archivos de destino para casos de uso de solo lectura, incluidas las pruebas y el desarrollo.

Conmutación por error y conmutación por recuperación del sistema de archivos

En caso de producirse una incidencia grave o cuando se realicen ejercicios de simulación de incidencias, puede realizar una conmutación por error a su sistema de archivos de réplica eliminando su configuración de replicación. Una vez eliminada la configuración de replicación, se puede escribir en la réplica y puede empezar a usarla en el flujo de trabajo de la aplicación. Cuando se elimina la incidencia grave o finaliza el ejercicio de simulación de incidencias, puede seguir utilizando la réplica como sistema de archivos principal o puede realizar una conmutación por recuperación para reanudar las operaciones en el sistema de archivos principal original.

Durante el proceso de conmutación por recuperación, puede optar por descartar los cambios realizados en el sistema de archivos de réplica o conservarlos copiándolos de nuevo en el sistema principal.

- Para descartar los cambios realizados en la réplica durante la conmutación por error, vuelva a crear la configuración de replicación original en el sistema de archivos principal, donde el sistema de archivos de réplica es el destino de la replicación. Durante la replicación, Amazon EFS sincroniza los sistemas de archivos actualizando los datos del sistema de archivos de réplica para que coincidan con los del sistema principal.
- Para replicar los cambios realizados en la réplica durante la conmutación por error, cree la configuración de replicación en el sistema de archivos de réplica, donde el sistema de archivos

principal es el destino de la replicación. Durante la replicación, Amazon EFS identifica y transfiere las diferencias del sistema de archivos de réplica al sistema de archivos principal. Una vez finalizada la replicación, puede reanudar la replicación del sistema de archivos principal recreando la configuración de replicación original o creando una nueva configuración.

El tiempo que tarda Amazon EFS en completar el proceso de replicación varía y depende de factores como el tamaño del sistema de archivos y el número de archivos que contiene. Para obtener más información, consulte [Rendimiento](#).

Crear una configuración de replicación


Puede utilizar la consola Amazon EFS, la API o la AWS CLI para replicar un sistema de archivos EFS. En las siguientes secciones se proporcionan instrucciones detalladas para utilizar cada uno de estos métodos.

Para crear un conjunto de configuración (consola)

1. Inicie sesión en la consola Amazon EFS AWS Management Console y ábrala en <https://console.aws.amazon.com/efs/>.
2. Abra el sistema de archivos que desea replicar:
 - a. En el panel de navegación izquierdo, elija Sistemas de archivos.
 - b. En la lista Sistemas de archivos, elija el sistema de archivos Amazon EFS que desee replicar. El sistema de archivos que elija no puede usarse como sistema de archivos de origen o destino en una configuración de replicación existente.
3. Seleccione la pestaña Replicación y, a continuación, en la sección Replicación, elija Crear replicación. Se abre la página Crear replicación.
4. En la sección Configuración de replicación, defina la configuración de replicación:
 - a. Para la Configuración de replicación, elija si desea replicar el sistema de archivos en un sistema de archivos nuevo o existente.
 - b. En Destination Región de AWS, elija el lugar Región de AWS en el que desea replicar el sistema de archivos.
5. Si va a replicar en un nuevo sistema de archivos de destino, en la sección Configuración del sistema de archivos de destino, defina la configuración del sistema de archivos de destino.


- a. En Tipo de sistema de archivos, elija una opción de almacenamiento para el sistema de archivos.
 - Para crear un sistema de archivos que almacene datos de forma redundante en varias zonas de disponibilidad separadas geográficamente dentro de una Región de AWS, elija Regional.
 - Para crear un sistema de archivos que almacene datos de forma redundante en una única zona de disponibilidad de una Región de AWS, elija Una zona y, a continuación, seleccione la zona de disponibilidad.

Para obtener más información, consulte [Tipos de sistemas de archivos EFS](#).

 Note

Los sistemas de archivos One Zone no están disponibles en todas las zonas de disponibilidad en la Regiones de AWS donde Amazon EFS está disponible.

- b. En el caso del Cifrado, el cifrado de los datos en reposo se habilita automáticamente en el sistema de archivos de destino. EFS utiliza su clave de servicio de AWS Key Management Service (AWS KMS) para Amazon EFS (aws/elasticfilesystem) de forma predeterminada. Para usar una clave de KMS diferente, elija una clave de KMS o introduzca el ARN de una clave existente.

 Important

Después de crear el sistema de archivos, no se puede cambiar la clave KMS.

6. Si va a replicar en un sistema de archivos de destino existente, elija Examinar EFS y, a continuación, seleccione el sistema de archivos. La ruta de acceso al sistema de archivos de destino aparece en el cuadro Destino.

Si la protección contra sobrescritura de la replicación está habilitada en el sistema de archivos, aparece una advertencia en la que se le pide que deshabilite la protección. Para deshabilitar la protección, seleccione Deshabilitar la protección y, a continuación, desactive la Protección contra sobrescritura de la replicación. Tras deshabilitar la protección, haga clic en el botón Actualizar para borrar el mensaje.

7. Elija Crear replicación. Si va a realizar la replicación en un nuevo sistema de archivos, aparecerá un mensaje en el que se le solicitará que confirme la replicación. Escriba confirmar en el cuadro de entrada y, a continuación, haga clic en Crear replicación.

Aparece la sección Replicación, que muestra los detalles de la replicación. El valor del estado de la replicación está activado inicialmente y el campo Última sincronización está en blanco. Cuando el estado sea Activado, Última sincronización muestra Sincronización inicial en curso.

8. Para ver la información de configuración del sistema de archivos de destino, elija el ID del sistema de archivos encima del sistema de archivos de destino. La página de detalles del sistema de archivos del sistema de archivos de destino aparece en una nueva pestaña del navegador (en función de la configuración del navegador).

Para crear una configuración de replicación (consola)

Para crear una configuración de replicación, utilice el comando `create-replication-configuration` de la CLI. El comando API equivalente es [CreateReplicationConfiguration](#).

Example : creación de una configuración de replicación para un sistema de archivos de destino Regional

En el siguiente ejemplo, se crea una configuración de replicación para el `fs-0123456789abcdef1` del sistema de archivos. En este ejemplo, se utiliza el `Region` parámetro para crear un sistema de archivos de destino en `eu-west-2` Región de AWS El parámetro `KmsKeyId` especifica el ID de la clave KMS que se va a utilizar al cifrar el sistema de archivos de destino.

```
aws efs create-replication-configuration \
--source-file-system-id fs-0123456789abcdef1 \
--destinations "[{\\"Region\\":\\"eu-west-2\\", \\"KmsKeyId\\":\\"arn:aws:kms:us-east-2:111122223333:key/abcd1234-ef56-ab78-cd90-1111abcd2222\\"}]"
```

AWS CLI Responde de la siguiente manera:

```
{
  "SourceFileSystemArn": "arn:aws:elasticfilesystem:us-east-1:111122223333:file-system/fs-0123456789abcdef1",
  "SourceFileSystemRegion": "us-east-1",
  "Destinations": [
    {
      "Status": "ENABLING",
      "FileSystemId": "fs-0123456789abcde22",
    }
  ]
}
```

```
        "Region": "eu-west-2"
    }
],
"SourceFileSystemId": "fs-0123456789abcdef1",
"CreationTime": 1641491892.0,
"OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:us-
east-1:111122223333:file-system/fs-0123456789abcdef1"
}
```

Example : creación de una configuración de replicación para un sistema de archivos de destino One Zone

En el siguiente ejemplo, se crea una configuración de replicación para el *fs-0123456789abcdef1* del sistema de archivos. En este ejemplo, se utiliza el parámetro `AvailabilityZoneName` para crear un sistema de archivos de destino One Zone en la zona de disponibilidad *us-west-2a*. Como no se especifica ninguna clave de KMS, el sistema de archivos de destino se cifra con la clave de AWS KMS servicio predeterminada de la cuenta para Amazon EFS (`aws/elasticfilesystem`).

```
aws efs create-replication-configuration \
--source-file-system-id fs-0123456789abcdef1 \
--destinations AvailabilityZoneName=us-west-2a
```

Visualización de las configuraciones de replicación

Para ver la configuración de replicación de un sistema de archivos, puede utilizar la consola Amazon EFS o la AWS CLI.

Para crear una configuración de replicación (consola)

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. En el panel de navegación izquierdo, elija Sistemas de archivos.
3. Elija un sistema de archivos de la lista.
4. Seleccione la pestaña Replicación para ver la sección Replicación.

En la sección Replicación, puede ver la siguiente información sobre la configuración de la replicación:

- El estado de replicación puede ser Activando, Activado, Eliminando, Pausando, En pausa o Error.

El estado de En pausa se produce como resultado de la exclusión voluntaria de la región de origen o destino después de crear la configuración de replicación. Para reanudar la replicación del sistema de archivos, debe volver a inscribirse en la Región de AWS. Para obtener más información, consulte [Administración de Regiones de AWS](#) en la Guía de referencia general de AWS .

El estado de replicación se produce después de crear una replicación, con el sistema de archivos como sistema de archivos de origen o de destino.

El estado de error se produce cuando el sistema de archivos de origen o de destino (o ambos) se encuentra en un estado de error e irrecuperable. Para obtener más información, consulte [Supervisión de estado de replicación](#) . Para recuperarlo, debe eliminar la configuración de replicación y, a continuación, restaurar la copia de seguridad más reciente del sistema de archivos defectuoso (ya sea el de origen o el de destino) en un nuevo sistema de archivos.

- La dirección de replicación muestra la dirección en la que se replican los datos. El primer sistema de archivos de la lista es el origen y sus datos se replican en el segundo sistema de archivos de la lista, que es el destino.
- Última sincronización muestra cuándo se produjo la última sincronización correcta en el sistema de archivos de destino. Todos los cambios en los datos del sistema de archivos de origen que se hayan producido antes de esa hora se han replicado correctamente en el sistema de archivos de destino. Es posible que cualquier cambio que se haya producido después de este tiempo no se haya replicado por completo.
- Los sistemas de archivos de replicación enumeran cada sistema de archivos de la configuración de replicación según su ID de sistema de archivos, la función que desempeña en la configuración de la Región de AWS replicación (origen o destino), su ubicación y su permiso. Un sistema de archivos de origen tiene el permiso de escritura y un sistema de archivos de destino tiene el permiso de solo lectura.

Para crear una configuración de replicación (CLI)

Para ver la configuración de replicación, utilice el comando `describe-replication-configurations` de la CLI. Puede ver la configuración de replicación de un sistema de archivos específico o todas las configuraciones de replicación de un sistema concreto Cuenta de AWS de un sistema Región de AWS. El comando API equivalente es [DescribeReplicationConfigurations](#).

Para ver la configuración de replicación de un sistema de archivos, utilice el parámetro de solicitud URI de `file-system-id`. Puede especificar el ID de un sistema de archivos de origen o de destino.

```
aws efs describe-replication-configurations --file-system-id fs-0123456789abcdef1
```

```
{
  "Replications": [
    {
      "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-west-1:111122223333:file-system/fs-abcdef0123456789a",
      "CreationTime": 1641491892.0,
      "SourceFileSystemRegion": "eu-west-1",
      "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-west-1:111122223333:file-system/fs-abcdef0123456789a",
      "SourceFileSystemId": "fs-abcdef0123456789a",
      "Destinations": [
        {
          "Status": "ENABLED",
          "FileSystemId": "fs-0123456789abcdef1",
          "Region": "us-east-1"
        }
      ]
    }
  ]
}
```

Para ver todas las configuraciones de replicación de una cuenta en un Región de AWS, no especifique el `file-system-id` parámetro.

```
aws efs describe-replication-configurations
```

```
{
  "Replications": [
    {
      "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-west-1:555555555555:file-system/fs-0123456789abcdef1",
      "CreationTime": 1641491892.0,
      "SourceFileSystemRegion": "eu-west-1",
      "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-west-1:555555555555:file-system/fs-0123456789abcdef1",
      "SourceFileSystemId": "fs-0123456789abcdef1",
    }
  ]
}
```



```

    "Destinations": [
      {
        "Status": "ENABLED",
        "FileSystemId": "fs-abcdef0123456789a",
        "Region": "us-east-1",
        "LastReplicatedTimestamp": 1641491802.375
      }
    ],
    {
      "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-021345abcdef6789a",
      "CreationTime": 1641491822.0,
      "SourceFileSystemRegion": "eu-west-1",
      "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-021345abcdef6789a",
      "SourceFileSystemId": "fs-021345abcdef6789a",
      "Destinations": [
        {
          "Status": "ENABLED",
          "FileSystemId": "fs-012abc3456789def1",
          "Region": "us-east-1",
          "LastReplicatedTimestamp": 1641491823.575
        }
      ]
    }
  ]
}

```

Eliminar configuraciones de replicación

Si necesita realizar una conmutación por error al sistema de archivos de destino, elimine la configuración de replicación de la que es miembro. Tras eliminar una configuración de replicación, se puede escribir en el sistema de archivos de destino y se vuelve a habilitar su protección contra sobrescritura de la replicación. Para obtener más información, consulte [Conmutación por error y conmutación por recuperación del sistema de archivos](#).

Eliminar una configuración de replicación y cambiar el sistema de archivos de destino para que se pueda escribir puede tardar varios minutos en completarse. Tras eliminar la configuración, Amazon EFS podría escribir algunos datos en un directorio `lost+found` del directorio raíz del sistema de archivos de destino, utilizando la siguiente convención de nomenclatura:

```
efs-replication-lost+found-source-file-system-id-TIMESTAMP
```

Note

No se puede eliminar un sistema de archivos que forme parte de una configuración de replicación. Debe eliminar la configuración de replicación antes de eliminar el sistema de archivos.

Puede eliminar una configuración de replicación existente del sistema de archivos de origen o de destino mediante la consola, la CLI o la API.

Para eliminar una configuración de replicación (consola)

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. En el panel de navegación izquierdo, elija Sistemas de archivos.
3. Elija el sistema de archivos de origen o de destino que se encuentra en la configuración de replicación que desea eliminar.
4. Seleccione la pestaña Replicación para ver la sección Replicación.
5. Elija Eliminar replicación para eliminar la configuración de replicación. Cuando se le indique, confirme su elección.

Para eliminar una configuración de replicación (CLI)

Para eliminar una configuración de replicación, utilice el comando `delete-replication-configuration` de la CLI. El comando API equivalente es [DeleteReplicationConfiguration](#).

Para especificar qué configuración de replicación va a eliminar, utilice el parámetro `source-file-system-id`.

```
aws efs --region us-west-2 delete-replication-configuration \  
--source-file-system-id fs-0123456789abcdef1
```

Supervisión de estado de replicación

Puede supervisar el momento en que se completó la última sincronización correcta en una configuración de replicación. Todos los cambios en los datos del sistema de archivos de origen que

se hayan producido antes de esa hora se han replicado correctamente en el sistema de archivos de destino. Es posible que cualquier cambio que se haya producido después de este tiempo no se haya replicado por completo. Para supervisar cuándo finalizó correctamente la última replicación, puede utilizar la consola, la CLI, la API o Amazon CloudWatch.

- En la consola: la propiedad Última sincronización de la sección Detalles del sistema de archivos > Replicación muestra la hora en que se completó la última sincronización correcta entre el origen y el destino.
- En la CLI o la API: la propiedad `LastReplicatedTimestamp` del objeto `Destination` muestra la hora en que se completó la última sincronización correcta. Para acceder a esta propiedad, utilice el comando `describe-replication-configurations` de la CLI. [DescribeReplicationConfigurations](#) es la operación de API equivalente.
- En CloudWatch: la `TimeSinceLastSync` CloudWatch métrica de Amazon EFS muestra el tiempo transcurrido desde que se completó la última sincronización correcta. Para obtener más información, consulte [CloudWatch Métricas de Amazon para Amazon EFS](#).

También puede supervisar el estado de una configuración de replicación mediante la consola, la CLI o la API. Una configuración de replicación puede tener uno de los valores de estado que se describen en la siguiente tabla.

Estado de replicación	Descripción
ENABLED	La configuración de replicación está en buen estado y disponible para su uso.
ENABLING	Amazon EFS está creando la configuración de replicación.
DELETING	Amazon EFS está eliminando la configuración de replicación en respuesta a una solicitud de eliminación iniciada por el usuario.
PAUSING	Amazon EFS está pausando la replicación, como resultado de haber excluido la región de uno o ambos sistemas de archivos de la configuración de replicación.
PAUSED	La replicación se detiene como resultado de la exclusión de la región para uno o ambos sistemas de archivos de la configuración de replicación. Para reanudar la replicación, debe volver a inscribirse en la Región de AWS. Para

Estado de replicación	Descripción
	obtener más información, consulte Administración de Regiones de AWS en la Guía de referencia general de AWS .
ERROR	Uno (o ambos) de los sistemas de archivos de la configuración de replicación está en un estado fallido e irrecuperable. Para acceder a los datos del sistema de archivos, restaure una copia de seguridad del sistema de archivos defectuoso en un sistema de archivos nuevo. Para obtener más información, consulte Restauración de un punto de recuperación .

Tutoriales de Amazon Elastic File System

Esta sección ofrece tutoriales que puede usar para explorar Amazon EFS y probar la configuración integral.

Temas

- [Tutorial: Cree un sistema de archivos Amazon EFS y móntelo en una instancia de Amazon EC2 mediante AWS CLI](#)
- [Tutorial: Configurar un servidor web Apache y ofrecer archivos de Amazon EFS](#)
- [Tutorial: Crear subdirectorios que se pueden escribir por usuario y configurar la opción de volver a montar automáticamente al reiniciar](#)
- [Tutorial: Crear y montar un sistema de archivos en las instalaciones con AWS Direct Connect y una VPN](#)
- [Tutorial: Montar un sistema de archivos desde una VPC distinta](#)
- [Tutorial: Aplicar cifrado en reposo a un sistema de archivos de Amazon EFS](#)
- [Tutorial: Habilite la eliminación raíz mediante la autorización de IAM para clientes NFS](#)

Tutorial: Cree un sistema de archivos Amazon EFS y móntelo en una instancia de Amazon EC2 mediante AWS CLI

En este tutorial, se utiliza AWS CLI para explorar la API de Amazon EFS. En este tutorial, crea un sistema de archivos cifrado de Amazon EFS, lo monta en una instancia Amazon EC2 en su VPC y prueba la configuración.

Note

Este tutorial es similar al ejercicio de introducción. En el ejercicio [Introducción](#), utiliza la consola para crear recursos de EC2 y Amazon EFS. En este tutorial, utilizará la AWS CLI para hacer lo mismo, principalmente para familiarizarse con la API de Amazon EFS.

En este tutorial, creará los siguientes AWS recursos en su cuenta:

- Recursos de Amazon EC2:

- Dos grupos de seguridad (para la instancia de EC2 y el sistema de archivos de Amazon EFS).

Añada reglas a los grupos de seguridad para autorizar el acceso de entrada/salida adecuado. De este modo, la instancia EC2 puede conectarse al sistema de archivos a través del destino de montaje mediante un puerto TCP NFSv4.1 estándar.

- Una instancia EC2 de Amazon en su VPC.
- Recursos de Amazon EFS:
 - Un sistema de archivos.
 - Un destino de montaje para su sistema de archivos.

Para montar su sistema de archivos en una instancia EC2 tiene que crear un destino de montaje en la VPC. Puede crear un destino de montaje en cada una de las zonas de disponibilidad de la VPC. Para obtener más información, consulte [Cómo funciona Amazon EFS](#).

A continuación, prueba el sistema de archivos en su instancia EC2. El paso de limpieza al final del tutorial le ofrece información para que elimine estos recursos.

El tutorial crea todos estos recursos en la región Oeste de EE. UU. (Oregón) (us-west-2). Sea cual sea el Región de AWS que utilices, asegúrate de usarlo de forma coherente. Todos sus recursos (su VPC, los recursos de EC2 y los recursos de Amazon EFS) deben estar en la misma Región de AWS.

Antes de empezar

- Puedes usar tus credenciales raíz Cuenta de AWS para iniciar sesión en la consola e intentar el ejercicio de introducción. Sin embargo, AWS Identity and Access Management (IAM) recomienda que no utilice las credenciales raíz de su Cuenta de AWS. En su lugar, cree un usuario administrador en su cuenta y utilice esas credenciales para administrar los recursos de su cuenta. En su lugar, cree un usuario administrador en su cuenta y utilice esas credenciales para administrar los recursos de su cuenta. Para obtener más información, consulte [Asignar Cuenta de AWS acceso a un usuario del Centro de identidades de IAM](#) en la Guía del AWS IAM Identity Center usuario.
- Puede utilizar una VPC predeterminada o una VPC personalizada que haya creado en su cuenta. Para este tutorial, la configuración de la VPC predeterminada funciona. Sin embargo, si utiliza una VPC personalizada, verifique lo siguiente:
 - Los nombres de host de DNS están habilitados. A fin de obtener más información, consulte [Actualización de soporte de DNS para su VPC](#) en la guía del usuario de Amazon VPC.

- La gateway de Internet está conectada a su VPC. Para obtener más información, consulte [Gateways de Internet](#) en la Guía del usuario de Amazon VPC.
- Las subredes de VPC se configuran para solicitar direcciones IP públicas para instancias lanzadas en las subredes de la VPC. Para obtener más información, consulte [Direcciones IP en su VPC](#) en la Guía del usuario de Amazon VPC.
- La tabla de ruteo de la VPC incluye una regla para enviar todo el tráfico vinculado a Internet a la gateway de Internet.
- Debe configurar el perfil de administrador/usuario AWS CLI y añadirlo.

Configurando el AWS CLI

Utilice las siguientes instrucciones para configurar el perfil de usuario AWS CLI y.

Para configurar el AWS CLI

1. Descargue y configure la AWS CLI. Para obtener instrucciones, consulte los siguientes temas en la Guía del usuario de AWS Command Line Interface .

[Cómo configurarlo con la interfaz de línea de AWS comandos](#)

[Instalación de la interfaz de línea de AWS comandos](#)

[Configuración de la interfaz de línea de AWS comandos](#)

2. Definir perfiles.

Las credenciales de usuario se almacenan en el AWS CLI config archivo. Los comandos CLI de ejemplo de este tutorial especifican el perfil adminuser. Cree el perfil adminuser en el archivo config. También puede definir el perfil de usuario del administrador como predeterminado en el archivo config como se muestra.

```
[profile adminuser]
aws_access_key_id = admin user access key ID
aws_secret_access_key = admin user secret access key
region = us-west-2

[default]
aws_access_key_id = admin user access key ID
aws_secret_access_key = admin user secret access key
```

```
region = us-west-2
```

El perfil anterior también establece el valor predeterminado Región de AWS. Si no especifica una región en el comando de la CLI, se supone la región us-west-2.

3. Verifique la configuración introduciendo el siguiente comando en el símbolo del sistema. Ambos comandos no proporcionan las credenciales de forma explícita, por lo que se utilizan las credenciales del perfil predeterminado.

- Pruebe el comando de ayuda

También puede especificar el perfil de usuario de forma explícita añadiendo el parámetro `--profile`.

```
aws help
```

```
aws help \  
--profile adminuser
```

Siguiente paso

[Paso 1: Crear los recursos de Amazon ECS](#)

Paso 1: Crear los recursos de Amazon ECS

En este paso, hará lo siguiente:

- Cree dos grupos de seguridad.
- Añada reglas a los grupos de seguridad para autorizar el acceso adicional.
- Lanzar una instancia EC2. Cree y monte un sistema de archivos de Amazon EFS en esta instancia en el siguiente paso.

Temas

- [Paso 1.1: Crear dos grupos de seguridad](#)
- [Paso 1.2: Añadir reglas a los grupos de seguridad para autorizar el acceso de entrada/salida](#)
- [Paso 1.3: Lanzar una instancia EC2](#)

Paso 1.1: Crear dos grupos de seguridad

En esta sección, crea grupos de seguridad en su VPC para la instancia de EC2 y el destino de montaje de Amazon EFS. Más adelante en el tutorial, asigna estos grupos de seguridad a una instancia de EC2 y un destino de montaje de Amazon EFS. Para obtener información sobre los grupos de seguridad, consulte Grupos de [seguridad de Amazon EC2 para instancias de Linux](#).

Para crear grupos de seguridad

1. Crear dos grupos de seguridad utilizando el comando de la CLI `create-security-group`:
 - a. Cree un grupo de seguridad (`efs-walkthrough1-ec2-sg`) para la instancia EC2 y proporcionar el ID de su VPC.

```
$ aws ec2 create-security-group \  
--region us-west-2 \  
--group-name efs-walkthrough1-ec2-sg \  
--description "Amazon EFS walkthrough 1, SG for EC2 instance" \  
--vpc-id vpc-id-in-us-west-2 \  
--profile adminuser
```

Anote el ID del grupo de seguridad. A continuación, se muestra un ejemplo de respuesta.

```
{  
  "GroupId": "sg-aexample"  
}
```

Puede encontrar el ID de la VPC utilizando el siguiente comando.

```
$ aws ec2 describe-vpcs
```

- b. Cree un grupo de seguridad (`efs-walkthrough1-mt-sg`) para su destino de montaje de Amazon EFS. Tiene que proporcionar su ID de VPC.

```
$ aws ec2 create-security-group \  
--region us-west-2 \  
--group-name efs-walkthrough1-mt-sg \  
--description "Amazon EFS walkthrough 1, SG for mount target" \  
--vpc-id vpc-id-in-us-west-2 \  

```

```
--profile adminuser
```

Anote el ID del grupo de seguridad. A continuación, se muestra un ejemplo de respuesta.

```
{  
  "GroupId": "sg-aexample"  
}
```

2. Verifique los grupos de seguridad.

```
aws ec2 describe-security-groups \  
--group-ids list of security group IDs separated by space \  
--profile adminuser \  
--region us-west-2
```

Ambos deben tener solo una regla de salida que permita que todo el tráfico salga.

En la siguiente sección, autoriza el acceso adicional que permite lo siguiente:

- Permitirle conectar a su instancia EC2.
- Habilite el tráfico entre una instancia de EC2 y un destino de montaje de Amazon EFS (al que asociará estos grupos de seguridad más adelante en este tutorial).

Paso 1.2: Añadir reglas a los grupos de seguridad para autorizar el acceso de entrada/salida

En este paso, añada reglas a los grupos de seguridad para autorizar el acceso de entrada/salida.

Para añadir reglas

1. Autorice las conexiones Secure Shell (SSH) de entrada al grupo de seguridad para la instancia EC2 (`efs-walkthrough1-ec2-sg`) para que pueda conectarse a la instancia EC2 mediante SSH desde cualquier host.

```
$ aws ec2 authorize-security-group-ingress \  
--group-id id of the security group created for EC2 instance \  
--protocol tcp \  
--port 22 \  
--cidr 0.0.0.0/0 \  
--profile adminuser \  

```

```
--region us-west-2
```

Compruebe que el grupo de seguridad tenga la regla de entrada y salida que ha añadido.

```
aws ec2 describe-security-groups \  
--region us-west-2 \  
--profile adminuser \  
--group-id security-group-id
```

2. Autorice el acceso de entrada al grupo de seguridad para el destino de montaje de Amazon EFS (efs-walkthrough1-mt-sg).

En la línea de comandos, ejecute el siguiente AWS CLI `authorize-security-group-ingress` comando con el perfil `adminuser` para añadir la regla de entrada.

```
$ aws ec2 authorize-security-group-ingress \  
--group-id ID of the security group created for Amazon EFS mount target \  
--protocol tcp \  
--port 2049 \  
--source-group ID of the security group created for EC2 instance \  
--profile adminuser \  
--region us-west-2
```

3. Compruebe que ambos grupos de seguridad autorizan ahora el acceso de entrada.

```
aws ec2 describe-security-groups \  
--group-names efs-walkthrough1-ec2-sg efs-walkthrough1-mt-sg \  
--profile adminuser \  
--region us-west-2
```

Paso 1.3: Lanzar una instancia EC2

En este paso, lance una instancia EC2.


Para iniciar una instancia de EC2

1. Reúna la siguiente información que debe proporcionar al lanzar una instancia EC2:

- Nombre del par de claves:
 - Para obtener información introductoria, consulte [Configuración para usar Amazon EC2](#).

- Para obtener instrucciones sobre cómo crear un archivo.pem, consulte [Creación de un par de claves](#) en la Guía del usuario de Amazon EC2.
- El ID único de la imagen de Amazon Machine (AMI) que desea lanzar.

El AWS CLI comando que utilice para lanzar una instancia EC2 requiere el ID de la AMI que desee implementar como parámetro. El ejercicio utiliza la AMI de Amazon Linux HVM.

 Note

Puede utilizar la mayoría de las AMI basadas en Linux de uso general. Si utiliza otra AMI de Linux, asegúrese de utilizar el administrador de paquetes de la distribución para instalar el cliente de NFS en la instancia. Además, es posible que tenga que añadir paquetes de software conforme los necesite.

Para la AMI de Amazon Linux HVM, puede encontrar los ID más recientes en [AMI de Amazon Linux](#). Usted elige el valor de ID de la tabla de ID de la AMI de Amazon Linux de la siguiente manera:

- Elija la región EE. UU. Oeste (Oregón). Este tutorial supone que está creando todos los recursos en la región Oeste de EE. UU. (Oregón) (us-west-2).
- Elija el tipo EBS-backed HVM 64-bit (porque en el comando de la CLI especifica el tipo de instancia t2.micro, que no admite el almacén de instancias).
- ID del grupo de seguridad que ha creado para una instancia EC2.
- Región de AWS. Este tutorial utiliza la región us-west-2.
- Su ID de subred de VPC donde desea lanzar la instancia. Puede obtener la lista de subredes utilizando el comando describe-subnets.

```
$ aws ec2 describe-subnets \
  --region us-west-2 \
  --filters "Name=vpc-id,Values=vpc-id" \
  --profile adminuser
```

Después de elegir el ID de subred, anote los siguientes valores del resultado de describe-subnets:

- ID de subred: necesita este valor a la hora de crear un destino de montaje. En este ejercicio, deberá crear un destino de montaje en la misma subred en la que lanza una instancia EC2.
- Zona de disponibilidad de la subred: necesita este valor para construir el nombre de DNS de su destino de montaje, que se utiliza para montar un sistema de archivos en la instancia EC2.

2. Ejecute el siguiente AWS CLI `run-instances` comando para lanzar una instancia EC2.

```
$ aws ec2 run-instances \  
--image-id AMI ID \  
--count 1 \  
--instance-type t2.micro \  
--associate-public-ip-address \  
--key-name key-pair-name \  
--security-group-ids ID of the security group created for EC2 instance \  
--subnet-id VPC subnet ID \  
--region us-west-2 \  
--profile adminuser
```

3. Anote el ID de instancia devuelto por el comando `run-instances`.
4. La instancia de EC2 que ha creado deben tener un nombre de DNS público que utilice para conectarse a la instancia EC2 y montar el sistema de archivos en ella. El nombre de DNS público tiene el siguiente formato:

```
ec2-xx-xx-xx-xxx.compute-1.amazonaws.com
```

Ejecute el siguiente comando de la CLI y anote el nombre de DNS público.

```
aws ec2 describe-instances \  
--instance-ids EC2 instance ID \  
--region us-west-2 \  
--profile adminuser
```

Si no encuentra el nombre de DNS público, compruebe la configuración de la VPC en la que ha lanzado la instancia EC2. Para obtener más información, consulte [Antes de empezar](#).

5. (Opcional) Asigne un nombre a la instancia EC2 que ha creado. Para ello, añada una etiqueta con el nombre de clave y el valor establecido en el nombre que desea asignar a la instancia. Para ello, ejecute el siguiente AWS CLI `create-tags` comando.

```
$ aws ec2 create-tags \  
--resources EC2-instance-ID \  
--tags Key=Name,Value=Provide-instance-name \  
--region us-west-2 \  
--profile adminuser
```

Siguiente paso

[Paso 2: Crear los recursos de Amazon EFS](#)

Paso 2: Crear los recursos de Amazon EFS

En este paso, hará lo siguiente:

- Cree un sistema de archivos de EFS cifrado.
- Habilitar la administración del ciclo de vida
- Cree un destino de montaje en la zona de disponibilidad en la que ha lanzado la instancia EC2.

Temas

- [Paso 2.1: Crear un sistema de archivos de Amazon EFS](#)
- [Paso 2.2: Habilitar la administración del ciclo de vida](#)
- [Paso 2.3: Crear un destino de montaje](#)

Paso 2.1: Crear un sistema de archivos de Amazon EFS

En este paso, se crea un sistema de archivos de Amazon EFS. Anote el `FileSystemId` para utilizarlo posteriormente al crear destinos de montaje para el sistema de archivos en el siguiente paso.

Para crear un sistema de archivos

- Cree un sistema de archivos con la etiqueta `Name` opcional.
 - a. En la línea de comandos, ejecute el siguiente `create-file-system` comando AWS CLI.

```
$ aws efs create-file-system \  

```

```
--encrypted \  
--creation-token FileSystemForWalkthrough1 \  
--tags Key=Name,Value=SomeExampleNameValue \  
--region us-west-2 \  
--profile adminuser
```

Obtendrá la siguiente respuesta.

```
{  
  "OwnerId": "111122223333",  
  "CreationToken": "FileSystemForWalkthrough1",  
  "FileSystemId": "fs-c657c8bf",  
  "CreationTime": 1548950706.0,  
  "LifecycleState": "creating",  
  "NumberOfMountTargets": 0,  
  "SizeInBytes": {  
    "Value": 0,  
    "ValueInIA": 0,  
    "ValueInStandard": 0  
  },  
  "PerformanceMode": "generalPurpose",  
  "Encrypted": true,  
  "KmsKeyId": "arn:aws:kms:us-west-2:111122223333:a5c11222-7a99-43c8-9dcc-  
abcdef123456",  
  "ThroughputMode": "bursting",  
  "Tags": [  
    {  
      "Key": "Name",  
      "Value": "SomeExampleNameValue"  
    }  
  ]  
}
```

- b. Anote el valor `FileSystemId`. Necesitará este valor cuando cree un destino de montaje para este sistema de archivos en [Paso 2.3: Crear un destino de montaje](#).

Paso 2.2: Habilitar la administración del ciclo de vida

En este paso, habilita la administración del ciclo de vida en su sistema de archivos para utilizar la clase de almacenamiento Acceso poco frecuente. Para obtener más información, consulte [Administrar el almacenamiento del sistema de archivos](#) y [Clases de almacenamiento de EFS](#).

Para habilitar la administración del ciclo de vida

- En la línea de comandos, ejecute el siguiente AWS CLI `put-lifecycle-configuration` comando.

```
$ aws efs put-lifecycle-configuration \  
--file-system-id fs-c657c8bf \  
--lifecycle-policies TransitionToIA=AFTER_30_DAYS \  
--region us-west-2 \  
--profile adminuser
```

Obtendrá la siguiente respuesta.

```
{  
  "LifecyclePolicies": [  
    {  
      "TransitionToIA": "AFTER_30_DAYS"  
    }  
  ]  
}
```

Paso 2.3: Crear un destino de montaje

En este paso, crea un destino de montaje para el sistema de archivos en la zona de disponibilidad en la que se ha lanzado la instancia EC2.

1. Asegúrese de que dispone de la siguiente información:

- ID del sistema de archivos (por ejemplo, `fs-example`) para el que se crea el destino de montaje.
- ID de subred de VPC en la que ha lanzado la instancia EC2 en el [Paso 1](#).

En este tutorial, crea el destino de montaje en la misma subred en la que ha lanzado la instancia EC2, por lo que necesita el ID de subred (por ejemplo, `subnet-example`).

- ID del grupo de seguridad que ha creado para el destino de montaje en el paso anterior.
2. En la línea de comandos, ejecute el siguiente AWS CLI `create-mount-target` comando.


```
$ aws efs create-mount-target \  
--file-system-id file-system-id \  
--subnet-id subnet-id \  
--security-group ID-of-the security-group-created-for-mount-target \  
--region us-west-2 \  
--profile adminuser
```

Obtendrá la siguiente respuesta.

```
{  
  "MountTargetId": "fsmt-example",  
  "NetworkInterfaceId": "eni-example",  
  "FileSystemId": "fs-example",  
  "PerformanceMode" : "generalPurpose",  
  "LifecycleState": "available",  
  "SubnetId": "fs-subnet-example",  
  "OwnerId": "account-id",  
  "IpAddress": "xxx.xx.xx.xxx"  
}
```

3. También puede utilizar el comando `describe-mount-targets` para obtener las descripciones de los destinos de montaje que ha creado en un sistema de archivos.

```
$ aws efs describe-mount-targets \  
--file-system-id file-system-id \  
--region us-west-2 \  
--profile adminuser
```

Siguiente paso

[Paso 3: Montar el sistema de archivos en la instancia EC2 y probar](#)

Paso 3: Montar el sistema de archivos en la instancia EC2 y probar

En este paso, hará lo siguiente:

Temas

- [Paso 3.1: Recopilar información](#)
- [Paso 3.2: Instalar el cliente NFS en la instancia EC2](#)

- [Paso 3.3: Montar el sistema de archivos en su instancia de EC2 y probar](#)

Paso 3.1: Recopilar información

Asegúrese de que dispone de la siguiente información a medida que siga los pasos de esta sección:

- Nombre de DNS público de su instancia EC2 en el siguiente formato:

```
ec2-xx-xxx-xxx-xx.aws-region.compute.amazonaws.com
```

- Nombre de DNS de su sistema de archivos. Puede construir este nombre de DNS usando el siguiente formulario genérico:

```
file-system-id.efs.aws-region.amazonaws.com
```

La instancia EC2 en la que se monta el sistema de archivos mediante el destino de montaje puede resolver el nombre DNS del sistema de archivos en la dirección IP del destino de montaje.

Note

Amazon EFS no requiere que su instancia de Amazon EC2 tenga una dirección IP pública o un nombre de DNS público. Los requisitos indicados con anterioridad son solo para este ejemplo del tutorial, para garantizar que podrá conectarse a través de SSH a la instancia desde fuera de la VPC.

Paso 3.2: Instalar el cliente NFS en la instancia EC2

Puede conectarse a la instancia EC2 desde Windows o desde un equipo que ejecute Linux, macOS X o cualquier otra variante de Unix.

Para instalar un cliente NFS

1. Conéctese a su instancia EC2:

- Para conectarse a la instancia desde un equipo que ejecute macOS o Linux, especifique el archivo `.pem` para su comando SSH con la opción `-i` y la ruta a su clave privada.

- Para conectarte a la instancia desde un ordenador con Windows, puedes usar PuTTY, MindTerm o bien. Si pretende utilizar PuTTY, debe instalarlo y utilizar el siguiente procedimiento para convertir el archivo.pem a un archivo.ppk.

Para obtener más información, consulte los siguientes temas de la Guía del usuario de Amazon EC2:

- [Conéctate a tu instancia de Linux desde Windows con PuTTY](#)
- [Conéctate a tu instancia de Linux desde Linux o macOS mediante SSH](#)

2. Ejecute los siguientes comandos en la instancia EC2 usando la sesión de SSH:


- a. (Opcional) Obtener actualizaciones y reiniciar.

```
$ sudo yum -y update
$ sudo reboot
```

Tras el reinicio, vuelva a conectarse a su instancia EC2.

- b. Instale el cliente NFS.

```
$ sudo yum -y install nfs-utils
```

 Note

Si elige la AMI de Amazon Linux Amazon Linux AMI 2016.03.0 al lanzar su instancia de Amazon EC2, no tendrá que instalar `nfs-utils`, porque ya está incluido en la AMI de forma predeterminada.

Paso 3.3: Montar el sistema de archivos en su instancia de EC2 y probar

Ahora monta el sistema de archivos en su instancia EC2.

1. Haga un directorio ("efs-mount-point").

```
$ mkdir ~/efs-mount-point
```

2. Monte el sistema de archivos de Amazon EFS.

```
$ sudo mount -t nfs -o
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-DNS:/ ~/efs-mount-point
```

La instancia EC2 puede resolver el nombre de DNS del destino de montaje a la dirección IP. Como alternativa, puede especificar la dirección IP del destino de montaje directamente.

```
$ sudo mount -t nfs -o
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-ip:/ ~/efs-mount-point
```

3. Ahora que tiene el sistema de archivos de Amazon EFS montado en la instancia de EC2, puede crear archivos.

- a. Cambie el directorio.

```
$ cd ~/efs-mount-point
```

- b. Enumera el contenido del directorio.

```
$ ls -al
```

Debe estar vacío.

```
drwxr-xr-x 2 root    root    4096 Dec 29 22:33 .
drwx----- 4 ec2-user ec2-user 4096 Dec 29 22:54 ..
```

- c. El directorio raíz de un sistema de archivos, en el momento de su creación, es propiedad del usuario raíz que es quien puede escribir en el mismo, por lo que es necesario cambiar los permisos para añadir archivos.

```
$ sudo chmod go+rw .
```

Ahora, si prueba el comando `ls -al` verá que los permisos se han modificado.

```
drwxrwxrwx 2 root    root    4096 Dec 29 22:33 .
drwx----- 4 ec2-user ec2-user 4096 Dec 29 22:54 ..
```

- d. Cree un archivo de texto .

```
$ touch test-file.txt
```

- e. Genere un listado del contenido del directorio.

```
$ ls -l
```

Ya ha creado y montado correctamente un sistema de archivos de Amazon EFS en la instancia de EC2 en su VPC.

El sistema de archivos que ha montado no persistirá una vez que se reinicie. Para volver a montar automáticamente el directorio, puede utilizar el archivo `fstab`. Para obtener más información, consulte [Remontaje automático al reiniciar](#). Si está utilizando un grupo de Auto Scaling para lanzar instancias EC2, también puede definir scripts en una configuración de lanzamiento. Para ver un ejemplo, consulte [Tutorial: Configurar un servidor web Apache y ofrecer archivos de Amazon EFS](#).

Siguiente paso

[Paso 4: Limpiar](#)

Paso 4: Limpiar

Si ya no necesita los recursos que ha creado, debe eliminarlos. Puede hacerlo con la CLI.

- Elimine los recursos de EC2 (la instancia de EC2 y los dos grupos de seguridad). Amazon EFS elimina la interfaz de red al eliminar el destino de montaje.
- Elimine los recursos de Amazon EFS (sistema de archivos, destino de montaje).

Para eliminar AWS los recursos creados en este tutorial

1. Finalice la instancia EC2 que ha creado para este tutorial.

```
$ aws ec2 terminate-instances \
  --instance-ids instance-id \
  --profile adminuser
```

También puede eliminar recursos de EC2 a través de la consola. Para obtener instrucciones, consulte [Terminar una instancia](#).

2. Eliminar el destino de montaje.

Debe eliminar los destinos de montaje creados para el sistema de archivos antes de eliminar el sistema de archivos. Puede obtener una lista de destinos de montaje utilizando el comando de la CLI `describe-mount-targets`.

```
$ aws efs describe-mount-targets \  
--file-system-id file-system-ID \  
--profile adminuser \  
--region aws-region
```

A continuación, elimine el destino de montaje utilizando el comando de la CLI `delete-mount-target`.

```
$ aws efs delete-mount-target \  
--mount-target-id ID-of-mount-target-to-delete \  
--profile adminuser \  
--region aws-region
```

3. (Opcional) Elimine los dos grupos de seguridad que ha creado. No hay que pagar para crear grupos de seguridad.

Debe eliminar el grupo de seguridad del destino de montaje en primer lugar, antes de eliminar el grupo de seguridad de la instancia EC2. El grupo de seguridad del destino de montaje tiene una regla que hace referencia al grupos de seguridad de EC2. Por lo tanto, no puede eliminar en primer lugar el grupo de seguridad de la instancia EC2.

Para obtener instrucciones, consulte [Eliminar un grupo de seguridad](#) en la Guía del usuario de Amazon EC2.

4. Elimine el sistema de archivos utilizando el comando de la CLI `delete-file-system`. Puede obtener una lista de los sistemas de archivos utilizando el comando de la CLI `describe-file-systems`. Puede obtener el ID del sistema de archivos de la respuesta.

```
aws efs describe-file-systems \  
--profile adminuser \  
--region aws-region
```

Elimine el sistema de archivos proporcionando el ID de sistema de archivos.

```
$ aws efs delete-file-system \  
--file-system-id ID-of-file-system-to-delete \  
--region aws-region \  
--profile adminuser
```

Tutorial: Configurar un servidor web Apache y ofrecer archivos de Amazon EFS

Puede disponer de instancias de EC2 que ejecutan el servidor web Apache que ofrece archivos almacenados en su sistema de archivos de Amazon EFS. Puede ser una instancia de EC2, o si la aplicación lo necesita, puede disponer de varias instancias de EC2 que ofrecen archivos desde su sistema de archivos de Amazon EFS. Se describen los siguientes procedimientos.

- [Configurar un servidor web Apache en una instancia EC2.](#)
- [Configurar un servidor web Apache en varias instancias EC2 mediante la creación de un grupo de Auto Scaling.](#) Puede crear varias instancias de EC2 con Amazon EC2 Auto Scaling, AWS un servicio que le permite aumentar o disminuir el número de instancias de EC2 en un grupo según las necesidades de su aplicación. Si dispone de varios servidores web, también necesita un balanceador de carga para distribuir el tráfico de solicitudes entre ellos.

Note

Para ambos procedimientos, debe crear todos los recursos en la región Oeste de EE. UU. (Oregón) (us-west-2).

Una sola instancia de EC2 para ofrecer archivos

Siga los pasos para configurar un servidor web Apache en una instancia de EC2 para ofrecer los archivos que cree en su sistema de archivos de Amazon EFS.

1. Siga los pasos que se indican en el ejercicio de introducción, a fin de disponer de una configuración activa que conste de lo siguiente:
 - Sistema de archivos de Amazon EFS

- instancia de EC2
- Sistema de archivos montado en la instancia EC2

Para ver instrucciones, consulte [Introducción a Amazon Elastic File System](#). Cuando siga los pasos, anote lo siguiente:

- Nombre DNS público de la instancia EC2.
 - Nombre DNS público del destino de montaje creado en la misma zona de disponibilidad en la que ha lanzado la instancia EC2.
2. (Opcional) Puede elegir desmontar el sistema de archivos desde el punto de montaje que creó en el ejercicio de introducción.

```
$ sudo umount ~/efs-mount-point
```

En este tutorial crea otro punto de montaje para el sistema de archivos.

3. En la instancia EC2, instale el servidor web Apache y configúrelo como se indica a continuación:
- a. Conéctese a su instancia EC2 e instale el servidor web Apache.

```
$ sudo yum -y install httpd
```

- b. Inicie el servicio .

```
$ sudo service httpd start
```

- c. Cree un punto de montaje.

En primer lugar, tenga en cuenta que DocumentRoot en el archivo `/etc/httpd/conf/httpd.conf` apunta a `/var/www/html` (DocumentRoot `"/var/www/html"`).

Montará su sistema de archivos de Amazon EFS en un subdirectorio bajo el documento raíz.

Cree un subdirectorio denominado `efs-mount-point` para usarlo como punto de montaje para su sistema de archivos, en `/var/www/html`.

```
$ sudo mkdir /var/www/html/efs-mount-point
```


- d. Monte su sistema de archivos de Amazon EFS usando el siguiente comando: reemplace `file-system-id` con el ID de su sistema de archivos.

```
$ sudo mount -t efs file-system-id:/ /var/www/html/efs-mount-point
```

4. Pruebe la configuración.

- a. Añada una regla en el grupo de seguridad de la instancia EC2, que ha creado en el ejercicio de introducción, para permitir el tráfico HTTP en el puerto TCP 80 desde cualquier lugar.

Después de agregar la regla, el grupo de seguridad de la instancia EC2 tendrá las siguientes reglas de entrada.

Security Group: sg-13881977

Description Inbound Outbound Tags

Edit

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
SSH	TCP	22	0.0.0.0
HTTP	TCP	80	0.0.0.0

Para ver instrucciones, consulte [Cree un grupo de seguridad mediante la consola](#).

- b. Cree un archivo html de muestra.
 - i. Cambie el directorio al punto de montaje.

```
$ cd /var/www/html/efs-mount-point
```

- ii. Haga un subdirectorio llamado `sampledir` y cambie la propiedad.

```
$ sudo mkdir sampledir
$ sudo chown ec2-user sampledir
$ sudo chmod -R o+r sampledir
```

Cambie el directorio para poder crear archivos en el subdirectorio `sampledir`.

```
$ cd sampledir
```

- iii. Cree un archivo `hello.html` de muestra.

```
$ echo "<html><h1>Hello from Amazon EFS</h1></html>" > hello.html
```

- c. Abra una ventana del navegador e introduzca la dirección URL para acceder al archivo (es el nombre de DNS pública de la instancia EC2 seguido del nombre de archivo). Por ejemplo:

```
http://EC2-instance-public-DNS/efs-mount-point/sampledir/hello.html
```

Ahora está ofreciendo páginas web almacenadas en un sistema de archivos de Amazon EFS.

Note

Esta configuración no configura la instancia de EC2 para que inicie automáticamente el servidor web (httpd) durante el arranque y además no monta el sistema de archivos durante el arranque. En el siguiente tutorial se crea una configuración de lanzamiento para hacerlo.

Varias instancias de EC2 para ofrecer archivos

Siga los pasos para ofrecer el mismo contenido en su sistema de archivos de Amazon EFS desde varias instancias de EC2 para mejorar la escalabilidad o la disponibilidad.

1. Siga los pasos que se indican en el ejercicio [Cree rápidamente un sistema de archivos con la configuración recomendada \(consola\)](#), para tener un sistema de archivos de Amazon EFS creado y probado.

Important

En este tutorial no se usa la instancia EC2 que ha creado en el ejercicio de introducción. En su lugar, puede lanzar nuevas instancias EC2.

2. Cree un balanceador de carga en su VPC siguiendo estos pasos.
 - a. Definir un balanceador de carga


En la sección Basic Configuration (Configuración básica), seleccione la VPC donde también se crean las instancias EC2 en las que se monta el sistema de archivos.

En la sección **Seleccionar subredes**, seleccione todas las subredes disponibles . Para obtener más información, consulte el script `c1oud-config` en la siguiente sección.

b. **Asignar grupos de seguridad**

Cree un nuevo grupo de seguridad para el balanceador de carga para permitir el acceso HTTP desde el puerto 80 desde cualquier lugar, tal y como se muestra a continuación:


- Tipo: HTTP
- Protocolo: TCP
- Rango de puertos: 80
- Origen: cualquiera (0.0.0.0/0)

 **Note**

Cuando todo funciona, también puede actualizar la regla de entrada del grupo de seguridad de la instancia EC2 para permitir el tráfico HTTP únicamente desde el balanceador de carga.

c. **Configure una comprobación de estado**

Establezca el valor de Ping Path (Ruta de ping) en `/efs-mount-point/test.html`. El `efs-mount-point` es el subdirectorio en el que tiene el sistema de archivos montado. Añade la página `test.html` más adelante en este procedimiento.

 **Note**

No incluya ninguna instancia EC2. Posteriormente, cree un grupo de Auto Scaling en el que lanzar la instancia EC2 y especifique este balanceador de carga.

Para obtener más información sobre la creación de un equilibrador de carga, consulte [Introducción a Elastic Load Balancing](#) en la Guía del usuario de Elastic Load Balancing.

Cree un grupo de Auto Scaling con dos instancias EC2. En primer lugar, debe crear una configuración de lanzamiento que describa las instancias. A continuación, debe crear un grupo

de Auto Scaling especificando la configuración de lanzamiento. Los pasos siguientes ofrecen información de configuración que especifica para crear un grupo de Auto Scaling desde la consola de Amazon EC2.

1. Seleccione Launch Configurations (Configuraciones de lanzamiento) en AUTO SCALING en el panel de navegación de la izquierda.
2. Seleccione Create Auto Scaling group (Crear grupo de Auto Scaling) para lanzar el asistente.
3. Elija Create launch configuration.
4. En Inicio rápido, seleccione la versión más reciente de la AMI de Amazon Linux 2. Se trata de la misma AMI que utiliza en [Cree su sistema de archivos EFS y lance su instancia EC2](#) del ejercicio de introducción.
5. En la sección Advanced (Avanzado), haga lo siguiente:
 - Para IP Address Type (Tipo de dirección IP), elija Assign a public IP address to every instance (Asignar una dirección IP pública a cada instancia).
 - Copie y pegue el siguiente script en el cuadro User data (Datos del usuario).

Debe actualizar el script proporcionando valores para *file-system-id* y *aws-region* (si se ha seguido el ejercicio de introducción, habrá creado el sistema de archivos en la región us-west-2).

En el script, tenga en cuenta lo siguiente:

- El script instala el cliente NFS y el servidor web Apache.
- El comando echo escribe la siguiente entrada en el archivo `/etc/fstab` identificando el nombre de DNS del sistema de archivos y el subdirectorío donde montarlo. Esta entrada garantiza que el archivo se monte después de cada reinicio del sistema. Tenga en cuenta que el nombre de DNS del sistema de archivos se construye de forma dinámica. Para obtener más información, consulte [Montaje en Amazon EC2 con un nombre de DNS](#).

```
file-system-ID.efs.aws-region.amazonaws.com:/ /var/www/html/efs-mount-point  
nfs4 defaults
```


- Crea el subdirectorío `efs-mount-point` y monta el sistema de archivos en el mismo.
- Crea una página `test.html` para que la comprobación de estado de ELB pueda encontrar el archivo (al crear un equilibrador de carga ha especificado este archivo como el punto de ping).

Para obtener más información sobre los scripts de datos de usuario, consulte [Metadatos de instancia y datos de usuario](#).

```
#cloud-config
package_upgrade: true
packages:
- nfs-utils
- httpd
runcmd:
- echo "$(curl -s http://169.254.169.254/latest/meta-data/placement/availability-zone).file-system-id.efs.aws-region.amazonaws.com:/ /var/www/html/efs-mount-point nfs4 defaults" >> /etc/fstab
- mkdir /var/www/html/efs-mount-point
- mount -a
- touch /var/www/html/efs-mount-point/test.html
- service httpd start
- chkconfig httpd on
```

6. Para Assign a security group (Asignar un grupo de seguridad), elija Select an existing security group (Seleccionar un grupo de seguridad existente) y, a continuación, el grupo de seguridad que ha creado para la instancia EC2.
7. Ahora, configure los detalles del grupo de escalado automático con la siguiente información:
 - a. Para Group size (Tamaño del grupo), elija **Start with 2 instances**. Creará dos instancias EC2.
 - b. Seleccione la VPC en la lista Network (Red).
 - c. Seleccione una subred en la misma zona de disponibilidad que utilizó al especificar el ID del destino de montaje en el script de datos de usuario al crear la configuración de lanzamiento en el paso anterior.
 - d. En la sección Detalles avanzados
 - i. Para Load Balancing (Balanceador de carga), elija Receive traffic from Elastic Load Balancer(s) (Recibir tráfico de balanceadores de carga elásticos) y, a continuación, seleccione el balanceador de carga que ha creado para este ejercicio.
 - ii. En Health Check Type (Tipo de comprobación de estado), seleccione ELB.
8. Siga las instrucciones para crear un grupo de escalado automático en [Configuración de una aplicación con escalado y balanceo de carga aplicados](#) en la Guía del usuario de Amazon EC2 Auto Scaling. Utilice la información de las tablas anteriores cuando proceda.

9. Tras la correcta creación del grupo de Auto Scaling, dispone de dos instancias EC2 con `nfs-utils` y el servidor web Apache instalado. En cada instancia, verifique que tiene el subdirectorio `/var/www/html/efs-mount-point` y su sistema de archivos de Amazon EFS montado en él. Para obtener instrucciones sobre cómo conectarse a una instancia EC2, consulte [Conectarse a su instancia de Linux](#) en la Guía del usuario de Amazon EC2.

 Note

Si elige la AMI de Amazon Linux Amazon Linux AMI 2016.03.0 al lanzar su instancia de Amazon EC2, no tendrá que instalar `nfs-utils`, porque ya está incluido en la AMI de forma predeterminada.

10. Cree una página de muestra (`index.html`).

- a. Cambie el directorio.

```
$ cd /var/www/html/efs-mount-point
```

- b. Haga un subdirectorio para `sampledir` y cambie la propiedad. Y cambie el directorio para poder crear archivos en el subdirectorio `sampledir`. Si ha seguido el [Una sola instancia de EC2 para ofrecer archivos](#) anterior, ya ha creado el subdirectorio `sampledir`, de modo que puede omitir este paso.

```
$ sudo mkdir sampledir
$ sudo chown ec2-user sampledir
$ sudo chmod -R o+r sampledir
$ cd sampledir
```

- c. Cree un archivo `index.html` de muestra.

```
$ echo "<html><h1>Hello from Amazon EFS</h1></html>" > index.html
```

11. Ahora puede probar la configuración. Con el nombre de DNS público del balanceador de carga, acceda a la página `index.html`.

```
http://load balancer public DNS Name/efs-mount-point/sampledir/index.html
```

El balanceador de carga envía una solicitud a una de las instancias EC2 que ejecuta el servidor web Apache. A continuación, el servidor web ofrece el archivo que está almacenado en su sistema de archivos de Amazon EFS.

Tutorial: Crear subdirectorios que se pueden escribir por usuario y configurar la opción de volver a montar automáticamente al reiniciar

Tras crear un sistema de archivos de Amazon EFS y montarlo localmente en la instancia de EC2, se expone un directorio vacío denominado *raíz del sistema de archivos*. Un caso de uso común consiste en crear un subdirectorio "que se puede escribir" debajo de esta raíz del sistema de archivos para cada usuario que cree en la instancia EC2 y montarlo en el directorio principal del usuario. Todos los archivos y subdirectorios que el usuario crea en su directorio principal se crean entonces en el sistema de archivos Amazon EFS.

En este tutorial, primero crea un usuario "mike" en su instancia EC2. A continuación, monta un subdirectorio de Amazon EFS en el directorio principal del usuario mike. El tutorial también explica cómo configurar volver a montar de forma automática los subdirectorios si se reinicia el sistema.

Supongamos que tiene un sistema de archivos Amazon EFS creado y montado en un directorio local de su instancia de EC2. Vamos a llamarlo *EFScroot*.

Note

Puede seguir el [Introducción](#) ejercicio para crear y montar un sistema de archivos de Amazon EFS en la instancia EC2.

En los siguientes pasos, se crea un usuario (mike), se crea un subdirectorio para el usuario (*EFScroot/mike*), se convierte al usuario mike en el propietario del subdirectorio, se le conceden todos los permisos y, por último, se monta el subdirectorio Amazon EFS en el directorio principal del usuario (/home/mike).

1. Cree el usuario mike:

- Inicie sesión en la instancia EC2. Utilizando privilegios raíz (en este caso, utilizando el comando sudo), cree el usuario mike y asigne una contraseña.

```
$ sudo useradd -c "Mike Smith" mike
$ sudo passwd mike
```

Esto también crea un directorio principal, `/home/mike`, para el usuario.

2. Cree un subdirectorio bajo *EFSroot* para el usuario `mike`:

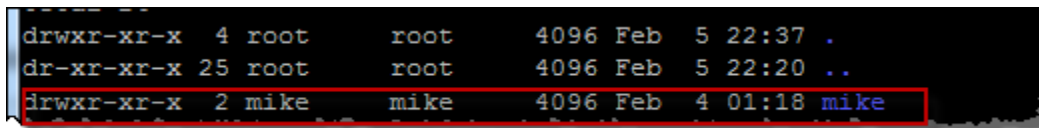
a. Cree el subdirectorio `mike` bajo *EFSroot*.

```
$ sudo mkdir /EFSroot/mike
```

Tendrá que sustituir *EFSroot* por el nombre de su directorio local.

b. El usuario raíz y el grupo raíz son los propietarios del subdirectorio `/mike` (puede verificarlo utilizando el comando `ls -l`). Para habilitar los permisos completos para el usuario `mike` en este subdirectorio, conceda a `mike` la propiedad del directorio.

```
$ sudo chown mike:mike /EFSroot/mike
```



```
drwxr-xr-x  4 root   root   4096 Feb  5 22:37 .
dr-xr-xr-x 25 root   root   4096 Feb  5 22:20 ..
drwxr-xr-x  2 mike   mike   4096 Feb  4 01:18 mike
```

3. Utilice el comando `mount` para montar el subdirectorio *EFSroot/mike* en el directorio principal de `mike`.

```
$ sudo mount -t nfs -o
nfsvers=4.1,rsize=1048576,wsrize=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-DNS:/mike /home/mike
```

La dirección *Mount-Target-DNS* identifica la raíz remota del sistema de archivos Amazon EFS.

Ahora, el directorio principal del usuario `mike` es un subdirectorio en el que Mike puede escribir en el sistema de archivos Amazon EFS. Si desmonta este destino de montaje, el usuario no puede obtener acceso a su directorio de EFS sin volver a montar, lo que requiere permisos raíz.

Remontaje automático al reiniciar

Puede utilizar el archivo `fstab` para volver a montar automáticamente su sistema de archivos después de cualquier reinicio del sistema. Para obtener más información, consulte [Cómo montar su sistema de archivos de Amazon EFS automáticamente](#).

Tutorial: Crear y montar un sistema de archivos en las instalaciones con AWS Direct Connect y una VPN

En este tutorial, se utiliza AWS Management Console para crear y montar un sistema de archivos en un cliente local. Para ello, utilice una AWS Direct Connect conexión o una conexión en un AWS Virtual Private Network (VPC) VPN.

Note

No se admite el uso de Amazon EFS con clientes basados en Microsoft Windows.

Temas

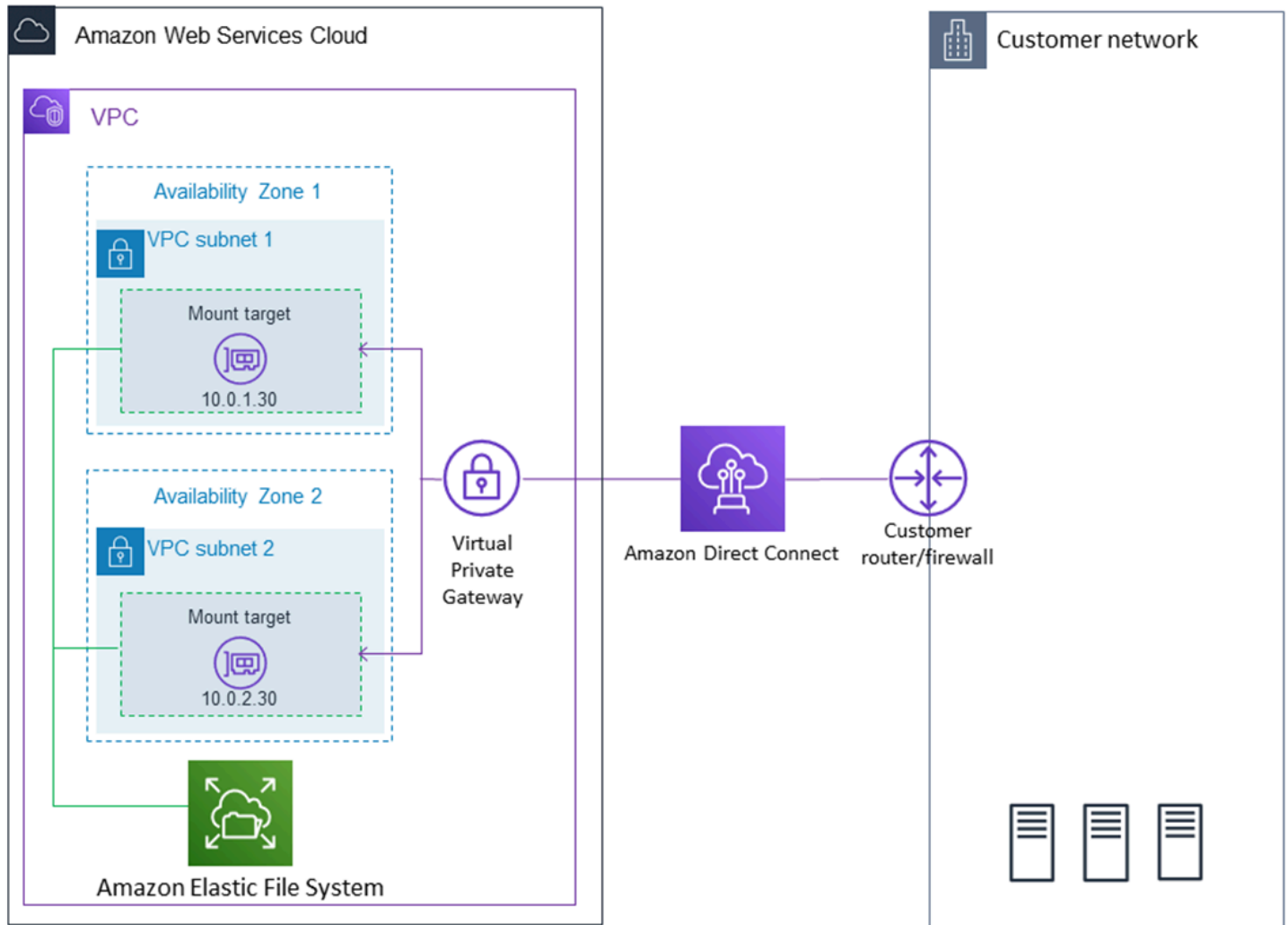
- [Antes de empezar](#)
- [Paso 1: Crear los recursos de Amazon Elastic File System](#)
- [Paso 2: Instalar el cliente NFS](#)
- [Paso 3: Montar el sistema de archivos de Amazon EFS en su cliente en las instalaciones](#)
- [Paso 4: Limpiar recursos y proteger la cuenta de AWS](#)
- [Opcional: Cifrado de datos en tránsito](#)

En este tutorial, asumimos que ya tienes una conexión AWS Direct Connect o una VPN. Si no dispone de una, puede iniciar el proceso de conexión ahora y volver a este tutorial cuando se haya establecido la conexión. Para obtener más información AWS Direct Connect, consulte la [Guía del AWS Direct Connect usuario](#). Para obtener más información acerca de cómo configurar una conexión VPN, consulte [Conexiones de la VPN](#) en la Guía del usuario de Amazon VPC.

Cuando dispone de una AWS Direct Connect conexión VPN, crea un sistema de archivos Amazon EFS y un destino de montaje en su Amazon VPC. Después, descarga e instala las `amazon-efs-utils`

herramientas. A continuación, probará el sistema de archivos desde su cliente local. Por último, el paso de limpieza al final del tutorial le ofrece información para que elimine estos recursos.

El tutorial crea todos estos recursos en la región Oeste de EE. UU. (Oregón) (`us-west-2`). Independientemente de la Región de AWS que use, asegúrese de usarlo de manera consistente. Todos sus recursos (su VPC, su destino de montaje y su sistema de archivos Amazon EFS) deben estar en el Región de AWS mismo lugar, como se muestra en el siguiente diagrama.



Note

En algunos casos, la aplicación local es posible que tenga que saber si el sistema de archivos se encuentra disponible. En estos casos, la aplicación debe ser capaz de apuntar a una dirección IP de punto de montaje diferente si el primer punto de montaje deja de estar disponible temporalmente. En este caso, le recomendamos que tenga dos clientes locales

conectados a su sistema de archivos a través de distintas zonas de disponibilidad (AZ) para mayor disponibilidad.

Antes de empezar

Puede usar sus credenciales raíz Cuenta de AWS para iniciar sesión en la consola e intentar este ejercicio. Sin embargo, las prácticas recomendadas de AWS Identity and Access Management (IAM) recomiendan que no utilices las credenciales raíz de tu Cuenta de AWS. En su lugar, cree un usuario administrador en su cuenta y utilice esas credenciales para administrar los recursos de su cuenta. Para obtener más información, consulte [Asignar Cuenta de AWS acceso a un usuario del Centro de identidades de IAM](#) en la Guía del AWS IAM Identity Center usuario.

Puede utilizar una VPC predeterminada o una VPC personalizada que haya creado en su cuenta. Para este tutorial, la configuración de la VPC predeterminada funciona. Sin embargo, si utiliza una VPC personalizada, verifique lo siguiente:

- La gateway de Internet está conectada a su VPC. Para obtener más información, consulte [Gateways de Internet](#) en la Guía del usuario de Amazon VPC.
- La tabla de ruteo de la VPC incluye una regla para enviar todo el tráfico vinculado a Internet a la gateway de Internet.

Paso 1: Crear los recursos de Amazon Elastic File System

En este paso, crea el sistema de archivos de Amazon EFS y los destinos de montaje.

Cree su sistema de archivos de Amazon EFS

1. Abra la consola de Amazon EFS en <https://console.aws.amazon.com/efs>.
2. Seleccione Crear sistema de archivos.
3. Seleccione su VPC predeterminada en la lista VPC.
4. Seleccione las casillas de verificación para todas las zonas de disponibilidad. Asegúrese de que todos tengan las subredes predeterminadas, direcciones IP automáticas y los grupos de seguridad predeterminados elegidos. Estos son sus destinos de montaje. Para obtener más información, consulte [Administrar destinos de montaje](#).
5. Elija Paso siguiente.

6. Asigne un nombre al sistema de archivos, mantenga el modo general purpose (fines generales) seleccionado como modo de desempeño predeterminado y elija Next Step (Paso siguiente).
7. Seleccione Crear sistema de archivos.
8. Elija su sistema de archivos de la lista y anote el valor de Security group (Grupo de seguridad). Necesitará este valor para el siguiente paso.

El sistema de archivos que acaba de crear tiene destinos de montaje. Cada destino de montaje tiene un grupo de seguridad asociado. El grupo de seguridad funciona como un firewall virtual que controla el tráfico de red. Si no proporciona un grupo de seguridad al crear un destino de montaje, Amazon EFS le asocia el grupo de seguridad predeterminado de la VPC. Si ha seguido los pasos anteriores exactamente, entonces los destinos de montaje están utilizando el grupo de seguridad predeterminado.

A continuación, añadirá una regla al grupo de seguridad del destino de montaje para permitir el tráfico entrante al puerto de Network File System (NFS) (2049). Puede utilizarla AWS Management Console para añadir la regla a los grupos de seguridad de su destino de montaje en su VPC.

Para permitir el tráfico entrante al puerto NFS

1. [Inicie sesión en la consola Amazon EC2 AWS Management Console y ábrala en https://console.aws.amazon.com/ec2/.](https://console.aws.amazon.com/ec2/)
2. En NETWORK & SECURITY (RED Y SEGURIDAD), elija Security Groups (Grupos de seguridad).
3. Elija el grupo de seguridad asociado a su sistema de archivos. Ha tomado nota de ello al final de [Paso 1: Crear los recursos de Amazon Elastic File System.](#)
4. En el panel de pestañas que aparece debajo de la lista de grupos de seguridad, elija la pestaña Inbound (Entrante).
5. Elija Editar.
6. Elija Add Rule (Añadir regla) y elija una regla del siguiente tipo:
 - Type (Tipo): NFS
 - Source (Origen): Anywhere (Cualquiera)

Le recomendamos que solo use el origen Anywhere (Cualquiera) para pruebas. Tiene la opción de crear un origen personalizado definido en la dirección IP del cliente local o utilizar la consola del propio cliente y elegir My IP (Mi IP).

Note

No es necesario añadir una regla de salida, ya que la regla de salida predeterminada permite que salga todo el tráfico. Si no dispone de esta regla de salida predeterminada, añada una regla de salida para abrir una conexión TCP en el puerto NFS, identificando el grupo de seguridad de destino de montaje como destino.

Paso 2: Instalar el cliente NFS

En este paso, instalará y configurará el cliente NFS.

Para instalar el cliente NFS en el servidor local

Note

Si necesita cifrar datos en tránsito, utilice el ayudante de montaje de Amazon EFS, `amazon-efs-utils`, en lugar del cliente NFS. Para obtener información sobre la instalación `amazon-efs-utils`, consulte la sección Opcional: cifrado de datos en tránsito.

1. Obtenga acceso al terminal para su cliente local.
2. Instale NFS.

Si utiliza Red Hat Linux, instale NFS con el siguiente comando.

```
$ sudo yum -y install nfs-utils
```

Si utiliza Ubuntu, instale NFS con el siguiente comando.

```
$ sudo apt-get -y install nfs-common
```

Paso 3: Montar el sistema de archivos de Amazon EFS en su cliente en las instalaciones

Para crear un directorio de montaje

1. Haga un directorio para el punto de montaje con el siguiente comando.

Example

```
mkdir ~/efs
```

2. Elija su dirección IP preferida del destino de montaje en la zona de disponibilidad. Puede medir la latencia de sus clientes de Linux locales. Para ello, utilice una herramienta basada en el terminal como `ping` frente a la dirección IP de sus instancias EC2 en diferentes zonas de disponibilidad para encontrar la que tenga la latencia más baja.
- Ejecute el comando de montaje para montar el sistema de archivos utilizando la dirección IP del destino de montaje.

```
$ sudo mount -t nfs -o  
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport mount-  
target-IP:/ ~/efs
```

Ahora que ha montado su sistema de archivos de Amazon EFS, puede probarlo con el procedimiento que se indica a continuación.

Para probar la conexión del sistema de archivos de Amazon EFS

1. Cambie los directorios al nuevo directorio que ha creado con el comando siguiente.

```
$ cd ~/efs
```

2. Cree un subdirectorio y cambie la propiedad de dicho subdirectorio a su usuario de instancia EC2. A continuación, diríjase a ese nuevo directorio con los siguientes comandos.

```
$ sudo mkdir getting-started  
$ sudo chown ec2-user getting-started  
$ cd getting-started
```

3. Cree un archivo de texto con el siguiente comando.

```
$ touch test-file.txt
```

4. Muestre el contenido del directorio con el siguiente comando.

```
$ ls -al
```

Como resultado, se crea el siguiente archivo.

```
-rw-rw-r-- 1 username username 0 Nov 15 15:32 test-file.txt
```

También puede montar el sistema de archivos automáticamente mediante la incorporación de una entrada en el archivo `/etc/fstab`. Para obtener más información, consulte [Cómo montar su sistema de archivos de Amazon EFS automáticamente](#).

Warning

Use la opción `_netdev`, empleada para identificar los sistemas de archivos de red, cuando monte su sistema de archivos automáticamente. Si falta `_netdev`, la instancia EC2 puede dejar de responder. Este resultado se debe a que los sistemas de archivos de red se deben inicializar después de que la instancia de procesamiento inicia sus redes. Para obtener más información, consulte [Se produce un error de montaje automático y la instancia no responde](#).

Paso 4: Limpiar recursos y proteger la cuenta de AWS

Una vez que haya terminado este tutorial o si no desea explorarlo, debe seguir estos pasos para limpiar sus recursos y proteger su cuenta de AWS .


Para limpiar los recursos y proteger su Cuenta de AWS

1. Desmonte el sistema de archivos de Amazon EFS con el siguiente comando.

```
$ sudo umount ~/efs
```

2. Abra la consola de Amazon EFS en <https://console.aws.amazon.com/efs>.

3. Elija el sistema de archivos de Amazon EFS que desea eliminar de la lista de sistemas de archivos.
4. En Acciones, seleccione Eliminar sistema de archivos.
5. En el cuadro de diálogo Eliminar sistema de archivos permanentemente, escriba el ID del sistema de archivos de Amazon EFS que quiera eliminar y luego seleccione Eliminar sistema de archivos.
6. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
7. En el panel de navegación, elija Grupos de seguridad.
8. Seleccione el nombre del grupo de seguridad al que añadió la regla a para este tutorial.

 Warning

No elimine el grupo de seguridad predeterminado para la VPC.

9. En Acciones, elija Editar reglas de entrada.
10. Elija la X al final de la regla de entrada que ha añadido y seleccione Save (Guardar).

Opcional: Cifrado de datos en tránsito

Para cifrar los datos en tránsito, utilice el asistente de montaje de Amazon EFS `amazon-efs-utils`, en lugar del cliente NFS.

El `amazon-efs-utils` paquete es una colección de código abierto de herramientas de Amazon EFS. La `amazon-efs-utils` colección incluye un asistente de montaje y herramientas que facilitan el cifrado de los datos en tránsito para Amazon EFS. Para obtener más información sobre este paquete, consulte [Instalación de las herramientas de Amazon EFS](#). Este paquete está disponible como descarga gratuita y puede obtenerlo clonando el repositorio del paquete. GitHub

Para clonar desde `amazon-efs-utils` GitHub

1. Obtenga acceso al terminal para su cliente local.
2. Desde el terminal, clona la `amazon-efs-utils` herramienta en el directorio que prefieras con el siguiente comando. GitHub

```
git clone https://github.com/aws/efs-utils
```



Ahora que tiene el paquete, puede instalarlo. Esta instalación se gestiona de forma distinta en función de la distribución de Linux de su cliente local. Se admiten las siguientes distribuciones:

- Amazon Linux 2
- Amazon Linux
- Red Hat Enterprise Linux (y sus derivados como CentOS) versión 7 y posteriores
- Ubuntu 16.04 LTS y posterior

Para compilar e instalar `amazon-efs-utils` como un paquete RPM

1. Abra una terminal en su cliente y navegue hasta el directorio desde GitHub el que se ha clonado el `amazon-efs-utils` paquete.
2. Compile el paquete con el siguiente comando.

```
make rpm
```

 Note

Si aún no lo ha hecho, instale el paquete `rpm-builder` con el comando siguiente.

```
sudo yum -y install rpm-build
```

3. Instale el paquete con el siguiente comando.

```
sudo yum -y install build/amazon-efs-utils*.rpm
```

Para compilar e instalar `amazon-efs-utils` como un paquete deb

1. Abra una terminal en su cliente y navegue hasta el directorio desde el que se ha clonado el `amazon-efs-utils` paquete. GitHub
2. Compile el paquete con el siguiente comando.

```
./build-deb.sh
```

3. Instale el paquete con el siguiente comando.

```
sudo apt-get install build/amazon-efs-utils*deb
```

Una vez instalado el paquete, configúrelo `amazon-efs-utils` para usarlo en su Región de AWS red AWS Direct Connect o VPN.

Para configurarlo `amazon-efs-utils` para su uso en su Región de AWS

1. Con el editor de textos que prefiera, abra `/etc/amazon/efs/efs-utils.conf` para editarlo.
2. Busque la línea `dns_name_format = {fs_id}.efs.{region}.amazonaws.com`.
3. Cambie `{region}` con el ID de la región de AWS , por ejemplo `us-west-2`.

Para montar el sistema de archivos de EFS en su cliente local, en primer lugar, abra un terminal en su cliente Linux local. Para montar el sistema, necesita el ID del sistema de archivos, la dirección IP del destino de montaje para uno de sus destinos de montaje y la Región de AWS del sistema de archivos. Si ha creado varios destinos de montaje para su sistema de archivos, entonces puede elegir cualquiera de estos.

Cuando tenga esa información, puede montar el sistema de archivos en tres pasos:

Para crear un directorio de montaje

1. Haga un directorio para el punto de montaje con el siguiente comando.

Example

```
mkdir ~/efs
```

2. Elija su dirección IP preferida del destino de montaje en la zona de disponibilidad. Puede medir la latencia de sus clientes de Linux locales. Para ello, utilice una herramienta basada en el terminal como `ping` frente a la dirección IP de sus instancias EC2 en diferentes zonas de disponibilidad para encontrar la que tenga la latencia más baja.

Para actualizar `/etc/hosts`

- Agregue una entrada a su archivo `/etc/hosts` local con el ID de sistema de archivos y la dirección IP del destino de montaje, en el siguiente formato.

```
mount-target-IP-Address file-system-ID.efs.region.amazonaws.com
```

Example

```
192.0.2.0 fs-12345678.efs.us-west-2.amazonaws.com
```

Para crear un directorio de montaje

1. Haga un directorio para el punto de montaje con el siguiente comando.

Example

```
mkdir ~/efs
```

2. Ejecute el comando de montaje para montar el sistema de archivos.

Example

```
sudo mount -t efs fs-12345678 ~/efs
```

Si desea utilizar el cifrado de datos en tránsito, el comando de montaje será parecido al siguiente.

Example

```
sudo mount -t efs -o tls fs-12345678 ~/efs
```

Tutorial: Montar un sistema de archivos desde una VPC distinta

En este tutorial, va a configurar una instancia de Amazon EC2 para montar un sistema de archivos de Amazon EFS que está en una nube privada virtual (VPC) distinta. Para ello, utilice el ayudante de montaje de EFS. El ayudante de montaje forma parte del conjunto de herramientas `amazon-efs-utils`. Para obtener más información acerca de `amazon-efs-utils`, consulte [Instalación de las herramientas de Amazon EFS](#).

La VPC del cliente y la VPC de su sistema de archivos de EFS deben conectarse mediante una interconexión de VPC o una gateway de tránsito de VPC. Cuando utiliza una interconexión de VPC o una gateway de tránsito para conectar las VPC, las instancias de Amazon EC2 en una VPC pueden acceder a los sistemas de archivos de EFS en otra VPC, incluso si las VPC pertenecen a diferentes cuentas.

Note

No se admite el uso de Amazon EFS con clientes basados en Microsoft Windows.

Temas

- [Antes de empezar](#)
- [Paso 1: Determinar el ID de la zona de disponibilidad del destino de montaje de EFS](#)
- [Paso 2: Determinar la dirección IP del destino de montaje](#)
- [Paso 3: Agregar una entrada de host para el destino de montaje](#)
- [Paso 4: Montar el sistema de archivos con el ayudante de montaje de EFS](#)
- [Paso 5: Limpiar recursos y proteger la cuenta de AWS](#)

Antes de empezar

En este tutorial, se supone que ya dispone de lo siguiente:

- El conjunto de herramientas `amazon-efs-utils` se instala en la instancia EC2 antes de utilizar este procedimiento. Para obtener instrucciones sobre cómo instalar `amazon-efs-utils`, consulte [Instalación de las herramientas de Amazon EFS](#).
- Uno de los siguientes:
 - Una interconexión con VPC entre la VPC donde reside el sistema de archivos de EFS y la VPC donde reside la instancia EC2. Una conexión de emparejamiento de VPC es una conexión de red entre dos instancias de VPC. Este tipo de conexión permite enrutar el tráfico entre ellas mediante direcciones de protocolo de Internet versión 4 (IPv4) o de protocolo de Internet versión 6 (IPv6) privadas. Puede utilizar el emparejamiento de VPC para conectar VPC dentro del mismo Región de AWS o entre uno y otro. Región de AWS Para obtener más información, consulte [Creación y aceptación de interconexiones de VPC](#) en la Guía de conexión de emparejamiento de Amazon VPC.

- Una gateway de tránsito que conecta la VPC donde reside el sistema de archivos EFS y la VPC donde reside la instancia EC2. Una puerta de enlace de tránsito es un hub de tránsito de red que puede utilizar para interconectar sus VPC y redes en las instalaciones. Para obtener más información, consulte [Introducción a las puertas de enlace de tránsito](#) en la Guía de puertas de enlace de tránsito de Amazon VPC.

Paso 1: Determinar el ID de la zona de disponibilidad del destino de montaje de EFS

Para garantizar una alta disponibilidad del sistema de archivos, recomendamos utilizar siempre una dirección IP del destino de montaje de EFS que esté en la misma zona de disponibilidad (AZ) que su cliente de NFS. Si va a montar un sistema de archivos de EFS que esté en otra cuenta, asegúrese de que el cliente de NFS y el destino de montaje de EFS estén en el mismo ID de la zona de disponibilidad. Este requisito se aplica porque los nombres de zona de disponibilidad pueden ser distintos entre las cuentas.

Para determinar la zona de disponibilidad de la instancia de EC2.

1. Conéctese a su instancia EC2:
 - Para conectarse a la instancia desde un equipo que ejecute macOS o Linux, especifique el archivo `.pem` para su comando SSH. Para ello, use la opción `-i` y la ruta a su clave privada.
 - Para conectarte a la instancia desde un ordenador con Windows, puedes usar PuTTY, MindTerm o bien. Para usar PuTTY, instálelo y convierta el archivo `.pem` en un archivo `.ppk`.

Para obtener más información, consulte los siguientes temas de la Guía del usuario de Amazon EC2:

- [Conéctate a tu instancia de Linux desde Linux o macOS mediante SSH](#)
- [Conéctate a tu instancia de Linux desde Windows con PuTTY](#)

2. Determine el ID de de la zona de disponibilidad en el que se encuentra la instancia de EC2 mediante el comando de la CLI `describe-availability-zones`, como se indica a continuación.

```
[ec2-user@ip-10.0.0.1] $ aws ec2 describe-availability-zones --zone-name
{
  "AvailabilityZones": [
```

```

    {
      "State": "available",
      "ZoneName": "us-east-2b",
      "Messages": [],
      "ZoneId": "use2-az2",
      "RegionName": "us-east-2"
    }
  ]
}

```

El ID de la zona de disponibilidad se devuelve en la propiedad `ZoneId`, `use2-az2`.

Paso 2: Determinar la dirección IP del destino de montaje

Ahora que conoce el ID de la zona de disponibilidad de la instancia de EC2, puede recuperar la dirección IP del destino de montaje que está en el mismo ID de zona de disponibilidad.

Para determinar la dirección IP del destino de montaje en el mismo ID de la zona de disponibilidad

- Recupere la dirección IP del destino de montaje para su sistema de archivos en el ID de AZ `use2-az2` mediante el comando de la CLI `describe-mount-targets`, como se indica a continuación.

```

$ aws efs describe-mount-targets --file-system-id file_system_id
{
  "MountTargets": [
    {
      "OwnerId": "111122223333",
      "MountTargetId": "fsmt-11223344",
      =====> "AvailabilityZoneId": "use2-az2",
      "NetworkInterfaceId": "eni-048c09a306023eeec",
      "AvailabilityZoneName": "us-east-2b",
      "FileSystemId": "fs-01234567",
      "LifecycleState": "available",
      "SubnetId": "subnet-06eb0da37ee82a64f",
      "OwnerId": "958322738406",
      =====> "IpAddress": "10.0.2.153"
    },
    ...
    {
      "OwnerId": "111122223333",

```

```

    "MountTargetId": "fsmt-667788aa",
    "AvailabilityZoneId": "use2-az3",
    "NetworkInterfaceId": "eni-0edb579d21ed39261",
    "AvailabilityZoneName": "us-east-2c",
    "FileSystemId": "fs-01234567",
    "LifecycleState": "available",
    "SubnetId": "subnet-0ee85556822c441af",
    "OwnerId": "958322738406",
    "IpAddress": "10.0.3.107"
  }
]
}

```

El destino de montaje en el ID de la zona de disponibilidad use2-az2 tiene una dirección IP de 10.0.2.153.

Paso 3: Agregar una entrada de host para el destino de montaje

Ahora puede agregar una entrada en el archivo `/etc/hosts` de la instancia EC2 que asigne la dirección IP del destino de montaje al nombre de host de su sistema de archivos de EFS.

Para agregar una entrada de host para el destino de montaje

1. Agregue una línea para la dirección IP del destino de montaje al archivo `/etc/hosts` de la instancia EC2. La entrada utiliza el formato `mount-target-IP-Address file-system-ID.efs.region.amazonaws.com`. Utilice el comando siguiente para agregar la línea al archivo.

```
echo "10.0.2.153 fs-01234567.efs.us-east-2.amazonaws.com" | sudo tee -a /etc/hosts
```

2. Asegúrese de que los grupos de seguridad de VPC para la instancia de EC2 y el destino del montaje tengan reglas que permitan el acceso al sistema EFS, según sea necesario. Para obtener más información, consulte [Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje](#).

Paso 4: Montar el sistema de archivos con el ayudante de montaje de EFS

Para montar el sistema de archivos de EFS, primero debe crear un directorio de montaje en la instancia EC2. Después, utilizando el ayudante de montaje de EFS, puede montar el sistema de

archivos con una autorización de IAM o un punto de acceso EFS. Para obtener más información, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#) y [Trabajo con puntos de acceso de Amazon EFS](#).

Para crear un directorio de montaje

- Cree un directorio para montar el sistema de archivos mediante el comando siguiente.

```
$ sudo mkdir /mnt/efs/
```

Para montar el sistema de archivos con una autorización de IAM

- Utilice el comando siguiente para montar el sistema de archivos con una autorización de IAM.

```
$ sudo mount -t efs -o tls,iam file-system-id /mnt/efs/
```

Para montar el sistema de archivos con un punto de acceso EFS

- Utilice el comando siguiente para montar el sistema de archivos con un punto de acceso EFS.

```
$ sudo mount -t efs -o tls,accesspoint=access-point-id file-system-id /mnt/efs/
```

Ahora que ha montado su sistema de archivos de Amazon EFS, puede probarlo con el procedimiento que se indica a continuación.

Para probar la conexión del sistema de archivos de Amazon EFS

1. Cambie los directorios al nuevo directorio que ha creado con el comando siguiente.

```
$ cd ~/mnt/efs
```

2. Cree un subdirectorio y cambie la propiedad de dicho subdirectorio a su usuario de instancia EC2. A continuación, diríjase a ese nuevo directorio con los siguientes comandos.

```
$ sudo mkdir getting-started  
$ sudo chown ec2-user getting-started  
$ cd getting-started
```


3. Cree un archivo de texto con el siguiente comando.

```
$ touch test-file.txt
```

4. Muestre el contenido del directorio con el siguiente comando.

```
$ ls -al
```

Como resultado, se crea el siguiente archivo.

```
-rw-rw-r-- 1 username username 0 Nov 15 15:32 test-file.txt
```

También puede montar el sistema de archivos automáticamente mediante la incorporación de una entrada en el archivo `/etc/fstab`. Para obtener más información, consulte [Remontaje del sistema de archivos de EFS mediante /etc/fstab con el ayudante de montaje de EFS](#).

Warning

Use la opción `_netdev`, empleada para identificar los sistemas de archivos de red, cuando monte su sistema de archivos automáticamente. Si falta `_netdev`, la instancia EC2 puede dejar de responder. Este resultado se debe a que los sistemas de archivos de red se deben inicializar después de que la instancia de procesamiento inicia sus redes. Para obtener más información, consulte [Se produce un error de montaje automático y la instancia no responde](#).

Paso 5: Limpiar recursos y proteger la cuenta de AWS

Una vez que haya terminado este tutorial, o si no desea explorar los tutoriales, asegúrese de realizar los pasos siguientes. Limpie los recursos y proteja su Cuenta de AWS.


Para limpiar los recursos y proteger su Cuenta de AWS

1. Desmonte el sistema de archivos de Amazon EFS con el siguiente comando.

```
$ sudo umount ~/efs
```

2. Abra la consola de Amazon EFS en <https://console.aws.amazon.com/efs>.

3. Elija el sistema de archivos de Amazon EFS que desea eliminar de la lista de sistemas de archivos.
4. En Acciones, seleccione Eliminar sistema de archivos.
5. En el cuadro de diálogo Eliminar sistema de archivos permanentemente, escriba el ID del sistema de archivos de Amazon EFS que quiera eliminar y luego seleccione Eliminar sistema de archivos.
6. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
7. En el panel de navegación, elija Grupos de seguridad.
8. Seleccione el nombre del grupo de seguridad al que añadió la regla a para este tutorial.


 Warning

No elimine el grupo de seguridad predeterminado para la VPC.

9. En Acciones, elija Editar reglas de entrada.
10. Elija la X al final de la regla de entrada que ha añadido y seleccione Save (Guardar).

Tutorial: Aplicar cifrado en reposo a un sistema de archivos de Amazon EFS

A continuación, encontrará detalles acerca de cómo aplicar cifrado en reposo mediante Amazon CloudWatch y AWS CloudTrail. Este tutorial se basa en el [AWS documento técnico Cifrado de datos en reposo con sistemas de archivos cifrados de Amazon EFS](#).

 Note

El método para hacer cumplir la creación de sistemas de archivos de Amazon EFS cifrados en reposo descrito en este tutorial está obsoleto. El método preferido para aplicar en reposo a la creación de sistemas de archivos de `elasticfilesystem:EncryptedClave` de condición en AWS Identity and Access Management Políticas basadas en identidad. Para obtener más información, consulte [Ejemplo: Aplicación de la creación de sistemas de archivos cifrados](#). Puede utilizar este tutorial para crear alarmas de CloudWatch y validar que sus políticas de IAM impiden la creación de sistemas de archivos sin cifrar.

Aplicación del cifrado en reposo

Su organización podría necesitar el cifrado en reposo de todos los datos que cumplan una clasificación específica o que se asocien a una determinada aplicación, carga de trabajo o entorno. Puede aplicar políticas para el cifrado de datos en reposo para los sistemas de archivos de Amazon EFS mediante el uso de controles de detección. Estos controles detectan la creación de un sistema de archivos y verifican que el cifrado en reposo esté habilitado.

Si se detecta un sistema de archivos sin cifrado en reposo, puede responder de varias formas distintas. Estas van desde eliminar el sistema de archivos y destinos de montaje a notificar al administrador.

Si desea eliminar un sistema de archivos que carece de cifrado en reposo, pero desea conservar los datos, primero debe crear un nuevo sistema de archivos con cifrado en reposo. A continuación, copie los datos al nuevo sistema de archivos con cifrado en reposo. Una vez que se copian los datos, puede eliminar el sistema de archivos que carece de cifrado en reposo.

Detección de sistemas de archivos sin cifrar en reposo

Puede crear una alarma de CloudWatch para monitorear los registros de CloudTrail para `CreateFileSystemsEvent`. A continuación, puede activar la alarma para que notifique a un administrador si el sistema de archivos que se creó carecía de cifrado en reposo.

Crear un filtro de métricas

Para crear una alarma de CloudWatch que se active cuando se crea un sistema de archivos de Amazon EFS sin cifrado en reposo, utilice el siguiente procedimiento.

Antes de comenzar, debe disponer de un registro de seguimiento existente que envía registros de CloudTrail a un grupo de registros de CloudWatch Logs. Para obtener más información, consulte [Envío de eventos a CloudWatch Logs](#) en la AWS CloudTrail Guía del usuario de.

Para crear un filtro de métricas

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Logs.
3. En la lista de grupos de registro, seleccione el grupo de registro que creó para los eventos de registro de CloudTrail.

4. Elija Create Metric Filter.
5. En la página Define Logs Metric Filter (Definir filtro de métricas de registros), seleccione Filter Pattern (Patrón del filtro) y escriba lo siguiente:

```
{ ($.eventName = CreateFileSystem) && ($.responseElements.encrypted IS FALSE) }
```

6. Elija Assign Metric (Asignar métrica).
7. En Filter Name (Nombre del filtro), escriba **UnencryptedFileSystemCreated**.
8. En Metric Namespace (Espacio de nombres de métrica), escriba **CloudTrailMetrics**.
9. En Nombre de métrica, escriba **UnencryptedFileSystemCreatedEventCount**.
10. Elija Show advanced metric settings.
11. En Metric Value (Valor de la métrica), escriba **1**.
12. Elija Create Filter.

Crear una alarma

Después de crear el filtro de métricas, utilice el siguiente procedimiento para crear una alarma.

Para crear una alarma

1. En Filters (Filtros) en la página Log_Group_Name (Registro_Grupo_Nombre), al lado del nombre de archivo UnencryptedFileSystemCreated, seleccione Create Alarm (Crear alarma).
2. En la página Create Alarm (Crear alarma), defina los siguientes parámetros:
 - En Name (Nombre), escriba **Unencrypted File System Created**
 - En Whenever (Siempre que), haga lo siguiente:
 - Establezca is (es) en **> = 1**
 - Establezca for: (para:) en **1** periodo(s) consecutivo(s).
 - Para Treat missing data as (Tratar los datos que faltan como), seleccione good (not breaching threshold) (correctos [dentro del umbral]).
 - En Actions (Acciones), haga lo siguiente:
 - En Whenever this alarm, elija State is ALARM.
 - En Send notification to (Enviar notificación a), seleccione NotifyMe (Notificarme), New list (Nueva lista) y escriba un nombre de tema único para esta lista.

- En Email list (Lista de direcciones de correo electrónico), escriba la dirección de correo electrónico a donde desea que se envíen las notificaciones. (Debe recibir un correo electrónico en esta dirección para confirmar que ha creado esta alarma).
 - En Alarm Preview (Vista previa de la alarma), haga lo siguiente:
 - En Period (Periodo), seleccione 1 Minute (1 minuto).
 - En Statistic (Estadística), seleccione Standard (Estándar) y Sum (Suma).
3. Elija Create Alarm.

Probar la alarma para la Creación de sistemas de archivos sin cifrar

Para probar la alarma, cree un sistema de archivos sin cifrado en reposo, tal y como se indica a continuación.

Para probar la alarma, cree un sistema de archivos sin cifrado en reposo

1. Inicie sesión en AWS Management Console y abra la consola de Amazon EFS en <https://console.aws.amazon.com/efs/>.
2. Elegir Crear sistema de archivos de para visualizar Crear sistema de archivos de Cuadro de diálogo.
3. Para crear un sistema de archivos sin cifrar en reposo, elija Personalizar para visualizar Configuración del sistema de archivos (Se ha creado el certificado).
4. Para General Configuración, introduzca lo siguiente.
 - a. (Opcional) Introduzca un Nombre para el sistema de archivos.
 - b. Mantener Administración del ciclo de vida, Modo de desempeño, y Modo de desempeño Establecer en los valores predeterminados.
 - c. Desactivación de Criptografía Desactive Habilitar el cifrado de datos en reposo.
5. Elegir Próximo para continuar hasta Network Access paso en el proceso de configuración.
6. Elija el valor predeterminado Virtual Private Cloud (VPC).
7. Para Objetivos de montaje, seleccione el valor predeterminado Grupos de seguridad para cada destino de montaje.
8. Elegir Próximo para visualizar Política del sistema de archivos (Se ha creado el certificado).
9. Elegir Próximo para continuar hasta Revisar y crear (Se ha creado el certificado).

10. Revise el sistema de archivos y elija `CreateFileSystem` para crear el sistema de archivos y volver a la `Sistemas de archivos` (Se ha creado el certificado).

Su registro de seguimiento registra `CreateFileSystem` y suministra el evento a su grupo de registro de CloudWatch Logs. El evento activa la alarma métrica y CloudWatch Logs le envía una notificación sobre el cambio.

Tutorial: Habilite la eliminación raíz mediante la autorización de IAM para clientes NFS

En este tutorial, configurará Amazon EFS para impedir el acceso root a su sistema de archivos de Amazon EFS para todos los AWS principales, excepto para una única estación de trabajo de administración. Para ello, configure la autorización AWS Identity and Access Management (IAM) para los clientes del Sistema de archivos de red (NFS). Para obtener más información acerca de la autorización de IAM para clientes NFS en EFS, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#).

Para ello, es necesario configurar dos políticas de permisos de IAM, de la siguiente manera:

- Cree una política de sistema de archivos EFS que permita explícitamente el acceso de lectura y escritura al sistema de archivos y deniegue implícitamente el acceso del nodo raíz.
- Asigne una identidad de IAM a la estación de trabajo de administración de Amazon EC2 que requiera acceso root al sistema de archivos mediante un perfil de instancia de Amazon EC2. Para obtener más información sobre los perfiles de instancias de Amazon EC2, consulte [Uso de perfiles de instancia](#) en la Guía del AWS Identity and Access Management usuario.
- Asigne la política administrada de `AWS AmazonElasticFileSystemClientFullAccess` al rol de IAM de la estación de trabajo de administración. Para obtener más información sobre las políticas AWS administradas para EFS, consulte [Administración de identidades y acceso Amazon Elastic File System](#).

Para habilitar la agrupación de nodo raíz mediante la autorización de IAM para clientes NFS, utilice los procedimientos siguientes.

Para impedir el acceso root al sistema de archivos

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.

2. Elija Sistemas de archivos.
3. En la página File systems (Sistemas de archivo), elija el sistema de archivos donde desea habilitar la agrupación raíz.
4. En la página de detalles del sistema de archivos, elija Política del sistema de archivos y, a continuación, elija Editar. Aparece la página File system policy (Política del sistema de archivos).

Amazon EFS > File systems > fs-0d4d7e9a948cfa250 > policy

File system policy

Policy options

Select one or more of these common policy options, or create a custom policy using the editor. [Learn more](#)

- Prevent root access by default*
- Enforce read-only access by default*
- Prevent anonymous access
- Enforce in-transit encryption for all clients

* Identity-based policies can override these default permissions.

▶ Grant additional permissions

Policy editor {JSON} Clear

```

1  {
2  "Version": "2012-10-17",
3  "Id": "efs-policy-wizard-aa2f0cf3-ec20-41d8-b862-f979c442382b",
4  "Statement": [
5  {
6  "Sid": "efs-statement-04fb2116-6c7d-4314-8bab-d5fcf28a07c1",
7  "Effect": "Allow",
8  "Principal": {
9  "AWS": "*"
10 },
11 "Action": [
12 "elasticfilesystem:ClientWrite",
13 "elasticfilesystem:ClientMount"
14 ],
15 "Condition": {
16 "Bool": {
17 "elasticfilesystem:AccessedViaMountTarget": "true"
18 }
19 }
20 }
21 ]
22 }
```

Manual changes will prevent the use of the policy options on the left until the editor is cleared.

Cancel Save

5. Seleccione Impedir el acceso root de forma predeterminada* en Opciones de política. El objeto JSON de la política aparece en el editor de políticas.
6. Elija Save (Guardar) para guardar la política del sistema de archivos.

Los clientes que no son anónimos pueden obtener acceso raíz al sistema de archivos a través de una política basada en la identidad. Al adjuntar la política `AmazonElasticFileSystemClientFullAccess` gestionada a la función de la estación de trabajo, IAM concede el acceso raíz a la estación de trabajo en función de su política de identidad.

Para habilitar el acceso raíz desde la estación de trabajo de administración

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. crear un rol para Amazon EC2 llamado `EFS-client-root-access`. IAM crea un perfil de instancia con el mismo nombre que el rol de EC2 que creó.

3. Asigne la política administrada de AWS `AmazonElasticFileSystemClientFullAccess` a la función EC2 que ha creado. El contenido de esta política se muestra a continuación.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource": "*"
    }
  ]
}
```

4. Asocie el perfil de instancia a la instancia EC2 que está utilizando como estación de trabajo de administración, como se describe a continuación. Para obtener más información, consulte [Adjuntar un rol de IAM a una instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
 - a. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
 - b. En el panel de navegación, seleccione Instances (Instancia[s]).
 - c. Seleccione la instancia. Para Actions (Acciones), elija Instance Settings (Configuración de instancia) y, a continuación, elija Attach/Replace IAM role (Asociar/sustituir rol de IAM).
 - d. Seleccione el rol de IAM que creó en el primer paso, `EFS-client-root-access`, y elija Apply (Aplicar).
5. Instale el ayudante de montaje EFS en la estación de trabajo de administración. Para obtener más información sobre el asistente de montaje de EFS y el `amazon-efs-utils` paquete, consulte [Instalación de las herramientas de Amazon EFS](#).
6. Monte el sistema de archivos EFS en la estación de trabajo de administración mediante el siguiente comando con la opción de montaje `iam`.

```
$ sudo mount -t efs -o tls,iam file-system-id:/ efs-mount-point
```


Puede configurar la instancia Amazon EC2 para que monte automáticamente el sistema de archivos con la autorización de IAM. Para obtener más información sobre cómo montar un sistema de archivos de EFS con autorización de IAM, consulte [Montaje con autorización de IAM](#).

Seguridad en Amazon EFS

El [modelo de](#) se aplica a protección de datos en Amazon Elastic File System. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios 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:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

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 cuando trabaja con EFS u otros Servicios de AWS mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede 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.

Temas

- [Cifrado de datos en Amazon EFS](#)
- [Administración de identidades y acceso Amazon Elastic File System](#)
- [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#)
- [Control del acceso de red a sistemas de archivos de Amazon EFS para clientes NFS](#)
- [Trabajar con usuarios, grupos y permisos a nivel del sistema de archivos de red \(NFS\)](#)
- [Trabajo con puntos de acceso de Amazon EFS](#)
- [Bloqueo del acceso público a los sistemas de archivos de Amazon EFS](#)
- [Validación de conformidad para Amazon EFS](#)
- [Resiliencia en Amazon EFS](#)
- [Aislamiento de red para Amazon EFS](#)

Cifrado de datos en Amazon EFS

Amazon EFS admite dos formas de cifrado para sistemas de archivos, el cifrado de datos en tránsito y en reposo. Puede habilitar el cifrado de datos en reposo al crear un sistema de archivos de Amazon EFS. Puede habilitar el cifrado de datos en tránsito cuando monte el sistema de archivos.

Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Si su organización está sujeta a políticas reglamentarias o corporativas que requieren el cifrado de datos y metadatos en reposo, recomendamos crear un sistema de archivos cifrados en reposo y montando el sistema de archivos con el cifrado de datos en tránsito.

Cifrado de datos en reposo

Puede crear sistemas de archivos cifrados mediante la AWS Management Console AWS CLI, la o mediante programación a través de la API Amazon EFS o uno de los AWS SDK. Su organización podría necesitar el cifrado en reposo de todos los datos que cumplan una clasificación específica o que se asocien a una determinada aplicación, carga de trabajo o entorno.

Una vez creado un sistema de archivos de EFS, no puede cambiar su configuración de cifrado. Esto significa que no puede modificar un sistema de archivos no cifrado para cifrarlo. En su lugar, tiene que crear un nuevo sistema de archivos cifrado.

Note

La infraestructura de administración de AWS claves utiliza algoritmos criptográficos aprobados por la norma federal de procesamiento de información (FIPS) 140-2. La infraestructura se adhiere a las recomendaciones del Instituto Nacional de Normas y Tecnología (NIST) 800-57.

Aplicación de la creación de un sistema de archivos de Amazon EFS cifrado en reposo.

Puede utilizar la clave de condición de IAM `elasticfilesystem:Encrypted` en las políticas basadas en la identidad de AWS Identity and Access Management (IAM) para controlar si los usuarios pueden crear sistemas de archivos de Amazon EFS cifrados en reposo. Para obtener más información sobre el uso de la clave de condición, consulte [Ejemplo: Aplicación de la creación de sistemas de archivos cifrados](#).

También puede definir políticas de control de servicios (SCP) internas AWS Organizations para aplicar el cifrado Cuenta de AWS EFS a todos los miembros de su organización. Para obtener más información sobre las políticas de control de servicios AWS Organizations, consulte las [políticas de control de servicios](#) en la Guía del AWS Organizations usuario.

Cifrado de un sistema de archivos en reposo con la consola

Al crear un nuevo sistema de archivos mediante la consola de Amazon EFS, el cifrado en reposo se habilita de forma predeterminada. El siguiente procedimiento describe cómo habilitar el cifrado de un nuevo sistema de archivos cuando se crea desde la consola.

Note

El cifrado en reposo no está habilitado de forma predeterminada al crear un nuevo sistema de archivos mediante la AWS CLI, la API y los SDK. Para obtener más información, consulte [Cree un sistema de archivos \(AWS CLI\)](#).

Para cifrar un nuevo sistema de archivos en la consola de EFS

1. Abra la consola de Amazon Elastic File System en <https://console.aws.amazon.com/efs/>.
2. Seleccione Crear sistema de archivos para abrir el cuadro de diálogo Crear sistema de archivos.
3. De forma opcional, puede ingresar un nombre para el sistema de archivos.
4. Para nube privada virtual (VPC), seleccione su VPC o mantenga la opción configurada como la VPC predeterminada.
5. Seleccione Crear para crear un sistema de archivos que utilice las siguientes configuraciones recomendadas para el servicio:
 - El cifrado de datos en reposo está habilitado con su configuración predeterminada AWS KMS key para Amazon EFS (aws/elasticfilesystem).
 - Copias de seguridad automáticas activadas: Para obtener más información, consulte [Copia de seguridad de los sistemas de archivos de Amazon EFS](#).
 - Destinos de montaje: Amazon EFS crea destinos de montaje con la siguiente configuración:
 - Se encuentra en cada zona de disponibilidad en la Región de AWS que se creó el sistema de archivos.
 - Ubicada en las subredes predeterminadas de la VPC que ha seleccionado.
 - Seleccione el grupo de seguridad predeterminado para la VPC. Puede administrar grupos de seguridad después de crear el sistema de archivos.

Para obtener más información, consulte [Gestión de la accesibilidad de red del sistema de archivos](#).

- Modo de rendimiento de uso general: para obtener más información, consulte [Modos de rendimiento](#).
 - Modo de rendimiento elástico: para obtener más información, consulte [Modos de rendimiento](#).
 - Administración del ciclo de vida de habilitada con una política de 30 días: para obtener más información, consulte [Administrar el almacenamiento del sistema de archivos](#).
6. La página Sistemas de archivos aparece con un encabezado en la parte superior que muestra el estado del sistema de archivos que ha creado. Cuando el sistema de archivos esté disponible, aparecerá un enlace para acceder a la página de detalles del nuevo sistema de archivos en el encabezado.

Ahora tiene un nuevo sistema de encrypted-at-rest archivos.

Funcionamiento del cifrado en reposo

En un sistema de archivos cifrados, los datos y los metadatos se cifran automáticamente antes de escribirse en el sistema de archivos. Del mismo modo, cuando se leen los datos y metadatos, se descifran automáticamente antes de que se presenten a la aplicación. Estos procesos los administra Amazon EFS de forma transparente, por lo que no tiene que modificar las aplicaciones.

Amazon EFS utiliza un algoritmo de cifrado AES-256 EFS estándar de la industria para cifrar datos y metadatos de EFS en reposo. Para obtener más información, consulte los [Conceptos básicos de la criptografía](#) en la Guía del desarrollador de AWS Key Management Service .

Cómo utiliza Amazon EFS AWS KMS

Amazon EFS se integra con AWS Key Management Service (AWS KMS) para la administración de claves. Amazon EFS usa claves maestras de cliente para cifrar el sistema de archivos de la siguiente forma:

- Cifrado de metadatos en reposo: Amazon EFS utiliza Amazon EFS Clave administrada de AWS para cifrar y descifrar los metadatos del sistema de archivos (es decir, `aws/elasticfilesystem` los nombres de los archivos, los nombres de los directorios y el contenido de los directorios).
- Cifrado de datos de archivos en reposo: elija la clave administrada por el cliente usada para cifrar y descifrar los datos de archivo (es decir, el contenido de los archivos). Puede habilitar, deshabilitar o revocar concesiones en esta clave administrada por el cliente. Esta clave administrada por el cliente puede ser de uno de los dos siguientes tipos:
 - Clave administrada de AWS para Amazon EFS: esta es la clave administrada por el cliente predeterminada, `aws/elasticfilesystem`. No se le cobrará por crear ni almacenar una clave administrada por el cliente, pero sí por utilizarla. Para obtener más información, consulte [Precios de AWS Key Management Service](#).
 - Clave administrada por el cliente: se trata de la clave del KMS más flexible, ya que puede configurar las políticas de claves y concesiones para varios usuarios o servicios. Para obtener más información sobre la creación de claves administradas por el cliente, consulte [Creación de claves](#) en la Guía para AWS Key Management Service desarrolladores.

Si utiliza una clave administrada por el cliente para el cifrado y descifrado de datos de archivo, puede activar la rotación de claves. Cuando habilitas la rotación de claves, la rota AWS KMS automáticamente una vez al año. Además, una clave administrada por el cliente le permite elegir el momento en que desea deshabilitar, volver a habilitar, eliminar o revocar el acceso a su

clave gestionada por el cliente en cualquier momento. Para obtener más información, consulte [Administrar el acceso a la clave KMS de un sistema de archivos](#).

⚠ Important

Amazon EFS solo acepta claves simétricas administradas por el cliente. No puede usar claves asimétricas administradas por el cliente con Amazon EFS.

El cifrado y descifrado de datos en reposo se administran de forma transparente. Sin embargo, los ID de AWS cuenta específicos de Amazon EFS aparecen en AWS CloudTrail los registros relacionados con AWS KMS las acciones. Para obtener más información, consulte [Entradas de archivos de registro de Amazon EFS para sistemas de encrypted-at-rest archivos](#).

Políticas clave de Amazon EFS para AWS KMS

Las políticas de claves son la forma principal de controlar el acceso a las claves administradas por el cliente. Para obtener más información sobre las políticas de claves, consulte [Políticas de claves en AWS KMS](#) en la Guía para desarrolladores de AWS Key Management Service . En la siguiente lista se describen todos los permisos AWS KMS relacionados que Amazon EFS requiere o admite de otro modo para los sistemas de archivos cifrados en reposo:

- kms:Encrypt - (opcional): cifra texto plano en texto cifrado. Este permiso está incluido en la política de claves predeterminada.
- kms: Decrypt: (obligatorio) descifra texto cifrado. El texto cifrado es texto no cifrado que se ha cifrado previamente. Este permiso está incluido en la política de claves predeterminada.
- kms: ReEncrypt — (opcional) Cifra los datos del lado del servidor con una nueva clave administrada por el cliente, sin exponer el texto sin formato de los datos del lado del cliente. Los datos se descifran en primer lugar y luego se vuelven a cifrar. Este permiso está incluido en la política de claves predeterminada.
- kms: GenerateData KeyWithout Plaintext — (obligatorio) Devuelve una clave de cifrado de datos cifrada con una clave gestionada por el cliente. Este permiso está incluido en la política de claves predeterminada en kms: GenerateData Key*.
- kms: CreateGrant — (Obligatorio) Añade una concesión a una clave para especificar quién puede utilizarla y en qué condiciones. Las concesiones son mecanismos de permiso alternativo para las políticas de claves. Para obtener más información sobre las concesiones, consulte [Uso de](#)

[concesiones](#) en la Guía para desarrolladores de AWS Key Management Service . Este permiso está incluido en la política de claves predeterminada.

- kms: DescribeKey — (Obligatorio) Proporciona información detallada sobre la clave gestionada por el cliente especificada. Este permiso está incluido en la política de claves predeterminada.
- kms: ListAliases — (opcional) Muestra todos los alias clave de la cuenta. Si utiliza la consola para crear un sistema de archivos cifrados, este permiso rellena la lista Seleccionar clave maestra de KMS. Le recomendamos que utilice este permiso para proporcionar la mejor experiencia de usuario. Este permiso está incluido en la política de claves predeterminada.

Clave administrada de AWS para la política de Amazon EFS KMS

La política JSON de KMS Clave administrada de AWS para Amazon EFS `aws/elasticfilesystem` es la siguiente:

```
{
  "Version": "2012-10-17",
  "Id": "auto-elasticfilesystem-1",
  "Statement": [
    {
      "Sid": "Allow access to EFS for all principals in the account that are
authorized to use EFS",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "elasticfilesystem.us-east-2.amazonaws.com",
          "kms:CallerAccount": "111122223333"
        }
      }
    }
  ],
}
```



```
{
  "Sid": "Allow direct access to key metadata to the account",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "kms:Describe*",
    "kms:Get*",
    "kms:List*",
    "kms:RevokeGrant"
  ],
  "Resource": "*"
}
]
```

Cifrado de datos en tránsito

Habilitar el cifrado de datos en tránsito para el sistema de archivos de Amazon EFS se realiza habilitando TLS (Transport Layer Security) cuando se monta el sistema de archivos mediante dicho ayudante de montaje de Amazon EFS. Para obtener más información, consulte [Montaje del sistema de archivos de EFS mediante el ayudante de montaje de EFS.](#)

Cuando el cifrado de datos en tránsito se declara como una opción de montaje para su sistema de archivos de Amazon EFS, el ayudante de montaje inicializa un proceso stunnel cliente. Stunnel es una retransmisión de red multipropósito de código abierto. El proceso de stunnel cliente escucha en un puerto local el tráfico entrante y el ayudante de montaje redirige el tráfico de cliente de sistema de archivos de red (NFS) a este puerto local. El ayudante de montaje usa TLS versión 1.2 para comunicarse con su sistema de archivos.

Para montar el sistema de archivos de Amazon EFS con el ayudante de montaje con el cifrado de datos en tránsito habilitado

1. Obtenga acceso al terminal de la instancia a través de Secure Shell (SSH) e inicie sesión con el nombre de usuario adecuado. Para obtener más información sobre cómo hacerlo, consulta [Conéctate a tu instancia de Linux desde Linux o macOS mediante SSH.](#)
2. Ejecute el siguiente comando para montar el sistema de archivos.

```
sudo mount -t efs -o tls fs-12345678:/ /mnt/efs
```

Cómo funciona el cifrado en tránsito

Para habilitar el cifrado de datos en tránsito, Amazon EFS se conecta mediante TLS.

Recomendamos utilizar el asistente de montaje de EFS para montar el sistema de archivos, ya que simplifica el proceso de montaje en comparación con el montaje con `mount` de NFS. El asistente de montaje de EFS gestiona el proceso mediante `stunnel` para TLS. Aunque no utilice el ayudante de montaje, puede habilitar el cifrado de datos en tránsito. A grandes rasgos, los pasos para hacerlo son los siguientes:

Para habilitar el cifrado de datos en tránsito sin el ayudante de montaje de EFS

1. Descargue e instale `stunnel`, y anote el puerto en que la aplicación escucha. Consulte [Actualización de stunnel](#) para obtener instrucciones al respecto.
2. Ejecute `stunnel` para conectarse al sistema de archivos de Amazon EFS en el puerto 2049 mediante TLS.
3. Utilizando el cliente NFS, monte `localhost:port`, donde `port` es el puerto que anotó en el primer paso.

Debido a que el cifrado de datos en tránsito se configura según cada base de conexión, cada montaje configurado tiene un proceso `stunnel` específico que se ejecuta en la instancia. De forma predeterminada, el proceso de `stunnel` utilizado por el ayudante de montaje de EFS escucha en los puertos locales 20049 y 21049 y se conecta con Amazon EFS en el puerto 2049.

Note

De forma predeterminada, cuando se utiliza el ayudante de montaje de Amazon EFS con TLS, el ayudante de montaje aplica la comprobación de nombre de host del certificado. El ayudante de montaje de Amazon EFS utiliza el programa `stunnel` para la funcionalidad de TLS. Algunas versiones de Linux no incluyen una versión de `stunnel` que admita estas características de TLS de forma predeterminada. Cuando se utiliza una de esas versiones de Linux, montar un sistema de archivos de Amazon EFS mediante TLS da error.

Una vez instalado el `amazon-efs-utils` paquete, consulte para actualizar la versión de `stunnel` de su sistema. [Actualización de stunnel](#)

Si tiene problemas con el cifrado, consulte [Resolución de problemas de cifrado](#).

Cuando se utiliza el cifrado de datos en tránsito, la configuración de su cliente NFS se modifica. Cuando inspecciona los sistemas de archivos montados activamente, verá uno montado en 127.0.0.1 o localhost, tal y como se muestra en el siguiente ejemplo.

```
$ mount | column -t
127.0.0.1:/ on /home/ec2-user/efs          type nfs4
(rw,relatime,vers=4.1,rsize=1048576,wsiz=1048576,namlen=255,hard,proto=tcp,port=20127,timeo=600)
```

Cuando monta con TLS y el ayudante de montaje de Amazon EFS, vuelve a configurar el cliente NFS para montar en un puerto local. El ayudante de montaje de EFS inicia un proceso `stunnel` de cliente que escucha en este puerto local y `stunnel` abre una conexión cifrada al sistema de archivos de EFS usando TLS. El ayudante de montaje de EFS es responsable de la configuración y el mantenimiento de esta conexión cifrada y la configuración asociada.

Para determinar qué ID de sistema de archivos de Amazon EFS corresponde a qué punto de montaje, puede utilizar el siguiente comando. Reemplace *efs-mount-point* por la ruta local donde montó el sistema de archivos.

```
grep -E "Successfully mounted.*efs-mount-point" /var/log/amazon/efs/mount.log | tail -1
```

Cuando utiliza el ayudante de montaje para el cifrado de datos en tránsito, también se crea un proceso denominado `amazon-efs-mount-watchdog`. Este proceso de vigilancia garantiza que cada proceso de `stunnel` del montaje se está ejecutando y detiene el `stunnel` cuando el sistema de archivos de Amazon EFS está desmontado. Si por alguna razón un proceso de `stunnel` termina de forma inesperada, el proceso del `watchdog` lo reinicia.

Resolución de problemas de cifrado

A continuación, encontrará información sobre la solución de problemas de cifrado de Amazon EFS.

- [Error de montaje con cifrado de los datos en tránsito](#)
- [Interrupción del montaje con cifrado de los datos en tránsito](#)
- [No se puede crear un sistema de `ncrypted-at-rest` archivos](#)
- [El sistema de archivos cifrado no se puede usar](#)

Error de montaje con cifrado de los datos en tránsito

De forma predeterminada, cuando se utiliza el ayudante de montaje de Amazon EFS con TLS (Transport Layer Security), se aplica la comprobación del nombre de host. Algunos sistemas no admiten esta característica, por ejemplo, cuando se utiliza Red Hat Enterprise Linux o CentOS. En estos casos, se produce un error al montar un sistema de archivos de EFS mediante TLS.

Acción que debe ejecutarse

Se recomienda actualizar la versión de stunnel en el cliente para que admita la comprobación del nombre de host. Para obtener más información, consulte [Actualización de stunnel1](#).

Interrupción del montaje con cifrado de los datos en tránsito

Es posible, aunque poco probable, que su conexión cifrada a su sistema de archivos de Amazon EFS deje de responder o se interrumpa por eventos del lado del cliente.

Acción que debe ejecutarse

Si la conexión a su sistema de archivos de Amazon EFS con cifrado de datos en tránsito se interrumpe, siga estos pasos:

1. Asegúrese de que el servicio stunnel se está ejecutando en el cliente.
2. Confirme que la aplicación de vigilancia amazon-efs-mount-watchdog se está ejecutando en el cliente. Puede averiguar si esta aplicación se está ejecutando con el siguiente comando:

```
ps aux | grep [a]mazon-efs-mount-watchdog
```

3. Compruebe los registros de soporte. Para obtener más información, consulte [Obtención de registros de soporte](#).
4. Si lo desea, puede habilitar los registros de stunnel y comprobar también esa información. Puede cambiar la configuración de los registros en `/etc/amazon/efs/efs-utils.conf` para habilitar los registros de stunnel. Sin embargo, esto requiere desmontar y volver a montar el sistema de archivos con el ayudante de montaje para que los cambios surtan efecto.

Important

Habilitar los registros de stunnel puede utilizar una cantidad de espacio nada despreciable en el sistema de archivos.

Si las interrupciones continúan, ponte en contacto con AWS Support.

No se puede crear un sistema de encrypted-at-rest archivos

Intentó crear un nuevo sistema de encrypted-at-rest archivos. Sin embargo, aparece un mensaje de error que indica que no AWS KMS está disponible.

Acción que debe ejecutarse

Este error puede ocurrir en el raro caso de que deje de estar AWS KMS disponible temporalmente en su Región de AWS. Si esto ocurre, espere a que AWS KMS vuelva a estar completamente disponible y, a continuación, vuelva a intentar crear el sistema de archivos.

El sistema de archivos cifrado no se puede usar

Un sistema de archivos cifrados de forma coherente devuelve errores de servidor de NFS. Estos errores pueden producirse cuando EFS no puede recuperar la clave maestra AWS KMS por uno de los siguientes motivos:

- La clave se ha desactivado.
- La clave se ha eliminado.
- El permiso de Amazon EFS para utilizar la clave se ha revocado.
- AWS KMS no está disponible temporalmente.

Acción que debe ejecutarse

En primer lugar, confirme que la AWS KMS clave esté habilitada. Para ello, consulte las claves en la consola. Para obtener información, consulte [Visualización de claves](#) en la Guía del desarrollador de AWS Key Management Service .

Si la clave no está habilitada, habilítela. Para obtener más información, consulte [Habilitar y deshabilitar claves](#) en la Guía del desarrollador de AWS Key Management Service .

Si la clave está pendiente de eliminación, este estado deshabilita la clave. Puede cancelar la eliminación y volver a habilitar la clave. Para obtener más información, consulte [Programación y cancelación de eliminación de claves](#) en la Guía del desarrollador de AWS Key Management Service .

Si la clave está habilitada y el problema persiste, o si se produce algún problema al volver a activar la clave, ponte en contacto con AWS Support.

Administración de identidades y acceso Amazon Elastic File System

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 se puede autenticar (iniciar sesión) y autorizar (tener permisos) para utilizar los recursos de Amazon EFS. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona Amazon Elastic File System con IAM](#)
- [Ejemplos de políticas basadas en identidades de Amazon Elastic File System](#)
- [Ejemplos de políticas basadas en recursos de Amazon Elastic File System](#)
- [Políticas administradas por AWS para Amazon EFS](#)
- [Uso de etiquetas con Amazon EFS](#)
- [Uso de roles vinculados a servicios para Amazon EFS](#)
- [Solución de problemas de identidad y acceso de Amazon Elastic File System](#)

Público

La forma en que utilice AWS Identity and Access Management (IAM) varía, en función del trabajo que realice en Amazon EFS.

Usuario de servicio: si utiliza el servicio Amazon EFS para realizar el trabajo, el administrador proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Amazon EFS para realizar el trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica de Amazon EFS, consulte [Solución de problemas de identidad y acceso de Amazon Elastic File System](#).

Administrador de servicio: si está a cargo de los recursos de Amazon EFS de la empresa, probablemente tenga acceso completo a Amazon EFS. El trabajo consiste en determinar a qué características y recursos de Amazon EFS deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información acerca de cómo la empresa puede utilizar IAM con Amazon EFS, consulte [Cómo funciona Amazon Elastic File System con IAM](#).

Administrador de IAM: si es un administrador de IAM, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso a Amazon EFS. Para consultar ejemplos de políticas de Amazon EFS basadas en identidades que puede utilizar en IAM, consulte [Ejemplos de políticas basadas en identidades de Amazon Elastic File System](#).

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (del Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso a AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte [Cómo iniciar sesión en su Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte [Firma de solicitudes API de AWS](#) en la Guía del usuario de IAM.

Independientemente del método de autenticación que utilice, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación

multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactor](#) en la Guía del usuario de AWS IAM Identity Center y [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.

Usuario raíz de Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a los servicios de Servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de identidad. Cuando identidades federadas acceden a las Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. 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 en su Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran

credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte [Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración](#) en la Guía del Usuario de IAM.

Un [grupo de IAM](#) es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte [Cuándo crear un usuario de IAM \(en lugar de un rol\)](#) en la Guía del Usuario de IAM.

Roles de IAM

Un [rol de IAM](#) es una identidad en su Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Console [cambiando de roles](#). Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte [Uso de roles de IAM](#) en la Guía del Usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte [Creación de un rol para un proveedor de identidades de terceros](#) en la Guía del Usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center.
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
- **Reenviar sesiones de acceso (FAS):** cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza 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. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).
- **Rol de servicio:** un rol de servicio es un [rol de IAM](#) que adopta 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 [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.
- **Rol vinculado a servicios:** 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 su 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.
- **Aplicaciones que se ejecutan en Amazon EC2:** puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a

la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2](#) en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte [Cuándo crear un rol de IAM \(en lugar de un usuario\)](#) en la Guía del Usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de las políticas JSON](#) en la Guía del Usuario de IAM.

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.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. 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 en función de identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte [Elegir 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 política JSON que se asocian a un recurso. 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 en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Listas de control de acceso (ACL)

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 política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte [Información general de Lista de control de acceso \(ACL\)](#) en la Guía para Desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política en función de identidad puede conceder a una

entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del Usuario de IAM.

- **Políticas de control de servicio (SCP):** las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada `rootlong`. Para más información sobre organizaciones y las SCP, consulte [Funcionamiento de las SCP](#) en la Guía del Usuario de AWS Organizations.
- **Políticas de sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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 sobre cómo AWS decide si permite 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 Elastic File System con IAM

Antes de utilizar IAM para administrar el acceso a Amazon EFS, obtenga información sobre qué características de IAM se encuentran disponibles con Amazon EFS.

Características de IAM que puede utilizar con Amazon Elastic File System

Características de IAM	Compatibilidad de Amazon EFS
Políticas basadas en identidad	Sí
Políticas basadas en recursos	Sí
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
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una perspectiva general sobre cómo funcionan Amazon EFS y otros servicios de AWS con la mayoría de las características de IAM, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Políticas de Amazon EFS basadas en identidades

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 identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Con las políticas basadas en identidad 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. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre los elementos que puede utilizar en una política JSON, consulte [Referencia de los elementos de las políticas JSON de IAM](#) en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para Amazon EFS

Para ver ejemplos de políticas basadas en identidades de Amazon EFS, consulte [Ejemplos de políticas basadas en identidades de Amazon Elastic File System](#).

Políticas basadas en recursos de Amazon EFS

Compatibilidad con las políticas basadas en recursos	Sí
--	----

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. 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 en función de 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. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política en

función de identidad adicional. Para más información, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del Usuario de IAM.

Para obtener información sobre el uso de una política de recursos para controlar el acceso a los datos del sistema de archivos, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#). Para obtener información sobre cómo asociar una política basada en recursos a un sistema de archivos, consulte [Creación de políticas de sistema de archivos](#).

Política basada en recursos de Amazon EFS

Para ver ejemplos de políticas basadas en recursos de Amazon EFS, consulte [Ejemplos de políticas basadas en recursos de Amazon Elastic File System](#).

Acciones de políticas para Amazon EFS

Admite acciones de política	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 permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Amazon EFS, consulte [Acciones definidas por Amazon Elastic File System](#) en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Amazon EFS utilizan el siguiente prefijo antes de la acción:

```
elasticfilesystem
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.


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

Para ver ejemplos de políticas basadas en identidades de Amazon EFS, consulte [Ejemplos de políticas basadas en identidades de Amazon Elastic File System](#).

Recursos de políticas para Amazon EFS

Admite 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. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, 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 Amazon EFS y sus ARN, consulte [Tipos de recurso definidos por Amazon Elastic File System](#) en la Referencia de autorizaciones de servicio. Para obtener información acerca de las acciones con las que puede especificar el ARN de cada recurso, consulte [Acciones definidas por Amazon Elastic File System](#).

Para ver ejemplos de políticas basadas en identidades de Amazon EFS, consulte [Ejemplos de políticas basadas en identidades de Amazon Elastic File System](#).

Claves de condición de políticas para Amazon EFS

Admite 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` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica AND. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación OR lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte [Elementos de la política de IAM: variables y etiquetas](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. 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 Amazon EFS, consulte [Claves de condición para Amazon Elastic File System](#) 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 Elastic File System](#).

Para ver ejemplos de políticas basadas en identidades de Amazon EFS, consulte [Ejemplos de políticas basadas en identidades de Amazon Elastic File System](#).

ACL en Amazon EFS

Admite las 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 Amazon EFS

Admite 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. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

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 [¿Qué es 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.

Uso de credenciales temporales con Amazon EFS

Admite el uso de credenciales temporales	Sí
--	----

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con

credenciales temporales, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Utilice credenciales temporales si inicia sesión en la AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte [Cambio a un rol \(consola\)](#) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulte [Credenciales de seguridad temporales en IAM](#).

Permisos de entidades principales entre servicios de Amazon EFS

Admite Forward access sessions (FAS)	Sí
--------------------------------------	----

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza 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. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).

Roles de servicio para Amazon EFS

Compatible con roles de servicio	Sí
----------------------------------	----

Un rol del 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 [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

Warning

Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Amazon EFS. Edite los roles de servicio solo cuando Amazon EFS proporcione orientación para hacerlo.

Roles vinculado a servicios para Amazon EFS

Admite roles vinculados a servicios	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 su 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.

Para obtener más información sobre cómo crear o administrar roles vinculados a servicios de Amazon EFS, consulte [Uso de roles vinculados a servicios para Amazon EFS](#).

Ejemplos de políticas basadas en identidades de Amazon Elastic File System

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de Amazon EFS. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política basada en identidad de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por Amazon EFS, incluido el formato de los ARN para cada tipo de recurso, consulte [Acciones, recursos y claves de condición para Amazon Elastic File System](#) en la Referencia de autorizaciones de servicio.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la consola de Amazon EFS](#)
- [Ejemplo: Permitir que los usuarios vean sus propios permisos](#)
- [Ejemplo: Aplicación de la creación de sistemas de archivos cifrados](#)
- [Ejemplo: Aplicación de la creación de sistemas de archivos sin cifrar](#)

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, eliminar o acceder a los recursos de Amazon EFS de la cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas de AWS, que conceden 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 los 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 trabajo](#) en la Guía del 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 de 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 política 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 AWS

CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.

- Utilice 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 la [Política de validación del analizador de acceso de IAM](#) en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para obtener más información, consulte [Configuración de acceso a una API protegida por MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Uso de la consola de Amazon EFS

Para acceder a la consola de Amazon Elastic File System, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle mostrar y consultar los detalles sobre los recursos de Amazon EFS en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para asegurarse de que los usuarios y los roles puedan seguir utilizando la consola de Amazon EFS, asocie también la política administrada por AWS `AmazonElasticFileSystemReadOnlyAccess` de Amazon EFS a las entidades. Para obtener más información, consulte [Adición de permisos a un usuario](#) en la Guía del usuario de IAM.

Puede consultar la `AmazonElasticFileSystemReadOnlyAccess` y otras políticas de servicios administrados de Amazon EFS en [Políticas administradas por AWS para Amazon EFS](#).

Ejemplo: Permitir que los usuarios vean 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 realizar 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:ListGroupsWithUser",
        "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": "*"
    }
  ]
}
```


Ejemplo: Aplicación de la creación de sistemas de archivos cifrados

En el siguiente ejemplo se muestra una política basada en identidades que autoriza a las entidades principales a crear solo sistemas de archivos cifrados.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "elasticfilesystem:CreateFileSystem",
      "Condition": {
        "Bool": {
          "elasticfilesystem:Encrypted": "true"
        }
      },
      "Resource": "*"
    }
  ]
}
```

Si esta política se asigna a un usuario que intenta crear un sistema de archivos sin cifrar, se produce un error en la solicitud. El usuario ve un mensaje similar al siguiente, independientemente de si utiliza la AWS Management Console, la AWS CLI o la API o el SDK de AWS:

```
User: arn:aws:iam::111122223333:user/username is not authorized to
perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

Ejemplo: Aplicación de la creación de sistemas de archivos sin cifrar

En el siguiente ejemplo se muestra una política basada en identidades que autoriza a las entidades principales a crear solo sistemas de archivos sin cifrar.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "elasticfilesystem:CreateFileSystem",
      "Condition": {
        "Bool": {
          "elasticfilesystem:Encrypted": "false"
        }
      },
    }
  ]
}
```

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

Si esta política se asigna a un usuario que intenta crear un sistema de archivos cifrado, se produce un error en la solicitud. El usuario ve un mensaje similar al siguiente, independientemente de si utiliza la AWS Management Console, la AWS CLI o la API o el SDK de AWS:

```
User: arn:aws:iam::111122223333:user/username is not authorized to
perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

También puede imponer la creación de sistemas de archivos de Amazon EFS cifrados o no cifrados mediante la creación de una política de control de servicios (SCP) de AWS Organizations. Para obtener más información acerca de las políticas de control de servicios en AWS Organizations, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations.

Ejemplos de políticas basadas en recursos de Amazon Elastic File System

En esta sección, puede encontrar políticas de sistema de archivos de ejemplo que conceden o deniegan permisos para varias acciones de Amazon EFS. Las políticas del sistema de archivos de Amazon EFS tienen un límite de 20 000 caracteres. Para obtener información sobre los elementos de una política basada en recursos, consulte [Políticas basadas en recursos de Amazon EFS](#).

Important

Si concede permiso a un usuario o rol de IAM individual en una política de sistema de archivos, no elimine ni vuelva a crear ese usuario o rol mientras la política siga vigente en el sistema de archivos. Si esto sucede, ese usuario o rol se bloquea efectivamente en el sistema de archivos y no podrá acceder a él. Para obtener más información, consulte [Especificación de una entidad principal](#) en la Guía del usuario de IAM.

Para obtener información acerca de cómo crear una política de sistema de archivos, consulte [Creación de políticas de sistema de archivos](#).

Temas

- [Ejemplo: conceder acceso de lectura y escritura a un rol de AWS específico](#)
- [Ejemplo: conceder acceso de solo lectura](#)
- [Ejemplo: Otorgar acceso a un punto de acceso de EFS](#)

Ejemplo: conceder acceso de lectura y escritura a un rol de AWS específico

En este ejemplo, la política de sistema de archivos de EFS tiene las características siguientes:

- El efecto es Allow.
- La entidad principal se establece en Testing_Role en la Cuenta de AWS.
- La acción se establece en ClientMount (lectura) y ClientWrite.
- La condición para conceder permisos se establece en AccessedViaMountTarget.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/Testing_Role"
      },
      "Action": [
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientMount"
      ],
      "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-system/
fs-1234abcd",
      "Condition": {
        "Bool": {
          "elasticfilesystem:AccessedViaMountTarget": "true"
        }
      }
    }
  ]
}
```

Ejemplo: conceder acceso de solo lectura

La siguiente política del sistema de archivos solo concede permisos ClientMount, o de solo lectura, a todos los roles de IAM EfsReadOnly.

```
{
  "Id": "read-only-example-policy02",
  "Statement": [
    {
      "Sid": "efs-statement-example02",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/EfsReadOnly"
      },
      "Action": [
        "elasticfilesystem:ClientMount"
      ],
      "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-system/
fs-12345678"
    }
  ]
}
```

Para obtener información sobre cómo establecer políticas adicionales del sistema de archivos, incluida la denegación del acceso raíz a todas las entidades principales de IAM, excepto una estación de trabajo de administración específica, consulte [Tutorial: Habilite la eliminación raíz mediante la autorización de IAM para clientes NFS](#).

Ejemplo: Otorgar acceso a un punto de acceso de EFS

Utilice una política de acceso de EFS para proporcionar a un cliente de NFS una vista específica de la aplicación en conjuntos de datos basados en archivos compartidos en un sistema de archivos de EFS. Conceder permisos de punto de acceso en el sistema de archivos mediante una política de sistema de archivos.

En este ejemplo de política de archivos se utiliza un elemento de condición para conceder un punto de acceso específico que se identifica por el acceso completo de su ARN al sistema de archivos.

Para obtener más información acerca de los puntos de acceso de EFS, consulte [Trabajo con puntos de acceso de Amazon EFS](#).

```
{
  "Id": "access-point-example03",
  "Statement": [
    {
      "Sid": "access-point-statement-example03",
      "Effect": "Allow",
```

```
    "Principal": {"AWS": "arn:aws:iam::555555555555:role/
EfsAccessPointFullAccess"},
    "Action": "elasticfilesystem:Client*",
    "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-system/
fs-12345678",
    "Condition": {
      "StringEquals": {
        "elasticfilesystem:AccessPointArn": "arn:aws:elasticfilesystem:us-
east-2:555555555555:access-point/fsap-12345678" }
      }
    }
  ]
}
```

Políticas administradas por AWS para Amazon EFS

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Considere que es posible que las políticas administradas por AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir [políticas administradas por el cliente](#) para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas de AWS. Si AWS actualiza los permisos definidos en una política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte [Políticas administradas por AWS](#) en la Guía del usuario de IAM.

política administrada por AWS: AmazonElasticfilesystemAccess

Puede adjuntar la política de AmazonElasticFileSystemFullAccess a las identidades de IAM.

Esta política concede permisos administrativos que brindan acceso completo a Amazon EFS y a los servicios relacionados de AWS a través de la AWS Management Console.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `elasticfilesystem`: permite que las entidades principales realicen todas las acciones en la consola de administración de Amazon EFS. También permite a las entidades principales crear (`elasticfilesystem:Backup`) y restaurar (`elasticfilesystem:Restore`) copias de seguridad mediante AWS Backup.
- `cloudwatch`: permite a las entidades principales describir las métricas y alarmas del sistema de archivos de Amazon CloudWatch para una métrica en la consola de Amazon EFS.
- `ec2`: permite a las entidades principales crear, eliminar y describir las interfaces de red, describir y modificar los atributos de las interfaces de red, describir las zonas de disponibilidad, los grupos de seguridad, las subredes, las nubes virtuales privadas (VPC) y los atributos de VPC asociados a un sistema de archivos de Amazon EFS en la consola de Amazon EFS.
- `kms`: permite a las entidades principales enumerar los alias de las claves AWS Key Management Service (AWS KMS) y describir las claves de KMS en la consola de Amazon EFS.
- `iam`: concede permiso para crear un rol asociado a un servicio que permite a un servicio de Amazon EFS administrar recursos de AWS en su nombre.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:Backup",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
```

```

    "elasticfilesystem:CreateTags",
    "elasticfilesystem:CreateAccessPoint",
    "elasticfilesystem:CreateReplicationConfiguration",
    "elasticfilesystem>DeleteFileSystem",
    "elasticfilesystem>DeleteMountTarget",
    "elasticfilesystem>DeleteTags",
    "elasticfilesystem>DeleteAccessPoint",
    "elasticfilesystem>DeleteFileSystemPolicy",
    "elasticfilesystem>DeleteReplicationConfiguration",
    "elasticfilesystem:DescribeAccountPreferences",
    "elasticfilesystem:DescribeBackupPolicy",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeFileSystemPolicy",
    "elasticfilesystem:DescribeLifecycleConfiguration",
    "elasticfilesystem:DescribeMountTargets",
    "elasticfilesystem:DescribeMountTargetSecurityGroups",
    "elasticfilesystem:DescribeReplicationConfigurations",
    "elasticfilesystem:DescribeTags",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:ModifyMountTargetSecurityGroups",
    "elasticfilesystem:PutAccountPreferences",
    "elasticfilesystem:PutBackupPolicy",
    "elasticfilesystem:PutLifecycleConfiguration",
    "elasticfilesystem:PutFileSystemPolicy",
    "elasticfilesystem:UpdateFileSystem",
    "elasticfilesystem:UpdateFileSystemProtection",
    "elasticfilesystem:TagResource",
    "elasticfilesystem:UntagResource",
    "elasticfilesystem:ListTagsForResource",
    "elasticfilesystem:Restore",
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Sid": "ElasticFileSystemFullAccess",
  "Effect": "Allow",
  "Resource": "*"
},
{
  "Action": "iam:CreateServiceLinkedRole",
  "Sid": "CreateServiceLinkedRoleForEFS",
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {

```

```

        "StringEquals": {
            "iam:AWSServiceName": [
                "elasticfilesystem.amazonaws.com"
            ]
        }
    }
}

```

Política gestionada por AWS: AmazonElasticFileSystemReadOnlyAccess

Puede adjuntar la política de AmazonElasticFileSystemReadOnlyAccess a las identidades de IAM.

Esta política también concede acceso de solo lectura a Amazon EFS de AWS Management Console.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `elasticfilesystem`: permite a las entidades principales describir los atributos de los sistemas de archivos de Amazon EFS, incluidas las preferencias de las cuentas, las políticas de copia de seguridad y del sistema de archivos, la configuración del ciclo de vida, los destinos de montaje y sus grupos de seguridad, etiquetas y puntos de acceso en la consola de Amazon EFS.
- `cloudwatch`: permite a las entidades principales recuperar las métricas de CloudWatch y describir alarmas para las métricas en la consola de Amazon EFS.
- `ec2`: permite a las entidades principales ver las zonas de disponibilidad, las interfaces de red y sus atributos, los grupos de seguridad, las subredes, las VPC y sus atributos en la consola de Amazon EFS.
- `kms`: permite que las entidades principales enumeren los alias de las claves de AWS KMS en la consola de Amazon EFS.

```

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

```



```

    "Effect": "Allow",
    "Action": [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "kms:ListAliases"
    ],
    "Resource": "*"
}
]
}

```

Política gestionada por AWS: AmazonElasticFileSystemClientReadWriteAccess

Puede adjuntar la política AmazonElasticFileSystemClientReadWriteAccess a una entidad de IAM.

Esta política proporciona acceso de cliente de lectura y escritura a un sistema de archivos de Amazon EFS. Esta política permite a los clientes de NFS montar, leer y escribir en los sistemas de archivos de Amazon EFS.

```

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

```

```

    "Effect": "Allow",
    "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource": "*"
}
]
}

```

Actualizaciones de Amazon EFS a políticas administradas por AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para Amazon EFS desde que este servicio comenzó a hacer un seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbese a la fuente RSS en la página [Historial de documentos](#) de Amazon EFS.

Cambio	Descripción	Fecha
Actualización de una política existente	Política: AmazonElasticFileSystemFullAccess Amazon EFS agregó un nuevo permiso para permitir a las entidades principales deshabilitar y habilitar la protección en un sistema de archivos. Los permisos son necesarios para permitir que Amazon EFS se replique en un sistema de archivos existente.	27 de noviembre de 2023
Actualización de una política existente	Política: AmazonElasticFileSystemServiceRolePolicy Amazon EFS agregó nuevos permisos para permitir a las entidades principales crear, describir y eliminar replicas de Amazon EFS y crear sistemas de archivos de Amazon EFS. Los permisos son necesarios para permitir que Amazon EFS administre las configuraciones de replicación del sistema de archivos en nombre del usuario.	25 de enero de 2022

Cambio	Descripción	Fecha
Actualización de una política existente	Política: AmazonElasticFileSystemReadOnlyAccess Amazon EFS agregó un nuevo permiso para permitir a las entidades principales describir las replicas de Amazon EFS. Los permisos son necesarios para permitir que los usuarios vean las configuraciones de replicación del sistema de archivos.	25 de enero de 2022
Actualización de una política existente	Política: AmazonElasticFileSystemFullAccess Amazon EFS agregó nuevos permisos para permitir a las entidades principales crear, describir y eliminar replicas de Amazon EFS. Los permisos son necesarios para permitir que los usuarios administran en las configuraciones de replicación del sistema de archivos.	25 de enero de 2022
Comenzó la política de seguimiento	Política: AmazonElasticFileSystemClientReadWriteAccess Otorga privilegios de lectura y escritura en los sistemas de archivos de Amazon EFS a los clientes de NFS.	3 de enero de 2022
Comenzó la política de seguimiento	Política: AmazonElasticFileSystemServiceRolePolicy Permisos de roles vinculados a un servicio para Amazon EFS.	8 de octubre de 2021

Cambio	Descripción	Fecha
Actualización de una política existente	Política: AmazonElasticFileSystemFullAccess Amazon EFS agregó nuevos permisos para permitir a las entidades principales modificar y describir las preferencias de las cuentas de Amazon EFS. Los permisos son necesarios para que los usuarios puedan ver y establecer los ajustes de las preferencias de la cuenta en la consola de Amazon EFS.	7 de mayo de 2021
Actualización de una política existente	Política: AmazonElasticFileSystemReadOnlyAccess Amazon EFS agregó nuevos permisos para permitir a las entidades principales describir las preferencias de las cuentas de Amazon EFS. Los permisos son necesarios para que los usuarios puedan ver los ajustes de las preferencias de la cuenta en la consola de Amazon EFS.	7 de mayo de 2021
Amazon EFS ha comenzado a hacer un seguimiento de los cambios	Amazon EFS comenzó a realizar el seguimiento de los cambios en sus políticas administradas de AWS	7 de mayo de 2021

Uso de etiquetas con Amazon EFS

Puede utilizar etiquetas para controlar el acceso a los recursos de Amazon EFS y para implementar el control de acceso basado en atributos (ABAC). Para obtener más información, consulte:

- [Etiquetado de los recursos de Amazon EFS](#)
- [Controlar el acceso mediante etiquetas](#)
- [¿Qué es ABAC para AWS?](#) en la Guía del usuario de IAM

Note

La replicación de Amazon EFS no permite el uso de etiquetas para el control de acceso basado en atributos (ABAC).

Para aplicar etiquetas a los recursos de Amazon EFS durante la creación, los usuarios deben tener ciertos permisos AWS Identity and Access Management (de IAM).

Concesión de permisos para etiquetar recursos durante la creación

Las siguientes acciones de creación de Amazon EFS le permiten especificar etiquetas al crear el recurso.

- `CreateAccessPoint`
- `CreateFileSystem`

Para permitir a los usuarios etiquetar recursos al crear los recursos, deben tener permisos para utilizar la acción que crea los recursos, como `elasticfilesystem:CreateAccessPoint` o `elasticfilesystem:CreateFileSystem`. Si se especifican etiquetas en la acción de creación de recursos, AWS realiza una autorización adicional en la `elasticfilesystem:TagResource` acción para verificar que los usuarios tengan permisos para crear etiquetas. Por lo tanto, los usuarios también deben tener permisos explícitos para usar la acción `elasticfilesystem:TagResource`.

En la definición de la política de IAM de la acción `elasticfilesystem:TagResource`, utilice el elemento `Condition` con la clave de condición `elasticfilesystem:CreateAction` para otorgar permisos de etiquetado a la acción que crea el recurso.

Example política: permite agregar etiquetas a sistemas de archivos solo en el momento de su creación

La siguiente política de ejemplo permite a los usuarios crear etiquetas durante la creación. No se permite a los usuarios etiquetar ningún recurso (no pueden llamar directamente a la acción `elasticfilesystem:TagResource`).

```
{
  "Statement": [
    {
```

```
    "Effect": "Allow",
    "Action": [
      "elasticfilesystem:CreateFileSystem"
    ],
    "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "elasticfilesystem:TagResource"
    ],
    "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/*",
    "Condition": {
      "StringEquals": {
        "elasticfilesystem:CreateAction": "CreateFileSystem"
      }
    }
  }
]
```

Uso de etiquetas para controlar el acceso a los recursos de Amazon EFS

Para controlar el acceso a los recursos y las acciones de Amazon EFS, puede utilizar políticas de IAM basadas en etiquetas. Puede proporcionar este control de dos maneras:

- Puede controlar el acceso a los recursos de Amazon EFS de basado en etiquetas.
- Puede controlar las etiquetas que se pueden pasar en una condición de solicitud de IAM.

Para obtener información sobre cómo utilizar las etiquetas para controlar el acceso a AWS los recursos, consulte [Controlar el acceso mediante etiquetas](#) en la Guía del usuario de IAM.

Controlar el acceso mediante etiquetas

Para controlar qué acciones puede realizar un usuario o un rol en un recurso de Amazon EFS, puede usar etiquetas en el recurso. Por ejemplo, puede permitir o denegar operaciones de API específicas en un recurso del sistema de archivos en función del par clave-valor de la etiqueta del recurso.

Example política: cree un sistema de archivos solo cuando se utilice una etiqueta específica

La siguiente política de ejemplo permite al usuario crear un sistema de archivos solo cuando lo etiqueta con un par clave-valor de etiqueta específico, en este ejemplo, `key=Department,value=Finance`.

```
{
  "Effect": "Allow",
  "Action": [
    "elasticfilesystem:CreateFileSystem",
    "elasticfilesystem:TagResource"
  ],
  "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/*",
  "Condition": {
    "StringEquals": {
      "aws:RequestTag/Department": "Finance"
    }
  }
}
```

Example política: eliminar sistemas de archivos con etiquetas específicas

La siguiente política de ejemplo permite a un usuario eliminar únicamente los sistemas de archivos que estén etiquetados con `Department=Finance`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem>DeleteFileSystem"
      ],
      "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    }
  ]
}
```

Uso de roles vinculados a servicios para Amazon EFS

Amazon Elastic File System usa un [rol vinculado a un servicio AWS Identity and Access Management \(IAM\)](#). El rol vinculado a un servicio de Amazon EFS es un tipo único de rol de IAM que está vinculado directamente a Amazon EFS. El rol predefinido vinculado a un servicio de Amazon EFS incluye permisos que el servicio requiere para llamar a otros Servicios de AWS en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Amazon EFS porque ya no tendrá que agregar los permisos necesarios de forma manual. Amazon EFS define los permisos de su rol vinculado a un servicio y solo Amazon EFS puede asumir su rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar el rol vinculado a un servicio de Amazon EFS después de eliminar los sistemas de archivos de Amazon EFS. De esta forma, se protegen los recursos de Amazon EFS, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

El rol vinculado a servicios permite que todas las llamadas a la API puedan verse a través de AWS CloudTrail. Esta ayuda a monitorear y auditar los requisitos, ya que se puede hacer un seguimiento de todas las acciones que Amazon EFS lleva a cabo en su nombre. Para obtener más información, consulte [Entradas de registro para roles vinculados al servicio EFS](#).

Permisos de roles vinculados a servicios para Amazon EFS

Amazon EFS usa la función vinculada al servicio denominada `AWSServiceRoleForAmazonElasticFileSystem` para permitir que Amazon EFS llame y administre AWS recursos en nombre de sus sistemas de archivos de EFS.

El rol vinculado a servicios `AWSServiceRoleForAmazonElasticFileSystem` confía en los siguientes servicios para asumir el rol:

- `elasticfilesystem.amazonaws.com`

La política de permisos del rol permite que Amazon EFS realice las acciones incluidas en el JSON de definición de la política:

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



```

    "Effect": "Allow",
    "Action": [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:*:*:key/*"
},
{
    "Effect": "Allow",
    "Action": [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
    ],
    "Resource": [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
    ],
    "Resource": [
        "arn:aws:backup:*:*:backup-plan:*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ]
}

```

```

    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": [
          "backup.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": [
      "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
    ],
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "backup.amazonaws.com"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "elasticfilesystem:DescribeFileSystems",
      "elasticfilesystem:CreateReplicationConfiguration",
      "elasticfilesystem:DescribeReplicationConfigurations",
      "elasticfilesystem>DeleteReplicationConfiguration"
    ],
    "Resource": "*"
  }
]
}

```

Note

Debe configurar manualmente los permisos de IAM para AWS KMS crear un nuevo sistema de archivos de Amazon EFS que esté cifrado en reposo. Para obtener más información, consulte [Cifrado de datos en reposo](#).

Creación de un rol vinculado a un servicio para Amazon EFS

Debe configurar permisos para permitir que una entidad de IAM (como un usuario, grupo o rol) cree un rol vinculado a un servicio. Para ello, agregue el `iam:CreateServiceLinkedRole` permiso a una entidad de IAM, como se muestra en el siguiente ejemplo.

```
{
  "Action": "iam:CreateServiceLinkedRole",
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": [
        "elasticfilesystem.amazonaws.com"
      ]
    }
  }
}
```

Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

No necesita crear manualmente un rol vinculado a servicios. Al crear los objetivos de montaje o una configuración de replicación para el AWS Management Console sistema de archivos de EFS en la AWS API de, Amazon EFS crea automáticamente el rol vinculado a un servicio. AWS CLI

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear los objetivos de montaje o una configuración de replicación para el sistema de archivos de EFS, Amazon EFS crea de nuevo el rol vinculado a un servicio por el usuario

Edición de un rol vinculado a un servicio para Amazon EFS

Amazon EFS no permite editar el rol `AWSServiceRoleForAmazonElasticFileSystem` vinculado a un servicio. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante 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 un servicio para Amazon EFS

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

Note

Si el servicio Amazon EFS 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 Amazon EFS utilizados por `AWSServiceRoleForAmazonElasticFileSystem`

Complete los siguientes pasos para eliminar los recursos de Amazon EFS utilizados por `AWSServiceRoleForAmazonElasticFileSystem`. Para obtener información detallada sobre el procedimiento, consulte [Limpie los recursos y proteja su AWS cuenta](#).

1. En la instancia de Amazon EC2, desmonte el sistema de archivos de Amazon EFS.
2. Elimine el sistema de archivos de Amazon EFS.
3. Elimine el grupo de seguridad personalizado para el sistema de archivos.

Warning

Si utilizó el grupo de seguridad predeterminado para la nube privada virtual (VPC), no elimine ese grupo de seguridad.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a un servicio `AWSServiceRoleForAmazonElasticFileSystem`. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Solución de problemas de identidad y acceso de Amazon Elastic File System

Utilice la siguiente información para diagnosticar y solucionar los problemas habituales que pueden surgir cuando se trabaja con Amazon EFS e IAM.

Temas

- [No tengo autorización para realizar una acción en Amazon EFS](#)
- [No tengo autorización para realizar la operación `iam:PassRole`](#)
- [Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de Amazon EFS](#)

No tengo autorización para realizar una acción en Amazon EFS

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 `elasticfilesystem:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
elasticfilesystem: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 `elasticfilesystem:GetWidget`.

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.

No tengo autorización para realizar la operación `iam:PassRole`

Si recibe un error que indica que no tiene autorización para llevar a cabo la acción `iam:PassRole`, las políticas se deben actualizar para permitirle pasar un rol a Amazon EFS.

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 a servicios. 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 Amazon EFS. Sin embargo, la acción requiere que el servicio cuente con permisos que concede 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 Amazon EFS

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. 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 más información, consulte lo siguiente:

- Para saber si Amazon EFS admite estas características, consulte [Cómo funciona Amazon Elastic File System con IAM](#).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte [Cómo proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a los 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 federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(federación de identidades\)](#) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del Usuario de IAM.

Uso de IAM para controlar el acceso a los datos del sistema de archivos

Puede usar políticas de identidad de IAM y políticas de recursos para controlar el acceso de los clientes de NFS a los recursos de Amazon EFS de una manera escalable y optimizada para entornos de nube. Mediante IAM, puede permitir que los clientes realicen acciones específicas en un sistema de archivos, incluido el acceso de solo lectura, escritura y raíz. Un permiso de “permitir” para una acción, ya sea en una política de identidad de IAM o en una política de recursos del sistema de archivos, permite el acceso a esa acción. No es necesario conceder el permiso tanto en una política de identidad como en una política de recursos.

Los clientes de NFS pueden identificarse mediante un rol de IAM al conectarse a un sistema de archivos de EFS. Cuando un cliente se conecta a un sistema de archivos, Amazon EFS evalúa la política de recursos de IAM del sistema de archivos, conocida como política del sistema de archivos, junto con las políticas basadas en la identidad de IAM para determinar los permisos de acceso del sistema de archivos que se deben conceder.

Cuando utiliza la autorización de IAM para clientes de NFS, las conexiones de cliente y las decisiones de autorización de IAM se registran en AWS CloudTrail. Para obtener más información sobre cómo registrar las llamadas a la API de Amazon EFS CloudTrail, consulte [Registro de llamadas a la API de Amazon EFS con AWS CloudTrail](#).

Important

Debe utilizar el ayudante de montaje de EFS para montar sus sistemas de archivos de Amazon EFS con el fin de utilizar la autorización de IAM para controlar el acceso de los clientes. Para obtener más información, consulte [Montaje con autorización de IAM](#).

Política predeterminada del sistema de archivos de EFS

La política predeterminada del sistema de archivos de EFS no utiliza IAM para autenticar y otorga acceso completo a cualquier cliente anónimo que pueda conectarse al sistema de archivos mediante un destino de montaje. La política predeterminada se aplica siempre que no se aplique una política de sistema de archivos configurada por el usuario, incluso al crear el sistema de archivos. Siempre que la política del sistema de archivos predeterminada esté en vigor, una operación de API [DescribeFileSystemPolicy](#) devuelve una respuesta `PolicyNotFound`.

Acciones de EFS para clientes

Puede especificar las siguientes acciones para clientes que acceden a un sistema de archivos mediante una política de sistema de archivos.

Acción	Descripción
<code>elasticfilesystem:ClientMount</code>	Proporciona acceso de solo lectura a un sistema de archivos.
<code>elasticfilesystem:ClientWrite</code>	Proporciona permisos de escritura en un sistema de archivos.
<code>elasticfilesystem:ClientRootAccess</code>	Proporciona la capacidad de utilizar el usuario raíz al acceder a un sistema de archivos.

Claves de condición de EFS para clientes

Cómo expresar condiciones, se usan claves de condición predefinidas. Amazon EFS tiene las siguientes claves de condición predefinidas para los clientes de NFS. No se aplica ninguna otra clave de condición cuando se utilizan los controles de IAM para proteger el acceso a los sistemas de archivos EFS.

Clave de condición de EFS	Descripción	Operador
<code>aws:SecureTransport</code>	Utilice esta clave para exigir a los clientes que utilicen TLS	Booleano

Clave de condición de EFS	Descripción	Operador
	al conectarse a un sistema de archivos de EFS.	
<code>aws:SourceIp</code>	Dirección IP privada del cliente que accede a un sistema de archivos de EFS.	Cadena
<code>elasticfilesystem:AccessPointArn</code>	ARN del punto de acceso de EFS al que se está conectando el cliente.	Cadena
<code>elasticfilesystem:AccessedViaMountTarget</code>	Use esta clave para impedir el acceso a un sistema de archivos de EFS por parte de los clientes que no utilizan destinos de montaje del sistema de archivos.	Booleano

Ejemplos de política del sistema de archivos

Para ver ejemplos de políticas del sistema de archivos de Amazon EFS, consulte [Ejemplos de políticas basadas en recursos de Amazon Elastic File System](#).

Control del acceso de red a sistemas de archivos de Amazon EFS para clientes NFS

Puede controlar el acceso de los clientes de NFS a los sistemas de archivos de Amazon EFS mediante la seguridad de capa de red y las políticas de sistema de archivos EFS. Puede utilizar los mecanismos de seguridad de capa de red disponibles con Amazon EC2, como reglas de grupo de seguridad de VPC y ACL de red. También puede usar AWS IAM para controlar el acceso a NFS con una política de sistema de archivos EFS y políticas basadas en la identidad.

Temas

- [Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje](#)
- [Puertos de origen para trabajar con EFS](#)

- [Consideraciones de seguridad para el acceso a la red](#)
- [Uso de puntos de enlace de VPC de interfaz en Amazon EFS](#)

Uso de grupos de seguridad de VPC para instancias de Amazon EC2 y destinos de montaje

Cuando use Amazon EFS, especificará los grupos de seguridad de Amazon EC2 para sus instancias EC2 y los grupos de seguridad de los destinos de montaje de EFS asociados al sistema de archivos. Un grupo de seguridad actúa como firewall y las reglas que agregue definen el flujo de tráfico. En el ejercicio de introducción, creó un grupo de seguridad al lanzar la instancia EC2. A continuación, asoció otra con el destino de montaje de EFS (es decir, el grupo de seguridad predeterminado para la VPC predeterminada). Esta estrategia funciona en el ejercicio de introducción, pero en el caso de un sistema de producción, debe configurar los grupos de seguridad con permisos mínimos para su uso con EFS.

Puede autorizar el acceso de entrada y de salida a su sistema de archivos de EFS. Para ello, tiene que añadir reglas que permitan a la instancia EC2 conectarse al sistema de archivos de Amazon EFS a través del destino de montaje utilizando el puerto NFS (sistema de archivos de red). Siga estos pasos para crear y actualizar los grupos de seguridad.

Para crear grupos de seguridad para instancias EC2 y destinos de montaje

1. Cree dos grupos de seguridad en su VPC.

Para obtener instrucciones, consulte el procedimiento “Para crear un grupo de seguridad” en [Creación de un grupo de seguridad](#) en la Guía del usuario de Amazon VPC.

2. Abra la consola de administración de Amazon VPC en <https://console.aws.amazon.com/vpc/> y compruebe las reglas predeterminadas para estos grupos de seguridad. Ambos grupos de seguridad deben tener una única regla de salida que permita la salida de tráfico.

Para actualizar el acceso necesario para los grupos de seguridad

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. Añada una regla al grupo de seguridad de EC2 para permitir el acceso de entrada mediante SSH desde cualquier host. De forma opcional, puede restringir la dirección Source (Origen).

No es necesario añadir una regla de salida, ya que la regla de salida predeterminada permite que salga todo el tráfico. Si no dispone de esta regla de salida predeterminada, añada una regla de salida para abrir la conexión TCP en el puerto NFS, identificando el grupo de seguridad de destino de montaje como destino.

Para obtener instrucciones, consulte [Añadir y eliminar reglas](#) en la Guía del usuario de Amazon VPC.

3. Agregue reglas de entrada y salida para el destino de montaje.
 - Añada una regla de entrada para el grupo de seguridad de destino de montaje para permitir el acceso de entrada desde el grupo de seguridad de EC2. Identifique el grupo de seguridad de EC2 como el origen.
 - Agregue una regla de salida para abrir la conexión TCP en todos los puertos NFS. Identifique el grupo de seguridad de EC2 como el destino.

Para obtener instrucciones, consulte [Añadir y eliminar reglas](#) en la Guía del usuario de Amazon VPC.

4. Compruebe que ambos grupos de seguridad autorizan ahora el acceso de entrada y de salida.

Para obtener más información sobre los grupos de seguridad, consulte Grupos de [seguridad de Amazon EC2 para instancias de Linux](#).

Puertos de origen para trabajar con EFS

Para admitir un amplio conjunto de clientes NFS, Amazon EFS permite establecer conexiones desde cualquier puerto de origen. Si necesita que solo los usuarios con privilegios puedan acceder a Amazon EFS, le recomendamos que utilice la siguiente regla de firewall de cliente. Conéctese a su sistema de archivos mediante SSH y ejecute el siguiente comando:

```
iptables -I OUTPUT 1 -m owner --uid-owner 1-4294967294 -m tcp -p tcp --dport 2049 -j DROP
```

Este comando inserta una nueva regla al inicio de la cadena OUTPUT (-I OUTPUT 1). La regla impide que un proceso sin privilegios que no es del kernel (-m owner --uid-owner 1-4294967294) abra una conexión al puerto NFS (-m tcp -p tcp -dport 2049).

Consideraciones de seguridad para el acceso a la red

Un cliente NFS versión 4.1 (NFSv4.1) solo puede montar un sistema de archivos si puede realizar una conexión de red al puerto NFS (puerto 2049 de TCP) de uno de los destinos de montaje del sistema de archivos. Del mismo modo, un cliente NFSv4.1 solo puede confirmar un ID de usuario y grupo cuando accede a un sistema de archivos si puede realizar esta conexión de red.

La capacidad de realizar esta conexión de red se rige mediante una combinación de lo siguiente:

- Aislamiento de red proporcionado por el VPC de los destinos de montaje: los destinos de montaje del sistema de archivos no pueden tener direcciones IP públicas asociadas a los mismos. Los únicos destinos que pueden montar sistemas de archivos son los siguientes:
 - Instancias de Amazon EC2 en la VPC de Amazon local
 - Instancias EC2 en las VPC conectadas
 - Servidores locales conectados a una Amazon VPC AWS Direct Connect mediante AWS Virtual Private Network una (VPN)
- ACL de red de las subredes de VPC del cliente y destinos de montaje, para el acceso desde fuera de las subredes del destino de montaje: para montar el sistema de archivos, el cliente debe poder realizar una conexión TCP al puerto NFS de un destino de montaje (y recibir el tráfico de retorno).
- Reglas de los grupos de seguridad de la VPC del cliente y de los destinos de montaje, para todos los accesos: para que una instancia EC2 monte un sistema de archivos, deben estar en vigor las siguientes reglas de grupo de seguridad:
 - El sistema de archivos debe tener un destino de montaje cuya interfaz de red tiene un grupo de seguridad con una regla que permite las conexiones de entrada en el puerto NFS desde la instancia. Puede habilitar las conexiones entrantes ya sea por dirección IP (rango de CIDR) o grupo de seguridad. El origen de las reglas de grupo de seguridad en las interfaces de red del destino de montaje es un factor clave del control de acceso al sistema de archivos. Las reglas de entrada distintas a la del puerto de NFS y las reglas de salida, no los usan las interfaces de red para los destinos de montaje del sistema de archivos.
 - La instancia de montaje debe tener una interfaz de red con un grupo de seguridad que permita las conexiones de entrada en el puerto NFS en uno de los destinos de montaje del sistema de archivos. Puede habilitar las conexiones salientes ya sea por dirección IP (rango de CIDR) o grupo de seguridad.

Para obtener más información, consulte [Administrar destinos de montaje](#).

Uso de puntos de enlace de VPC de interfaz en Amazon EFS

Para establecer una conexión privada entre su nube privada virtual (VPC) y la API de Amazon EFS, puede crear un punto de conexión de la VPC de tipo interfaz. El punto de conexión proporciona conectividad segura a la API de Amazon EFS sin necesidad de una puerta de enlace de Internet, una instancia NAT o una conexión de red privada virtual (VPN). Para obtener más información, consulte [Puntos de enlace de la VPC de la interfaz](#) en la Guía del usuario de Amazon VPC.

Los puntos finales de la VPC de interfaz cuentan con una función que permite la comunicación privada entre AWS servicios mediante direcciones IP privadas. AWS PrivateLink Para usarlo AWS PrivateLink, cree un punto de enlace de VPC de interfaz para Amazon EFS en su VPC mediante la consola, la API o la CLI de Amazon VPC. Al hacerlo, se crea una interfaz de red elástica en la subred con una dirección IP privada que sirve solicitudes API de Amazon EFS. También puede acceder a un punto final de VPC desde entornos locales o desde otras VPC mediante AWS VPN el emparejamiento de VPC. AWS Direct Connect Para obtener más información, consulte [Cómo acceder a los servicios AWS PrivateLink](#) en la Guía del usuario de Amazon VPC.

Creación de un punto final de interfaz para Amazon EFS

Para crear un punto de conexión de VPC de interfaz para Amazon EFS, utilice una de las siguientes opciones:

- **com.amazonaws.*region*.elasticfilesystem**: crea un punto de conexión para las operaciones de la API de Amazon EFS.
- **com.amazonaws.*region*.elasticfilesystem-fips**: crea un punto de conexión para la API de Amazon EFS que cumple con el [Estándar federal de procesamiento de información \(FIPS\) 140-2](#).

Para obtener una lista completa de los puntos de conexión de Amazon EFS, consulte [Amazon Elastic File System](#) en la Referencia general de Amazon Web Services.

Para obtener más información sobre cómo crear un punto de enlace de interfaz, consulte [Creación de un punto de enlace de interfaz](#) en la Guía del usuario de Amazon VPC.

Creación de una política de puntos de conexión de VPC para Amazon EFS

Para controlar el acceso a la API de Amazon EFS, puede adjuntar una política AWS Identity and Access Management (IAM) a su punto de enlace de VPC. La política especifica lo siguiente:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte [Controlar el acceso a servicios con puntos de conexión de VPC](#) en la Guía del usuario de Amazon VPC.

En el ejemplo siguiente se muestra una política de punto de enlace de la VPC que deniega a todos los usuarios el permiso para crear un sistema de archivos EFS a través del punto de enlace. La política de ejemplo también concede permiso a todos los usuarios para realizar todas las demás acciones.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "elasticfilesystem:CreateFileSystem",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

Para obtener más información, consulte [Uso de políticas de punto de conexión de la VPC](#) en la Guía del usuario de Amazon VPC.

Trabajar con usuarios, grupos y permisos a nivel del sistema de archivos de red (NFS)

Después de crear un sistema de archivos, de forma predeterminada, solo el usuario raíz (UID 0) dispone de permisos de lectura, escritura y ejecución. Para que otros usuarios modifiquen el sistema de archivos, el usuario raíz debe concederles acceso de forma explícita. Puede utilizar puntos de

acceso para automatizar la creación de directorios desde los que un usuario que no sea raíz puede escribir. Para obtener más información, consulte [Trabajo con puntos de acceso de Amazon EFS](#).

Los objetos de sistema de archivos de Amazon EFS tienen un modo de estilo Unix asociado a ellos. Este valor de modo define los permisos para realizar acciones en ese objeto. Los usuarios familiarizados con los sistemas de estilo UNIX pueden comprender fácilmente cómo se comporta Amazon EFS con respecto a estos permisos.

Además, en los sistemas de estilo Unix, los usuarios y los grupos se asignan a identificadores numéricos, que Amazon EFS utiliza para representar la propiedad del archivo. En el caso de Amazon EFS, los objetos del sistema de archivos (es decir, archivos, directorios, etc.) pertenecen a un único propietario y a un único grupo. Amazon EFS usa estos ID numéricos asignados para comprobar los permisos cuando un usuario intenta acceder a un objeto del sistema de archivos.

Note

El protocolo NFS admite un máximo de 16 ID de grupo (GID) por usuario y cualquier GID adicional se trunca a partir de las solicitudes de los clientes de NFS. Para obtener más información, consulte [Acceso denegado a los archivos permitidos en el sistema de archivos NFS](#).

A continuación, encontrará ejemplos de permisos y un debate sobre consideraciones de permisos de NFS en Amazon EFS.

Temas

- [Permisos de archivos y directorios](#)
- [Ejemplo de permisos y casos de uso del sistema de archivos de Amazon EFS](#)
- [Permisos de ID de usuario y grupo para los archivos y directorios de un sistema de archivos](#)
- [Sin agrupación de raíz](#)
- [Almacenamiento en caché de permisos](#)
- [Cambio de propiedad de objeto del sistema de archivos](#)
- [Puntos de acceso de EFS](#)

Permisos de archivos y directorios

Los archivos y directorios del sistema de archivos de EFS admiten los permisos de lectura, escritura y ejecución estándar de tipo Unix basados en el ID de usuario y de grupo certificado al montar el cliente NFSv4.1, a menos que se anulen mediante un punto de acceso de EFS. Para obtener más información, consulte [Trabajar con usuarios, grupos y permisos a nivel del sistema de archivos de red \(NFS\)](#).

Note

Por defecto, esta capa de control de acceso depende de la confianza en el cliente NFSv4.1 en su aserción del ID de grupo y usuario. Puede usar políticas basadas en recursos AWS Identity and Access Management (IAM) y políticas de identidad para autorizar a los clientes NFS y proporcionar permisos de solo lectura, escritura y acceso root. Puede utilizar puntos de acceso EFS para reemplazar la información de identidad de usuario y grupo del sistema operativo proporcionada por el cliente NFS. Para obtener más información, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#) y [Crear puntos de acceso](#).

Como ejemplo de permisos para leer, escribir y ejecutar archivos y directorios, Alice podría tener permisos para leer y escribir en los archivos que desea en su directorio personal en un sistema de archivos, `/alice`. Sin embargo, en este ejemplo Alice no tiene permiso para leer o escribir en ningún archivo en el directorio personal de Mark en el mismo sistema de archivos, `/mark`. Tanto Alice como Mark tienen permiso para leer, pero no para escribir archivos en el directorio compartido `/share`.

Ejemplo de permisos y casos de uso del sistema de archivos de Amazon EFS

Después de crear un sistema de archivos de Amazon EFS y destinos de montaje para el sistema de archivos en la VPC, puede montar el sistema de archivos remoto localmente en su instancia de Amazon EC2. El comando `mount` puede montar cualquier directorio en el sistema de archivos. No obstante, la primera vez que cree el sistema de archivos, solo hay un directorio raíz en `/`. El usuario raíz y el grupo raíz son propietarios del directorio montado.

El siguiente comando `mount` monta el directorio raíz de un sistema de archivos de Amazon EFS, identificado por el nombre de DNS del sistema de archivos, en el directorio local `/efs-mount-point`.


```
sudo mount -t nfs -o
nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport file-
system-id.efs.aws-region.amazonaws.com:/ efs-mount-point
```

El modo de permisos inicial permite:

- Permisos read-write-execute para el propietario raíz
- Permisos read-execute para el grupo raíz
- Permisos read-execute para otras personas

Solo el usuario raíz puede modificar este directorio. El usuario raíz también puede conceder a otros usuarios permisos para escribir en este directorio, por ejemplo:

- Crear subdirectorios que se pueden escribir por usuario. Para step-by-step obtener instrucciones, consulte [Tutorial: Crear subdirectorios que se pueden escribir por usuario y configurar la opción de volver a montar automáticamente al reiniciar](#).
- Permitir a los usuarios escribir en la raíz del sistema de archivos de Amazon EFS Un usuario con privilegios raíz puede conceder a otros usuarios acceso al sistema de archivos.
 - Para cambiar la propiedad del sistema de archivos de Amazon EFS a un usuario y grupo no-raíz, utilice lo siguiente:

```
$ sudo chown user:group /EFSroot
```

- Para cambiar los permisos del sistema de archivos a otros más permisivos, utilice lo siguiente:

```
$ sudo chmod 777 /EFSroot
```

Este comando otorga read-write-execute privilegios a todos los usuarios de todas las instancias EC2 que tienen el sistema de archivos montado.

Permisos de ID de usuario y grupo para los archivos y directorios de un sistema de archivos

Los archivos y directorios del sistema de archivos de Amazon EFS admiten los permisos de lectura, escritura y ejecución estándar de tipo Unix basados en el ID de usuario y el ID de grupo. Cuando un cliente NFS monta un sistema de archivos EFS sin utilizar un punto de acceso, el ID de usuario

y el ID de grupo proporcionados por el cliente son de confianza. Los puntos de acceso EFS se pueden utilizar para anular el ID de usuario y los ID de grupo utilizados por el cliente NFS. Cuando los usuarios intentan acceder a los archivos y directorios, Amazon EFS comprueba su ID de usuario e ID de grupo para comprobar si el usuario tiene permiso para acceder a los objetos. Amazon EFS también utiliza estos ID para indicar el propietario y el propietario de grupo para nuevos archivos y directorios que crea el usuario. Amazon EFS no examina los nombres de usuario o de grupo, solo utiliza identificadores numéricos.

Note

Al crear un usuario en una instancia EC2, puede asignar cualquier ID de usuario (UID) e ID de grupo (GID) numéricos al usuario. Los ID numéricos de usuario se establecen en el archivo `/etc/passwd` en sistemas Linux. Los ID de grupo numérico se encuentran en el archivo `/etc/group`. Estos archivos definen los mapeos entre nombres e ID. Fuera de la instancia de EC2, Amazon EFS no realiza ninguna autenticación de estos identificadores, incluido el ID raíz de 0.

Si un usuario accede a un sistema de archivos de Amazon EFS desde dos instancias EC2 diferentes, en función de si el UID del usuario es el mismo o diferente en dichas instancias, verá distinto comportamiento como se indica:

- Si los ID de usuario son los mismos en ambas instancias EC2, Amazon EFS considera que indican el mismo usuario, independientemente de la instancia EC2 que utilizan. La experiencia del usuario al acceder al sistema de archivos es la misma desde ambas instancias EC2.
- Si los ID de usuario no son iguales en ambas instancias EC2, Amazon EFS considera que los usuarios son usuarios diferentes. La experiencia del usuario no es la misma al acceder al sistema de archivos de Amazon EFS desde las dos instancias EC2 diferentes.
- Si dos usuarios distintos en distintas instancias EC2 comparten un ID, Amazon EFS los considera que son el mismo usuario.

Podría plantearse administrar los mapeos de ID de usuario entre instancias EC2 de forma coherente. Los usuarios pueden comprobar su ID numérico utilizando el comando `id`.

```
$ id
uid=502(joe) gid=502(joe) groups=502(joe)
```

Desactivar el mapeador de ID

Las utilidades de NFS en el sistema operativo incluyen un demonio denominado mapeador de ID que administra el mapeo entre nombres de usuario e ID. En Amazon Linux, el demonio se denomina `rpc.idmapd` y en Ubuntu se denomina `idmapd`. Traduce los ID de usuarios y grupos en nombres y viceversa. Sin embargo, Amazon EFS solo trata con ID numéricos. Le recomendamos que desactive este proceso en sus instancias EC2. En Amazon Linux, el mapeador de ID suele estar deshabilitado: si lo está, no lo habilite. Para desactivar el mapeador de ID, utilice los comandos que se muestran a continuación.

```
$ service rpcidmapd status
$ sudo service rpcidmapd stop
```

Sin agrupación de raíz

De forma predeterminada, la compresión de raíces está deshabilitada en los sistemas de archivos de EFS. Amazon EFS se comporta como un servidor NFS de Linux con `no_root_squash`. Si el ID de un usuario o grupo es 0, Amazon EFS trata a dicho usuario como usuario `root` e ignora las comprobaciones de permisos (permitiendo el acceso y la modificación de todos los objetos del sistema de archivos). El bloqueo de raíces se puede habilitar en una conexión de cliente cuando la política de identidad o recursos AWS Identity and Access Management (AWS IAM) no permite el acceso a la acción. `ClientRootAccess` Cuando la agrupación de raíz está habilitada, el usuario raíz se convierte a un usuario con permisos limitados en el servidor de NFS.

Para obtener más información, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#) y [Tutorial: Habilite la eliminación raíz mediante la autorización de IAM para clientes NFS](#).

Almacenamiento en caché de permisos

Amazon EFS almacena en caché los permisos de archivos durante un breve periodo de tiempo. Como resultado, es posible que haya un breve periodo en el que un usuario cuyo acceso se revocó recientemente, pueda seguir accediendo a ese objeto.

Cambio de propiedad de objeto del sistema de archivos

Amazon EFS aplica el atributo `chown_restricted` de POSIX. Esto significa que solo el usuario raíz puede cambiar el propietario de un objeto del sistema de archivos. El usuario raíz o propietario puede cambiar el grupo propietario de un objeto del sistema de archivos. Sin embargo, a menos que el usuario sea raíz, el grupo solo se puede cambiar a uno del que sea miembro el usuario propietario.

Puntos de acceso de EFS

Un punto de acceso aplica una ruta de usuario, grupo y sistema de archivos del sistema operativo a cualquier solicitud del sistema de archivos realizada mediante el punto de acceso. El usuario y el grupo del sistema operativo del punto de acceso anulan cualquier información de identidad proporcionada por el cliente NFS. La ruta del sistema de archivos se expone al cliente como directorio raíz del punto de acceso. Este enfoque garantiza que cada aplicación siempre utilice la identidad correcta del sistema operativo y el directorio correcto al acceder a conjuntos de datos basados en archivos compartidos. Las aplicaciones que utilizan el punto de acceso solo pueden acceder a los datos en su propio directorio e inferiores. Para obtener más información acerca de los puntos de acceso, consulte [Trabajo con puntos de acceso de Amazon EFS](#).

Trabajo con puntos de acceso de Amazon EFS

Los puntos de acceso de Amazon EFS son puntos de entrada específicos que la aplicación utiliza para acceder a un sistema de archivos de EFS y que facilitan la administración del acceso de las aplicaciones a conjuntos de datos compartidos. Los puntos de acceso pueden imponer una identidad de usuario, incluidos los grupos POSIX del usuario, para todas las solicitudes del sistema de archivos que se realizan a través del punto de acceso. Los puntos de acceso también pueden imponer un directorio raíz diferente para el sistema de archivos, de modo que los clientes solo puedan acceder a los datos del directorio especificado o de sus subdirectorios.

Puede usar políticas AWS Identity and Access Management (de IAM) para imponer que aplicaciones específicas usen un punto de acceso específico. Al combinar políticas de IAM con puntos de acceso, puede proporcionar fácilmente acceso seguro a conjuntos de datos específicos para sus aplicaciones.

Note

Debe crear al menos un destino de montaje en el sistema de archivos de EFS para utilizar los puntos de acceso.

Para obtener más información sobre cómo crear un punto de acceso, consulte [Crear puntos de acceso](#).

Temas

- [Creación de un punto de acceso](#)

- [Montaje de un sistema de archivos mediante un punto de acceso](#)
- [Aplicación de una identidad de usuario mediante un punto de acceso](#)
- [Aplicación de un directorio raíz con un punto de acceso](#)
- [Uso de puntos de acceso en políticas de IAM](#)

Creación de un punto de acceso

Puede crear puntos de acceso para un sistema de archivos Amazon EFS existente mediante la AWS Management Console API, AWS Command Line Interface (AWS CLI) y EFS. Un sistema de archivos puede tener un [máximo de 1000 puntos de acceso](#). No puede modificar un punto de acceso una vez creado.

Para conocer step-by-step los procedimientos para crear un punto de acceso, consulte [Crear puntos de acceso](#).

Montaje de un sistema de archivos mediante un punto de acceso

Utilice el ayudante de montaje EFS al montar un sistema de archivos mediante un punto de acceso. En el comando mount, incluya el ID del sistema de archivos, el ID del punto de acceso y la opción de montaje `tls`, como se muestra en el siguiente ejemplo.

```
$ mount -t efs -o tls,iam,accesspoint=fsap-abcdef0123456789a fs-  
abc0123def456789a: /localmountpoint
```

Para obtener más información sobre el montaje de sistemas de archivos mediante un punto de acceso, consulte [Montaje con puntos de acceso de EFS](#).

Aplicación de una identidad de usuario mediante un punto de acceso

Puede utilizar un punto de acceso para aplicar información de usuario y grupo para todas las solicitudes del sistema de archivos realizadas a través del punto de acceso. Para habilitar esta característica, debe especificar la identidad del sistema operativo que se aplicará al crear el punto de acceso.

Como parte de esto, proporciona lo siguiente:

- ID de usuario: el ID de usuario POSIX numérico para el usuario.

- ID de grupo: el ID de grupo POSIX numérico para el usuario.
- ID de grupos secundarios: una lista opcional de identificadores de grupos secundarios.

Cuando la aplicación de usuario está habilitada, Amazon EFS reemplaza los ID de usuario y grupo del cliente NFS por la identidad configurada en el punto de acceso para todas las operaciones del sistema de archivos. El cumplimiento de los usuarios también hace lo siguiente:

- El propietario y el grupo de los nuevos archivos y directorios se establecen en el ID de usuario y el ID de grupo del punto de acceso.
- EFS tiene en cuenta el ID de usuario, el ID de grupo y los ID de grupo secundario del punto de acceso al evaluar los permisos del sistema de archivos. EFS ignora los ID del cliente NFS.

Important

La aplicación de una identidad de usuario está sujeta al permiso `ClientRootAccess` de IAM.

Por ejemplo, en algunos casos puede configurar el ID de usuario del punto de acceso, el ID de grupo o ambos para que sean raíz (es decir, establecer el UID, el GID o ambos en 0). En tales casos, debe conceder el permiso de IAM `ClientRootAccess` al cliente NFS.

Aplicación de un directorio raíz con un punto de acceso

Puede utilizar un punto de acceso para anular el directorio raíz de un sistema de archivos. Cuando se aplica un directorio raíz, el cliente NFS que utiliza el punto de acceso utiliza el directorio raíz configurado en el punto de acceso en lugar del directorio raíz del sistema de archivos.

Para habilitar esta entidad, defina el atributo `Path` del punto de acceso al crear un punto de acceso. El atributo `Path` es la ruta completa del directorio raíz del sistema de archivos para todas las solicitudes del sistema de archivos realizadas a través de este punto de acceso. La ruta de acceso completa no puede superar los 100 caracteres de longitud. Puede incluir hasta cuatro subdirectorios.

Cuando se especifica un directorio raíz en un punto de acceso, se convierte en el directorio raíz del sistema de archivos para el cliente NFS que monta el punto de acceso. Por ejemplo, supongamos que el directorio raíz de su punto de acceso sea `/data`. En este caso, el montaje `fs-12345678: /` utilizando el punto de acceso tiene el mismo efecto que el montaje `fs-12345678: /data` sin usar el punto de acceso.

Al especificar un directorio raíz en el punto de acceso, asegúrese de que los permisos de directorio estén configurados para permitir que el usuario del punto de acceso monte correctamente el sistema de archivos. Concretamente, asegúrese de que el bit de ejecución esté configurado para el grupo o usuario del punto de acceso, o para todos los usuarios. Por ejemplo, si el permiso del directorio tiene el valor 755, el propietario del directorio puede enumerar, crear y montar archivos, y el resto de los usuarios pueden enumerar y montar archivos.

Creación del directorio raíz para un punto de acceso

Si no existe una ruta al directorio raíz para un punto de acceso en el sistema de archivos, Amazon EFS crea automáticamente ese directorio raíz con la propiedad y los permisos especificados. Amazon EFS no creará el directorio raíz si no especifica la propiedad y los permisos del directorio en el momento de la creación. Este enfoque permite aprovisionar el acceso al sistema de archivos para un usuario o aplicación específicos sin montar el sistema de archivos desde un host Linux. Para crear un directorio raíz, puede configurar la propiedad y el permiso del directorio raíz utilizando los siguientes atributos al crear un punto de acceso:

- `OwnerUid`: el ID de usuario POSIX numérico que se utilizará como propietario del directorio raíz.
- `OwnerGid`: el ID de grupo POSIX numérico que se utilizará como propietario del grupo del directorio raíz.
- `Permisos`: el modo Unix del directorio. Una configuración común es 755. Asegúrese de que el bit de ejecución esté configurado para el usuario del punto de acceso para que pueda montar archivos. Esta configuración da al propietario del directorio permiso para introducir, enumerar y escribir nuevos archivos en el directorio. Da permiso a todos los demás usuarios para introducir y enumerar archivos. Para obtener más información sobre cómo trabajar con los modos de archivo y directorio Unix, consulte [Trabajar con usuarios, grupos y permisos a nivel del sistema de archivos de red \(NFS\)](#).

Amazon EFS crea un directorio raíz de puntos de acceso solo si se especifican el `OwnUid` `OwnGid` y los permisos para el directorio. Si no proporciona dicha información, Amazon EFS no creará el directorio raíz. Si el directorio raíz no existe, los intentos de montaje utilizando el punto de acceso fallarán.

Al montar un sistema de archivos con un punto de acceso, se crea el directorio raíz del punto de acceso si el directorio aún no existe, siempre que el directorio raíz `OwnerUid` y los permisos se hayan especificado al crear el punto de acceso. Si el directorio raíz del punto de acceso ya existe antes de la hora de montaje, el punto de acceso no sobrescribirá los permisos existentes. Si elimina el

directorio raíz, EFS lo vuelve a crear la próxima vez que se monte el sistema de archivos utilizando el punto de acceso.

Note

Si no especifica la propiedad y los permisos de un directorio raíz de punto de acceso, Amazon EFS no creará el directorio raíz. Todos los intentos de montaje del punto de acceso fallarán.

Modelo de seguridad para directorios raíz de punto de acceso

Cuando una anulación de directorio raíz está en vigor, Amazon EFS se comporta como un servidor Linux NFS con la opción `no_subtree_check` habilitada.

En el protocolo NFS, los servidores generan identificadores de archivo que los clientes utilizan como referencias únicas al acceder a los archivos. EFS genera de forma segura identificadores de archivos impredecibles y específicos de un sistema de archivos EFS. Cuando se ha establecido una sustitución de directorio raíz, EFS no revela los identificadores de archivo para los archivos fuera del directorio raíz especificado. Sin embargo, en algunos casos, un usuario puede obtener un identificador de archivo para un archivo fuera de su punto de acceso mediante un out-of-band mecanismo. Por ejemplo, podrían hacerlo si tienen acceso a un segundo punto de acceso. Si lo hacen, pueden llevar a cabo operaciones de lectura y escritura en el archivo.

Los permisos de acceso y propiedad de archivos siempre se aplican, para acceder a archivos dentro y fuera del directorio raíz del punto de acceso de un usuario.

Uso de puntos de acceso en políticas de IAM

Puede utilizar una política de IAM para exigir que un cliente NFS específico, identificado por su rol de IAM, solo pueda acceder a un punto de acceso específico. Para ello, utilice la clave de condición de IAM `elasticfilesystem:AccessPointArn`. `AccessPointArn` es el nombre de recurso de Amazon (ARN) del punto de acceso con el que está montado el sistema de archivos.

A continuación se muestra un ejemplo de una política del sistema de archivos que permite que el rol de IAM `app1` tenga acceso al sistema de archivos mediante el punto de acceso `fsap-01234567`. La política también permite a `app2` utilizar el sistema de archivos utilizando el punto de acceso `fsap-89abcdef`.

```
{
```



```
"Version": "2012-10-17",
"Id": "MyFileSystemPolicy",
"Statement": [
  {
    "Sid": "App1Access",
    "Effect": "Allow",
    "Principal": { "AWS": "arn:aws:iam::111122223333:role/app1" },
    "Action": [
      "elasticfilesystem:ClientMount",
      "elasticfilesystem:ClientWrite"
    ],
    "Condition": {
      "StringEquals": {
        "elasticfilesystem:AccessPointArn" : "arn:aws:elasticfilesystem:us-
east-1:222233334444:access-point/fsap-01234567"
      }
    }
  },
  {
    "Sid": "App2Access",
    "Effect": "Allow",
    "Principal": { "AWS": "arn:aws:iam::111122223333:role/app2" },
    "Action": [
      "elasticfilesystem:ClientMount",
      "elasticfilesystem:ClientWrite"
    ],
    "Condition": {
      "StringEquals": {
        "elasticfilesystem:AccessPointArn" : "arn:aws:elasticfilesystem:us-
east-1:222233334444:access-point/fsap-89abcdef"
      }
    }
  }
]
```

Bloqueo del acceso público a los sistemas de archivos de Amazon EFS

La característica de acceso público de bloqueo de Amazon EFS proporciona ajustes que le ayudarán a administrar el acceso público a los sistemas de archivos de Amazon EFS. De forma

predeterminada, los sistemas de archivos Amazon EFS nuevos no permiten el acceso público. Sin embargo, puede modificar las políticas del sistema de archivos para permitirlo.

Important

Habilitar el acceso público en bloque ayuda a proteger sus recursos al impedir que el acceso público se otorgue a través de las políticas de recursos que se adjuntan directamente al sistema de archivos. Además de habilitar Bloqueo de acceso público, examine detenidamente las siguientes políticas para confirmar que no conceden acceso público:

- Políticas basadas en la identidad asociadas a las entidades AWS principales asociadas (por ejemplo, las funciones de IAM)
- Políticas basadas en recursos asociadas a los AWS recursos asociados (por ejemplo, claves (KMS))AWS Key Management Service

Temas

- [Bloqueo de acceso público con AWS Transfer Family](#)
- [Qué significa "pública"](#)

Bloqueo de acceso público con AWS Transfer Family

Al utilizar Amazon EFS con AWS Transfer Family, las solicitudes de acceso al sistema de archivos recibidas desde un servidor Transfer Family que sea propiedad de una cuenta diferente a la del sistema de archivos se bloquean si el sistema de archivos permite el acceso público. Amazon EFS evalúa las políticas de IAM del sistema de archivos y, si la política es pública, bloquea la solicitud. Para permitir el AWS Transfer Family acceso a su sistema de archivos, actualice la política del sistema de archivos para que no se considere público.

Note

El uso de Transfer Family con Amazon Cuenta de AWS EFS está desactivado de forma predeterminada para los sistemas de archivos EFS con políticas que permiten el acceso público que se crearon antes del 6 de enero de 2021. Para habilitar el uso de Transfer Family para acceder a su sistema de archivos, póngase en contacto con AWS Support.

Qué significa "pública"

Al evaluar si un sistema de archivos permite el acceso público, Amazon EFS asume que la política del sistema de archivos es pública. A continuación, evalúa la política del sistema de archivos para determinar si califica como no pública. Para que se considere no pública, una política de sistemas de archivos debe conceder acceso solo a valores fijos (valores que no contienen un comodín) de uno o más de los siguientes:

- Un conjunto de Classless Inter-Domain Routings (CIDR), mediante `aws:SourceIp`. Para obtener más información sobre CIDR, consulte [RFC 4632](#) en la página web de RFC Editor.
- Un AWS director, un usuario, un rol o un director de servicio (por ejemplo, `aws:PrincipalOrgID`)
- `aws:SourceArn`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:SourceOwner`
- `aws:SourceAccount`
- `elasticfilesystem:AccessedViaMountTarget`
- `aws:userid`, outside the pattern `"AROLEID:*"`

En virtud de estas reglas, la siguiente política de ejemplo se considera pública.

```
{
  "Version": "2012-10-17",
  "Id": "efs-policy-wizard-15ad9567-2546-4bbb-8168-5541b6fc0e55",
  "Statement": [
    {
      "Sid": "efs-statement-14a7191c-9401-40e7-a388-6af6cfb7dd9c",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientRootAccess"
      ]
    }
  ]
}
```

```
}
```

Puede hacer que esta política del sistema de archivos no sea pública mediante la clave de condición de EFS `elasticfilesystem:AccessedViaMountTarget` establecida como `"true"`. Se puede utilizar `elasticfilesystem:AccessedViaMountTarget` para permitir las acciones de EFS especificadas a los clientes que accedan al sistema de archivos de EFS mediante un destino de montaje del sistema de archivos. La siguiente política no pública utiliza la clave de condición `elasticfilesystem:AccessedViaMountTarget` establecida como `"true"`.

```
{
  "Version": "2012-10-17",
  "Id": "efs-policy-wizard-15ad9567-2546-4bbb-8168-5541b6fc0e55",
  "Statement": [
    {
      "Sid": "efs-statement-14a7191c-9401-40e7-a388-6af6cfb7dd9c",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientRootAccess"
      ],
      "Condition": {
        "Bool": {
          "elasticfilesystem:AccessedViaMountTarget": "true"
        }
      }
    }
  ]
}
```

Para obtener más información sobre las claves de condición de Amazon EFS, consulte [Claves de condición de EFS para clientes](#). Para obtener más información sobre la creación de políticas de sistemas de archivos, consulte [Creación de políticas de sistema de archivos](#).

Validación de conformidad para Amazon EFS


Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento](#)

[Servicios de AWS](#) de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de [arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

 Note

No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la [Referencia de servicios compatibles con HIPAA](#).

- [AWS Recursos de](#) cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).

- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Amazon EFS

La infraestructura AWS global se basa en Regiones de AWS las zonas de disponibilidad (AZ). Regiones de AWS proporcionan múltiples zonas de acceso aisladas y separadas físicamente, que están conectadas a redes de baja latencia, alto rendimiento y alta redundancia. Con las AZ, puede diseñar y operar aplicaciones y bases de datos que conmuten automáticamente por error entre zonas sin interrupciones. Las AZ tienen mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Los sistemas de archivos de Amazon EFS son resilientes a fallos de una o zonas de disponibilidad dentro de una Región de AWS. Los propios destinos de montaje están diseñados para ofrecer alta disponibilidad. Al diseñar para una alta disponibilidad y la conmutación por error a otras zonas de disponibilidad, tenga en cuenta que, si bien las direcciones IP y el DNS de los destinos de montaje de cada zona de disponibilidad son estáticos, son componentes redundantes respaldados por varios recursos. Para obtener más información, consulte [Cómo funciona Amazon EFS con Amazon EC2](#).

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura [AWS global](#).

Aislamiento de red para Amazon EFS

Como servicio gestionado, Amazon Elastic File System está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a Amazon EFS 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.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Estas API son llamables desde cualquier ubicación de red, pero Amazon EFS admite políticas de acceso basadas en recursos, que pueden incluir restricciones en función de la dirección IP de origen. También puede utilizar políticas de Amazon EFS para controlar el acceso desde puntos de conexión específicos de Amazon Virtual Private Cloud (Amazon VPC) o VPC específicas. De hecho, esto aísla el acceso a la red a un recurso de Amazon EFS determinado únicamente de la VPC específica de la red. AWS

Cuotas de Amazon EFS

A continuación, puede obtener información acerca de las cuotas a la hora de trabajar con Amazon EFS.

Temas

- [Cuotas de Amazon EFS que puede incrementar](#)
- [Cuotas de recursos de Amazon EFS que no puede cambiar.](#)
- [Cuotas para clientes NFS](#)
- [Cuotas para sistemas de archivos de Amazon EFS](#)
- [Funciones de NFSv4.0 y 4.1 no compatibles](#)
- [Consideraciones adicionales](#)
- [Solución de errores de operación de archivos](#)

Cuotas de Amazon EFS que puede incrementar

Service Quotas es un AWS servicio que le ayuda a administrar sus cuotas o límites desde un solo lugar. En la [consola de Service Quotas](#), puede ver todos los valores límite de Amazon EFS y solicitar un aumento de cuota para el número de sistemas de archivos EFS en una Región de AWS.

También puede solicitar un aumento de las siguientes cuotas Amazon EFS poniéndose en contacto con el servicio técnico de AWS . Para obtener más información, consulte [Solicitud de aumento de cuota](#). El equipo de servicio técnico de Amazon EFS revisa cada solicitud individualmente.

- Número de sistemas de archivos para cada cuenta de cliente.
- Cuota de rendimiento elástica por sistema de archivos regional para todos los clientes conectados en un Región de AWS.
- Cuota de rendimiento aprovisionada por sistema de archivos regional para todos los clientes conectados en un. Región de AWS

En la siguiente tabla se muestran las cuotas para cada recurso que puede cambiar.

Número de sistemas de archivos por cuenta de cliente

Recurso	Cuota predeterminada
Número de sistemas de archivos para cada cuenta de cliente en un Región de AWS	1 000

Sistemas de archivos regionales: rendimiento total predeterminado de Elastic por sistema de archivos para todos los clientes conectados en cada uno Región de AWS

Región de AWS	Rendimiento de lectura máximo	Rendimiento máximo de escritura (rendimiento medido)
Región del Este de EE. UU. (Ohio)	20 gibibytes por segundo () GiBps	5 GiBps
Región del Este de EE. UU (Norte de Virginia)		
Región del oeste de EE. UU (Oregón)		
Asia Pacífico (Tokio)		
Región de Europa (Irlanda)		
Todos los demás Regiones de AWS	3 GiBps	1 GiBps

Sistemas de archivos regionales: rendimiento total provisionado predeterminado por sistema de archivos para todos los clientes conectados en cada uno Región de AWS

Región de AWS	Rendimiento de lectura máximo	Rendimiento máximo de escritura (rendimiento medido)
Región del Este de EE. UU. (Ohio)	10 GiBps	3.33 GiBps

Región de AWS	Rendimiento de lectura máximo	Rendimiento máximo de escritura (rendimiento medido)
Región del Este de EE. UU (Norte de Virginia)		
Región del oeste de EE. UU (Oregón)		
Región de Europa (Irlanda)		
Todos los demás Regiones de AWS	3 GiBps	1 GiBps

Solicitud de aumento de cuota

Para solicitar un aumento de estas cuotas AWS Support, siga los siguientes pasos. El equipo de Amazon EFS revisa cada solicitud de aumento de cuota.

Para solicitar un aumento de cuota mediante AWS Support

1. Abra la página del [Centro de AWS Support](#) e inicie sesión si es necesario. A continuación, seleccione Crear caso.
2. En Crear caso, seleccione Aumento del límite de servicio.
3. En Tipo de límite, seleccione el tipo de límite que desea aumentar. Rellene los campos necesarios del formulario y, a continuación, seleccione el método de contacto que prefiera.

Cuotas de recursos de Amazon EFS que no puede cambiar.

Las cuotas de varios recursos de Amazon EFS que no se pueden cambiar, entre ellos:

- Cuotas para los recursos generales, como la cantidad de puntos de acceso o conexiones para cada sistema de archivos.
- Cuotas de rendimiento elásticas y aprovisionadas por sistema de archivos de una zona para todos los clientes conectados en un. Región de AWS

- Ampliar las cuotas de rendimiento por sistema de archivos regional o de una zona para todos los clientes conectados en un. Región de AWS

En las siguientes tablas se enumeran las cuotas de recursos generales, los límites de rendimiento del sistema de archivos de una zona y los límites de rendimiento de fragmentación que no se pueden cambiar.

Cuotas de recursos generales que no se pueden cambiar

Recurso	Cuota
Número de puntos de acceso para cada sistema de archivos	1 000
Número de conexiones para cada sistema de archivos	25 000
Número de destinos de montaje para cada sistema de archivos en una zona de disponibilidad	1
Número de destinos de montaje para cada nube privada virtual (VPC)	1.400
Número de grupos de seguridad para cada destino de montaje	5
Número de etiquetas para cada sistema de archivos	50
Número de VPC para cada sistema de archivos	1

Note

Los clientes también pueden conectarse a destinos de montaje que estén en una cuenta o VPC diferente a la del sistema de archivos. Para obtener más información, consulte [Montaje de sistemas de archivos EFS desde otro Cuenta de AWS o desde una VPC](#).

Sistemas de archivos de una zona: rendimiento total predeterminado de Elastic y Provisioned por sistema de archivos para todos los clientes conectados en cada uno Región de AWS

Región de AWS	Rendimiento de lectura máximo	Rendimiento máximo de escritura (rendimiento medido)
Todos Regiones de AWS	3 GiBps	1 GiBps

Sistemas de archivos regionales y de una sola zona: rendimiento total por sistema de archivos para todos los clientes conectados en cada uno Región de AWS

Región de AWS	Rendimiento de lectura máximo	Rendimiento de escritura máximo
Región del Este de EE. UU. (Ohio)	5 GiBps	3 GiBps
Región del Este de EE. UU. (Norte de Virginia)		
Región del oeste de EE. UU. (Oregón)		
Región de Asia-Pacífico (Sídney)		
Región de Europa (Irlanda)		
Todos los demás Regiones de AWS	3 GiBps	1 GiBps

Cuotas para clientes NFS

Se aplican las siguientes cuotas para los clientes NFS, suponiendo que se trata de un cliente Linux NFSv4.1:

- El rendimiento máximo combinado de lectura y escritura es de 1500 mebibytes por segundo (MiBps) para los sistemas de archivos que utilizan Elastic Throughput y se montan con la versión

2.0 o posterior del cliente Amazon EFS (amazon-efs-utils versión) o el controlador CSI de Amazon EFS (aws-efs-csi-driver). El rendimiento máximo para todos los demás sistemas de archivos es de 500. MiBps Para obtener más información acerca del desempeño, consulte [Resumen de rendimiento](#). El rendimiento del cliente NFS se calcula como el número total de bytes que se envían y se reciben, con un tamaño mínimo de solicitud NFS de 4 KB (tras aplicar una tasa de medición de 1/3 para las solicitudes de lectura).

- Hasta 65.536 usuarios activos de cada cliente pueden tener los archivos abiertos al mismo tiempo.
- Se abren hasta 65.536 archivos al mismo tiempo en la instancia. Describir los contenidos del directorio no cuenta como abrir un archivo.
- Cada montaje único del cliente puede adquirir hasta un total de 65 536 bloqueos por conexión.
- Al conectarse a Amazon EFS, los clientes de NFS ubicados localmente en las instalaciones o en otra Región de AWS pueden observar un desempeño inferior que cuando se conectan a EFS desde la misma Región de AWS. Este efecto se debe al aumento de la latencia de red. La latencia de red de 1 ms o menos es obligatoria para lograr un rendimiento máximo para cada cliente. Utilice el servicio de migración de DataSync datos al migrar conjuntos de datos de gran tamaño de servidores NFS locales a EFS.
- El protocolo NFS admite un máximo de 16 ID de grupo (GID) por usuario y cualquier GID adicional se trunca a partir de las solicitudes de los clientes de NFS. Para obtener más información, consulte [Acceso denegado a los archivos permitidos en el sistema de archivos NFS](#).
- No se admite el uso de Amazon EFS con Microsoft Windows.

Cuotas para sistemas de archivos de Amazon EFS

Las cuotas siguientes son específicas de los sistemas de archivos de Amazon EFS.

Recurso	Cuota
Longitud del nombre del archivo, en bytes	255
Longitud de enlace simbólico (symlink), en bytes	4.080
Número de enlaces físicos a un archivo	177
Tamaño de un solo archivo	52 673 613 135 872 bytes (47,9 TiB)
Número de niveles de profundidad del directorio	1 000

Recurso	Cuota
Número de bloqueos en un solo archivo en todas las instancias y usuarios	512
Límite de caracteres para cada política del sistema de archivos	20 000
*Número de operaciones de archivo por segundo en el modo de uso general	250.000

*Para obtener más información acerca del número de operaciones de archivos por segundo para el modo de uso general, consulte [Resumen de rendimiento](#).

Funciones de NFSv4.0 y 4.1 no compatibles

Aunque Amazon EFS no admite NFSv2 ni NFSv3, sí admite NFSv4.1 y NFSv4.0, excepto en lo que respecta a las siguientes características:

- pNFS
- Delegación de cliente o devoluciones de cualquier tipo
 - La operación OPEN siempre devuelve OPEN_DELEGATE_NONE como tipo de delegación.
 - La operación OPEN devuelve NFSERR_NOTSUPP para los tipos de reclamación CLAIM_DELEGATE_CUR y CLAIM_DELEGATE_PREV.
- Bloqueo obligatorio

Todos los bloqueos en Amazon EFS son consultivos, lo que significa que las operaciones de lectura y escritura no comprueban si hay bloqueos en conflicto antes de ejecutar la operación.

- Denegar compartir

NFS admite el concepto de denegación de uso compartido. El concepto de denegación del uso compartido se utiliza principalmente para clientes de Windows para que los usuarios denieguen el acceso de otras personas a un archivo particular que se ha abierto. Amazon EFS no admite esta opción y devuelve el error de NFS NFS4ERR_NOTSUPP para los comandos OPEN especificando un valor de denegación de uso compartido en lugar de OPEN4_SHARE_DENY_NONE. Los clientes NFS de Linux no utilizan más que OPEN4_SHARE_DENY_NONE.

- Listas de control de acceso (ACL)
- Amazon EFS no actualiza el atributo `time_access` en lecturas de archivo. Amazon EFS actualiza `time_access` en los siguientes eventos:
 - Cuando se crea un archivo (se crea un inode).
 - Cuando un cliente NFS realiza una llamada `setattr` explícita.
 - En una escritura al inode provocada, por ejemplo, por cambios en el tamaño del archivo o cambios en los metadatos del archivo.
 - Se actualiza algún atributo inode.
- Espacios de nombres
- Caché de respuestas persistente
- Seguridad basada en Kerberos
- Retención de datos NFSv4.1
- SetUID en directorios
- Tipos de archivo no compatibles cuando se utiliza la operación CREATE: dispositivos de bloque (NF4BLK), dispositivos de caracteres (NF4CHR), directorio de atributos (NF4ATTRDIR) y atributo designado (NF4NAMEDATTR).
- Atributos no compatibles: `FATTR4_ARCHIVE`, `FATTR4_FILES_AVAIL`, `FATTR4_FILES_FREE`, `FATTR4_FILES_TOTAL`, `FATTR4_FS_LOCATIONS`, `FATTR4_MIMETYPE`, `FATTR4_QUOTA_AVAIL_HARD`, `FATTR4_QUOTA_AVAIL_SOFT`, `FATTR4_QUOTA_USED`, `FATTR4_TIME_BACKUP` y `FATTR4_ACL`.

Un intento de definir estos atributos tendrá como resultado un error `NFS4ERR_ATTRNOTSUPP` que se envía de vuelta al cliente.

Consideraciones adicionales

Además, tenga en cuenta lo siguiente:

- Para obtener una lista de Regiones de AWS dónde puede crear los sistemas de archivos Amazon EFS, consulte [Referencia general de AWS](#).
- Amazon EFS no es compatible con la opción de montaje `nconnect`.
- Puede montar un sistema de archivos de Amazon EFS en servidores del centro de datos en las instalaciones mediante AWS Direct Connect y VPN. Para obtener más información, consulte [Montaje con clientes en las instalaciones](#).

Solución de errores de operación de archivos

Cuando accede a sistemas de archivos de Amazon EFS, se aplican determinados límites en los archivos del sistema de archivos. Superar estos límites provoca errores de operación de archivos. Para obtener más información acerca de los límites basados en archivos y cliente en Amazon EFS, consulte [Cuotas para clientes NFS](#). A continuación, puede encontrar algunos errores de operación de archivos comunes y los límites asociados a cada error.

Temas

- [El comando falla con el error "Cuota de disco superada"](#)
- [El comando falla con "error de E/S"](#)
- [El comando falla con el error "El nombre de archivo es demasiado largo"](#)
- [El comando produce el error "Archivo no encontrado"](#)
- [El comando falla con el error "Demasiados vínculos"](#)
- [El comando falla con el error "Archivo demasiado grande"](#)

El comando falla con el error "Cuota de disco superada"

Amazon EFS no admite actualmente cuotas de disco de usuario. Este error se puede producir si se ha superado alguno de los límites siguientes:

- Hasta 65.536 usuarios activos pueden tener archivos abiertos al mismo tiempo. Una cuenta de usuario a la que se accede varias veces cuenta como un usuario activo.
- Se pueden abrir hasta 65.536 archivos a la vez en una instancia. Describir los contenidos del directorio no cuenta como abrir un archivo.
- Cada soporte único del cliente puede adquirir hasta un total de 65 536 bloqueos por conexión.

Acción que debe ejecutarse

Si detecta este problema, puede resolverlo identificando cual de los límites anteriores está superando y, a continuación, realizar cambios para satisfacer dicho límite. Para obtener más información, consulte [Cuotas para clientes NFS](#).

El comando falla con "error de E/S"

Este error se produce cuando se detecta uno de los siguientes problemas:

- Más de 65 536 cuentas de usuario activas de cada instancia tienen archivos abiertos a la vez.

Acción que debe ejecutarse

Si encuentra este problema, puede resolverlo satisfaciendo el límite admitido de archivos abiertos en sus instancias. Para hacerlo, reduzca el número de usuarios activos que tienen archivos abiertos simultáneamente en sus instancias desde su sistema de archivos de Amazon EFS.

- Se eliminó la AWS KMS clave que cifraba el sistema de archivos.

Acción que debe ejecutarse

Si tiene este problema, ya no puede descifrar los datos que se habían cifrado con esa clave, lo que significa que no se pueden recuperar.

El comando falla con el error "El nombre de archivo es demasiado largo"

Este error se produce cuando el tamaño de un nombre de archivo o su vínculo simbólico (symlink) es demasiado largo. Los nombres de archivo tienen los siguientes límites:

- Un nombre puede tener hasta 255 bytes.
- Un vínculo simbólico puede tener hasta 4 080 bytes de tamaño.

Acción que debe ejecutarse

Si encuentra este problema, puede resolverlo reduciendo el tamaño de su nombre de archivo o la longitud de symlink para cumplir los límites admitidos.

El comando produce el error "Archivo no encontrado"

Este error se produce porque algunas versiones antiguas de 32 bits del conjunto de aplicaciones de Oracle E-Business utilizan interfaces de E/S de archivos de 32 bits y EFS utiliza números de inode de 64 bits. Las llamadas al sistema que pueden producir un error incluyen ``stat()`` y ``readdir()``.

Acción que debe ejecutarse

Si encuentra este error, puede resolverlo usando la opción de arranque `nfs.enable_ino64=0` kernel. Esta opción comprime los números de inode de EFS de 64 bits a 32 bits. Las opciones de arranque del kernel se manejan de manera diferente para diferentes distribuciones de Linux. En Amazon Linux, active esta opción agregando `nfs.enable_ino64=0 kernel` a la variable

GRUB_CMDLINE_LINUX_DEFAULT en `/etc/default/grub`. Consulte su distribución para obtener documentación específica sobre cómo activar las opciones de arranque del kernel.

El comando falla con el error "Demasiados vínculos"

Este error se produce cuando hay demasiados vínculos físicos a un archivo. Puede tener hasta 177 vínculos físicos en un archivo.

Acción que debe ejecutarse

Si detecta este problema, puede resolverlo reduciendo el número de vínculos físicos a un archivo para cumplir el límite admitido.

El comando falla con el error "Archivo demasiado grande"

Este error se produce cuando un archivo es demasiado grande. Un archivo único puede tener hasta 47.9 673 613 135 872 bytes (52 TiB) de tamaño.

Acción que debe ejecutarse

Si encuentra este problema, puede resolverlo reduciendo el tamaño de un archivo para satisfacer el límite admitido.

API de Amazon EFS

La API de Amazon EFS es un protocolo de red basado en [HTTP \(RFC 2616\)](#). Para cada llamada a la API, debe realizar una solicitud HTTP al punto final de la API de Amazon EFS específico de la región Región de AWS donde desea administrar los sistemas de archivos. La API utiliza documentos JSON (RFC 4627) para el cuerpo de las solicitudes y respuestas HTTP.

La API de Amazon EFS es un modelo de RPC. En este modelo, hay un conjunto fijo de operaciones y los clientes conocen la sintaxis de cada operación sin ninguna interacción previa. En la siguiente sección, encontrará una descripción de cada operación de API utilizando una notación RPC abstracta. Cada una tiene un nombre de operación que no aparece en la ruta. Para cada operación, el tema especifica el mapeo a los elementos de solicitud HTTP.

La operación específica de Amazon EFS a la que se asigna una solicitud determinada se determina mediante una combinación del método de la solicitud (GET, PUT, POST o DELETE) y de los distintos patrones que coincide su URI de solicitud. Si la operación es PUT o POST, Amazon EFS extrae los argumentos de llamada del segmento de ruta Request-URI, los parámetros de la consulta y el objeto JSON del cuerpo de la solicitud.

Note

Aunque los nombres de las operaciones, por ejemplo, `CreateFileSystem`, no aparecen en la red, son importantes en las políticas de AWS Identity and Access Management (IAM). Para obtener más información, consulte [Administración de identidades y acceso Amazon Elastic File System](#).

El nombre de la operación también se usa para nombrar los comandos de las herramientas de línea de comandos y los elementos de las API del AWS SDK. Por ejemplo, existe un comando de la AWS CLI llamado `create-file-system` que se asocia a la operación `CreateFileSystem`.

El nombre de la operación también aparece en AWS CloudTrail los registros de las llamadas a la API de Amazon EFS.

Punto de enlace de la API

El punto de enlace de la API es el nombre de DNS que se utiliza como host en el URI de HTTP de las llamadas al API. Estos extremos de la API son específicos de las regiones de AWS y adoptan la siguiente forma.

```
elasticfilesystem.aws-region.amazonaws.com
```

Por ejemplo, el punto de enlace de la API de Amazon EFS para la región EE. UU. es:

```
elasticfilesystem.us-west-2.amazonaws.com
```

Para obtener una lista de los sistemas compatibles con Amazon EFS (donde puede crear y administrar sistemas de archivos), consulte [Amazon Elastic File System](#) en Referencia general de AWS.

El punto final de la API específico de la región define el alcance de los recursos de Amazon EFS a los que se puede acceder al realizar una llamada a la API. Por ejemplo, si realiza la `DescribeFileSystems` operación con el punto de conexión anterior, obtendrá una lista de los sistemas de archivos de la región de EE. UU. Oeste (Oregón) que se han creado en su cuenta.

Versión de API

La versión de API utilizada en una llamada se identifica mediante el primer segmento de la ruta de la URI de la solicitud y su formato es una fecha ISO 8601. Por ejemplo, consulte [CreateFileSystem](#).

En la documentación se describe la versión 2015-02-01 del API.

Temas relacionados

En las secciones siguientes proporcione descripciones de las operaciones de las API, cómo crear una firma para la solicitud de autenticación y cómo conceder permisos para dichas operaciones de API utilizando las políticas de IAM.

- [Administración de identidades y acceso Amazon Elastic File System](#)
- [Acciones](#)
- [Data Types](#)

Trabajando con la tasa de solicitudes de la API de consultas para Amazon EFS

Las solicitudes de API de Amazon EFS se limitan para cada Cuenta de AWS región para mejorar el rendimiento del servicio. Todas las llamadas a la API de Amazon EFS juntas, independientemente de que provengan de una aplicación, de la AWS CLI consola de Amazon EFS o de la consola de Amazon EFS, no deben superar la tasa máxima de solicitudes de API permitida. La tasa máxima de solicitudes de API puede variar de un país a otro Regiones de AWS. Las solicitudes de API realizadas se atribuyen al subyacente Cuenta de AWS.

Si una solicitud de API supera la velocidad de las solicitudes de API en su categoría, la solicitud devuelve el código de error `ThrottlingException`. Para evitarlo, asegúrese de que la aplicación no reintenta las solicitudes de API a una velocidad elevada. Para ello, lleve a cabo el sondeo con precaución y emplee reintentos con retardo exponencial.

Sondeo

Es posible que la aplicación necesite llamar a una operación de API repetidamente para comprobar si hay alguna actualización de estado. Antes de comenzar el sondeo, indique el tiempo de solicitud para completarlo potencialmente. Cuando comience el sondeo, utilice un intervalo de suspensión adecuado entre las sucesivas solicitudes. Para obtener resultados óptimos, utilice un intervalo de suspensión creciente.

Reintentos para procesamiento por lotes

Es posible que su aplicación tenga que volver a intentar una solicitud de API cuando se produzca un error o procesar varios recursos (por ejemplo, todos sus sistemas de archivos de Amazon EFS). Para reducir la velocidad de solicitudes de API, utilice un intervalo de suspensión entre solicitudes sucesivas adecuado. Para obtener resultados óptimos, utilice un intervalo de suspensión creciente o variable.

Calcular el intervalo de sueño

Cuando tenga que sondear o reintentar una solicitud de API, recomendamos que utilice un algoritmo de retardo exponencial para calcular el intervalo de suspensión entre las llamadas al API. El retardo exponencial se basa en la idea de utilizar tiempos de espera progresivamente más largos entre reintentos para las respuestas a errores consecutivos. Para obtener más información y ejemplos

de implementación de este algoritmo, consulte [Reintentos de error y retroceso exponencialAWS](#)
[enReferencia general de Amazon Web Services](#).

Acciones

Se admiten las siguientes acciones:

- [CreateAccessPoint](#)
- [CreateFileSystem](#)
- [CreateMountTarget](#)
- [CreateReplicationConfiguration](#)
- [CreateTags](#)
- [DeleteAccessPoint](#)
- [DeleteFileSystem](#)
- [DeleteFileSystemPolicy](#)
- [DeleteMountTarget](#)
- [DeleteReplicationConfiguration](#)
- [DeleteTags](#)
- [DescribeAccessPoints](#)
- [DescribeAccountPreferences](#)
- [DescribeBackupPolicy](#)
- [DescribeFileSystemPolicy](#)
- [DescribeFileSystems](#)
- [DescribeLifecycleConfiguration](#)
- [DescribeMountTargets](#)
- [DescribeMountTargetSecurityGroups](#)
- [DescribeReplicationConfigurations](#)
- [DescribeTags](#)
- [ListTagsForResource](#)
- [ModifyMountTargetSecurityGroups](#)
- [PutAccountPreferences](#)
- [PutBackupPolicy](#)

- [PutFileSystemPolicy](#)
- [PutLifecycleConfiguration](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateFileSystem](#)
- [UpdateFileSystemProtection](#)

CreateAccessPoint

Crea un punto de acceso de EFS. Un punto de acceso es una vista específica de la aplicación en un sistema de archivos de EFS que aplica un usuario y un grupo del sistema operativo, así como una ruta del sistema de archivos, a cualquier solicitud del sistema de archivos realizada a través del punto de acceso. El usuario y el grupo del sistema operativo invalidan cualquier información de identidad proporcionada por el cliente de NFS. La ruta del sistema de archivos se expone como directorio raíz del punto de acceso. Las aplicaciones que utilizan el punto de acceso solo pueden acceder a los datos en el directorio y subdirectorios de la propia aplicación. Para obtener más información, consulte [Mounting a file system using EFS access points](#) (Montaje de un sistema de archivos mediante puntos de acceso de EFS).

Note

Si se envían varias solicitudes para crear puntos de acceso en el mismo sistema de archivos en rápida sucesión y el sistema de archivos se acerca al límite de 1000 puntos de acceso, es posible que estas solicitudes reciban una respuesta limitadora. Esto es para garantizar que el sistema de archivos no supere el límite de puntos de acceso indicada.

Esta operación necesita permisos para la acción `elasticfilesystem:CreateAccessPoint`.

Los puntos de acceso se pueden etiquetar al crearlos. Si se especifican etiquetas en la acción de creación, IAM realiza una autorización adicional en la acción `elasticfilesystem:TagResource` para verificar que los usuarios tengan permisos para crear etiquetas. Por lo tanto, usted debe conceder permisos explícitos para utilizar la acción `elasticfilesystem:TagResource`. Para obtener más información, consulte [Conceder permisos para etiquetar recursos durante la creación](#).

Sintaxis de la solicitud

```
POST /2015-02-01/access-points HTTP/1.1
Content-type: application/json
```

```
{
  "ClientToken": "string",
  "FileSystemId": "string",
  "PosixUser": {
    "Gid": number,
    "SecondaryGids": [ number ],
```



```
  "Uid": number
},
"RootDirectory": {
  "CreationInfo": {
    "OwnerGid": number,
    "OwnerUid": number,
    "Permissions": "string"
  },
  "Path": "string"
},
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
]
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

ClientToken

Cadena de hasta 64 caracteres ASCII que Amazon EFS utiliza para garantizar la creación idempotente.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: .+

Obligatorio: sí

FileSystemId

El ID del sistema de archivos de EFS al que el punto de acceso proporciona acceso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

[PosixUser](#)

El usuario y el grupo del sistema operativo aplicados a todas las solicitudes del sistema de archivos realizadas mediante el punto de acceso.

Tipo: objeto [PosixUser](#)

Obligatorio: no

[RootDirectory](#)

Especifica el directorio del sistema de archivos de EFS que el punto de acceso expone como directorio raíz del sistema de archivos a los clientes de NFS que utilizan el punto de acceso. Los clientes que utilizan el punto de acceso solo pueden acceder al directorio raíz e inferiores. Si `RootDirectory > Path` especificado no existe, Amazon EFS crea el directorio raíz utilizando la configuración de `CreationInfo` cuando un cliente se conecta a un punto de acceso. Al especificar un `RootDirectory`, debe proporcionar la `Path` y la `CreationInfo`.

Amazon EFS crea un directorio raíz solo si ha proporcionado `CreationInfo: OwnUid`, `OwnGID` y los permisos para el directorio. Si no proporciona dicha información, Amazon EFS no creará el directorio raíz. Si el directorio raíz no existe, los intentos de montaje utilizando el punto de acceso fallarán.

Tipo: objeto [RootDirectory](#)

Obligatorio: no

[Tags](#)

Crea las etiquetas asociadas al punto de acceso. Cada etiqueta es un par clave-valor, cada clave debe ser única. Para obtener más información, consulte los [AWS recursos de etiquetado](#) en la Guía de referencia AWS general.

Tipo: matriz de objetos [Tag](#)

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AccessPointArn": "string",
  "AccessPointId": "string",
  "ClientToken": "string",
  "FileSystemId": "string",
  "LifeCycleState": "string",
  "Name": "string",
  "OwnerId": "string",
  "PosixUser": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": number,
      "OwnerId": number,
      "Permissions": "string"
    },
    "Path": "string"
  },
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AccessPointArn

El nombre de recurso de Amazon (ARN) único asociado al punto de acceso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}$`

[AccessPointId](#)

El ID del punto de acceso, asignado por Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

[ClientToken](#)

La cadena opaca especificada en la solicitud para garantizar la creación de idempotentes.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `.+`

[FileSystemId](#)

El ID del sistema de archivos de EFS al que se aplica el punto de acceso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[LifecycleState](#)

Identifica la fase del ciclo de vida del punto de acceso.

Tipo: cadena

Valores válidos: `creating | available | updating | deleting | deleted | error`

Name

El nombre del punto de acceso. Este es el valor de la etiqueta Name.

Tipo: cadena

OwnerId

Identifica al Cuenta de AWS propietario del recurso del punto de acceso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^\d{12} | (\d{4}-\d{4}-\d{4})$`

PosixUser

La identidad POSIX completa, incluido el ID de usuario, el ID de grupo y los ID de grupo secundarios en el punto de acceso que se utiliza para todas las operaciones de archivos por los clientes de NFS que utilizan el punto de acceso.

Tipo: objeto [PosixUser](#)

RootDirectory

El directorio del sistema de archivos de EFS que el punto de acceso expone como directorio raíz a los clientes de NFS que utilizan el punto de acceso.

Tipo: objeto [RootDirectory](#)

Tags

Las etiquetas asociadas al punto de acceso, presentadas como una matriz de objetos Tag.

Tipo: matriz de objetos [Tag](#)

Errores

AccessPointAlreadyExists

Se devuelve si el punto de acceso que está intentando crear ya existe, con el token de creación que proporcionó en la solicitud.

Código de estado HTTP: 409

AccessPointLimitExceeded

Se devuelve si ya Cuenta de AWS se ha creado el número máximo de puntos de acceso permitidos por sistema de archivos. Para obtener más información, consulte <https://docs.aws.amazon.com/efs/latest/ug/limits.html#limits-efs-resources-per-account-per-region>.

Código de estado HTTP: 403

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

IncorrectFileSystemLifecycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no “disponible”.

Código de estado HTTP: 409

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

ThrottlingException

Se devuelve cuando la acción de la API `CreateAccessPoint` se ejecuta demasiado rápido y el número de puntos de acceso en el sistema de archivos se acerca al [límite de 120](#).

Código de estado HTTP: 429

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateFileSystem

Crea un nuevo sistema de archivos vacío. La operación requiere un token de creación en la solicitud que Amazon EFS usa para garantizar la creación idempotent (llamar a la operación con el mismo token de creación no tiene ningún efecto). Si actualmente no existe un sistema de archivos que sea propiedad de la persona que llama Cuenta de AWS con el token de creación especificado, esta operación hace lo siguiente:

- Crea un nuevo sistema de archivos vacío. El sistema de archivos tendrá un ID de Amazon EFS asignado y un estado de ciclo de vida inicial de `creating`.
- Se devuelve con la descripción del sistema de archivos creado.

De lo contrario, esta operación devuelve un error `FileSystemAlreadyExists` con el ID del sistema de archivos existente.

Note

Para casos de uso básicos, puede utilizar un UUID generado de forma aleatoria para el token de creación.

La operación idempotent le permite volver a intentar una llamada `CreateFileSystem` sin riesgo de crear un sistema de archivos adicional. Esto puede ocurrir cuando una llamada inicial produce un error de forma que queda la incertidumbre de si se creó o no un sistema de archivos. Por ejemplo, se agotó el tiempo de espera de nivel de transporte o se restableció la conexión. Siempre que utilice el mismo token de creación, si la llamada inicial hubiera realizado con éxito la creación de un sistema de archivos, el cliente puede deducir su existencia a partir del error `FileSystemAlreadyExists`.

Para obtener más información, consulte [Creación de recursos para Amazon EFS](#) en la Guía del usuario de Amazon EFS.

Note

La llamada `CreateFileSystem` realiza devuelve información mientras el estado de ciclo de vida del sistema de archivos siga siendo `creating`. Puede comprobar el estado de creación del sistema de archivos llamando a la operación [DescribeFileSystems](#), que entre otras cosas devuelve el estado del sistema de archivos.

Esta operación también tiene un parámetro `PerformanceMode` opcional que elige para su sistema de archivos. Se recomienda `generalPurpose` `PerformanceMode` para todos los sistemas de archivos. El modo `maxIO` es un tipo de rendimiento de la generación anterior que está diseñado para cargas de trabajo altamente paralelizadas que pueden tolerar latencias más altas que el modo `generalPurpose`. El modo `MaxIO` no es compatible con los sistemas de archivos `One Zone` o sistemas de archivos que utilicen rendimiento elástico.

El `PerformanceMode` no se puede cambiar después de haber creado el sistema de archivos. Para obtener más información, consulte [Amazon EFS: Modos de rendimiento](#).

El modo de rendimiento del sistema de archivos se puede configurar mediante el parámetro `ThroughputMode`.

Una vez que se ha creado totalmente el sistema de archivos, Amazon EFS establece su estado de ciclo de vida en `available`. A partir de ese momento puede crear uno o varios destinos de montaje para el sistema de archivos en la VPC. Para obtener más información, consulte [CreateMountTarget](#). Monte su sistema de archivos de Amazon EFS en instancias EC2 en su VPC a través de los destinos de montaje. Para obtener más información, consulte [Amazon EFS: cómo funciona](#).

Esta operación necesita permisos para la acción `elasticfilesystem:CreateFileSystem`.

Los sistemas de archivos se pueden etiquetar al crearlos. Si se especifican etiquetas en la acción de creación, IAM realiza una autorización adicional en la acción `elasticfilesystem:TagResource` para verificar que los usuarios tengan permisos para crear etiquetas. Por lo tanto, usted debe conceder permisos explícitos para utilizar la acción `elasticfilesystem:TagResource`. Para obtener más información, consulte [Conceder permisos para etiquetar recursos durante la creación](#).

Sintaxis de la solicitud

```
POST /2015-02-01/file-systems HTTP/1.1
Content-type: application/json

{
  "AvailabilityZoneName": "string",
  "Backup": boolean,
  "CreationToken": "string",
  "Encrypted": boolean,
  "KmsKeyId": "string",
  "PerformanceMode": "string",
  "ProvisionedThroughputInMibps": number,
  "Tags": [
```

```
{
  "Key": "string",
  "Value": "string"
},
"ThroughputMode": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

AvailabilityZoneName

Para los sistemas de archivos One Zone, especifique la zona de disponibilidad AWS en la que se creará el sistema de archivos. Utilice el formato `us-east-1a` para especificar la zona de disponibilidad. Para obtener más información acerca de los sistemas de archivos One Zone, consulte [Tipos de sistemas de archivos EFS](#) en la Guía del usuario de Amazon EFS.

Note

Los sistemas de archivos One Zone no están disponibles en todas las zonas de disponibilidad en las Regiones de AWS que Amazon EFS está disponible.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `.+`


Obligatorio: no

Backup

Especifica si las copias de seguridad automáticas están habilitadas en el sistema de archivos que está creando. Establezca el valor en `true` para habilitar copias de seguridad automáticas. Si va a

crear un sistema de archivos One Zone, las copias de seguridad automáticas están habilitadas de forma predeterminada. Para obtener más información, consulte [Copias de seguridad automáticas](#) en la Guía del usuario de Amazon EFS.

El valor predeterminado es `false`. Sin embargo, si especifica una `AvailabilityZoneName`, el valor predeterminado es `true`.

 Note

AWS Backup no está disponible en todos los Regiones de AWS lugares donde Amazon EFS está disponible.

Tipo: Booleano

Obligatorio: no

CreationToken

Una cadena de hasta 64 caracteres ASCII. Amazon EFS la utiliza para garantizar la creación de idempotentes.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `.+`

Obligatorio: sí

Encrypted

Un valor booleano que, si es verdadero, crea un sistema de archivos cifrado. Al crear un sistema de archivos cifrados, tiene la opción de especificar una AWS Key Management Service clave existente (clave KMS). Si no especifica una clave KMS, se utilizará la clave KMS por defecto para Amazon EFS, `/aws/elasticfilesystem`, se utiliza para proteger el sistema de archivos cifrado.

Tipo: Booleano

Obligatorio: no

KmsKeyId

El ID de la clave KMS que se va a utilizar para proteger el sistema de archivos cifrado. Este parámetro solo es necesario si quiere utilizar una clave KMS que no sea la predeterminada. Si no se especifica este parámetro, se utiliza la clave KMS de forma predeterminada para Amazon EFS. Puede usar los siguientes formatos para especificar este ID de clave KMS.

- ID de clave: un identificador único de la clave, por ejemplo `1234abcd-12ab-34cd-56ef-1234567890ab`.
- ARN: un nombre de recurso de Amazon (ARN) para la clave, por ejemplo `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- Alias de clave: un nombre de visualización creado con anterioridad para una clave, por ejemplo `alias/projectKey1`.
- ARN de alias de clave: un ARN para un alias de clave, por ejemplo `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`.

Si lo usa `KmsKeyId`, debe establecer el parámetro [CreateFileSystem:Encrypted](#) en true.

Important

EFS solo acepta claves KMS simétricas. No puede utilizar claves KMS asimétricas con sistemas de archivos de Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.


Patrón: `^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

Obligatorio: no

PerformanceMode

El modo de desempeño del sistema de archivos. Recomendamos el modo de rendimiento `generalPurpose` para todos los sistemas de archivos. Los sistemas de archivos que utilizan el modo de rendimiento `maxIO` pueden escalar a niveles superiores de rendimiento total y

operaciones por segundo, con la contrapartida de que la latencia es un poco mayor en la mayoría de las operaciones con archivos. El modo de rendimiento no se puede cambiar después de haber creado el sistema de archivos. El modo `maxIO` no es compatible con los sistemas de archivos `One Zone`.

 **Important**

Debido a las latencias por operación más altas con una E/S máx., recomendamos utilizar el modo de rendimiento de uso general para todos los sistemas de archivos.

El valor predeterminado es `generalPurpose`.

Tipo: cadena

Valores válidos: `generalPurpose` | `maxIO`

Obligatorio: no

[ProvisionedThroughputInMibps](#)

El rendimiento, medido en mebibytes por segundo (MiBps), que desea aprovisionar para el sistema de archivos que está creando. Obligatorio si `ThroughputMode` se establece en `provisioned`. Los valores válidos son de 1 a 3414 MiBps, y el límite superior depende de la región. Para aumentar este límite, póngase en contacto con [AWS Support](#) Para obtener más información, consulte [Cuotas de Amazon EFS que puede incrementar](#) en la Guía del usuario de Amazon EFS.

Tipo: Doble

Rango válido: valor mínimo de 1.0.

Obligatorio: no

[Tags](#)

Se utiliza para crear una o varias etiquetas asociadas al sistema de archivos. Las etiquetas son pares clave-valor que define el usuario. Asigne un nombre al sistema de archivos en el momento de su creación mediante la inclusión de un par clave-valor `"Key": "Name", "Value": "{value}"`. Cada clave debe ser única. Para obtener más información, consulte [AWS los recursos de etiquetado](#) en la Guía de referencia AWS general.

Tipo: matriz de objetos [Tag](#)

Obligatorio: no

[ThroughputMode](#)

Especifica el modo de rendimiento del sistema de archivos. El modo puede ser `bursting`, `provisioned` o `elastic`. Si establece `ThroughputMode` en `provisioned`, también debe establecer un valor para `ProvisionedThroughputInMibps`. Después de crear el sistema de archivos, puede disminuir el rendimiento aprovisionado del sistema de archivos o alternar los modos de rendimiento, con ciertas restricciones de tiempo. Para obtener más información, consulte [Especificación del rendimiento con el modo aprovisionado](#) en la Guía del usuario de Amazon EFS.

El valor predeterminado es `bursting`.

Tipo: cadena

Valores válidos: `bursting` | `provisioned` | `elastic`

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 201
Content-type: application/json

{
  "AvailabilityZoneId": "string",
  "AvailabilityZoneName": "string",
  "CreationTime": number,
  "CreationToken": "string",
  "Encrypted": boolean,
  "FileSystemArn": "string",
  "FileSystemId": "string",
  "FileSystemProtection": {
    "ReplicationOverwriteProtection": "string"
  },
  "KmsKeyId": "string",
  "LifecycleState": "string",
  "Name": "string",
  "NumberOfMountTargets": number,
```

```

"OwnerId": "string",
"PerformanceMode": "string",
"ProvisionedThroughputInMibps": number,
"SizeInBytes": {
  "Timestamp": number,
  "Value": number,
  "ValueInArchive": number,
  "ValueInIA": number,
  "ValueInStandard": number
},
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"ThroughputMode": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

AvailabilityZoneId

El identificador único y coherente de la zona de disponibilidad en la que se encuentra el sistema de archivos y solo es válido para los sistemas de archivos One Zone. Por ejemplo, use1-az1 es un identificador de zona de disponibilidad para el Región de AWS us-east-1 y tiene la misma ubicación en todas. Cuenta de AWS

Tipo: cadena

AvailabilityZoneName

Describe la zona de AWS disponibilidad en la que se encuentra el sistema de archivos y solo es válido para los sistemas de archivos de una zona. Para obtener más información, consulte [Uso de clases de almacenamiento de EFS](#) en la Guía del usuario de Amazon EFS.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: . +

CreationTime

Hora en que se creó el sistema de archivos, en segundos (desde 1970-01-01T 00:00:00 Z).

Tipo: marca temporal

CreationToken

La cadena opaca especificada en la solicitud.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: . +

Encrypted

Un valor booleano que, si es verdadero, indica que el sistema de archivos está cifrado.

Tipo: Booleano

FileSystemArn

Nombre de recurso de Amazon (ARN) para el sistema de archivos de EFS en el formato `arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id` . Ejemplo con datos de muestra: `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Tipo: cadena

FileSystemId

El ID del sistema de archivos, asignado por Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

FileSystemProtection

Describe la protección del sistema de archivos.

Tipo: objeto [FileSystemProtectionDescription](#)

[KmsKeyId](#)

El identificador de un sistema de archivos cifrado que AWS KMS key se utiliza para proteger el sistema de archivos cifrados.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

[LifecycleState](#)

La fase del ciclo de vida del sistema de archivos.

Tipo: cadena

Valores válidos: `creating | available | updating | deleting | deleted | error`

[Name](#)

Puede añadir etiquetas a un sistema de archivos, incluida una etiqueta Name. Para obtener más información, consulte [CreateFileSystem](#). Si el sistema de archivos tiene una etiqueta Name, Amazon EFS devuelve el valor de este campo.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 256.

Patrón: `^[\\p{L}\\p{Z}\\p{N}_.: /+=\\-@]*$`

[NumberOfMountTargets](#)

El número actual de destinos de montaje que tiene el sistema de archivos. Para obtener más información, consulte [CreateMountTarget](#).

Tipo: entero

Rango válido: valor mínimo de 0.

OwnerId

El Cuenta de AWS que creó el sistema de archivos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^\d{12})|(\d{4}-\d{4}-\d{4})$`

PerformanceMode

El modo de desempeño del sistema de archivos.

Tipo: cadena

Valores válidos: `generalPurpose | maxIO`

ProvisionedThroughputInMibps

La cantidad de rendimiento aprovisionada, medida en MiBps, para el sistema de archivos. Válido para los sistemas de archivos que utilizan `ThroughputMode` establecido en `provisioned`.

Tipo: Doble

Rango válido: valor mínimo de 0.0.

SizeInBytes

El último tamaño medido conocido (en bytes) de los datos almacenados en el sistema de archivos, en su campo `Value`, y el momento en que se determinó ese tamaño en su campo `Timestamp`. El valor de `Timestamp` es el número entero de segundos transcurridos desde 1970-01-01T 00:00:00 Z. El valor de `SizeInBytes` no representa el tamaño de una instantánea coherente del sistema de archivos, pero en última instancia es coherente cuando no hay escrituras en el sistema de archivos. Es decir, `SizeInBytes` representa el tamaño real solo si el sistema de archivos no se modifica durante un período superior a un par de horas. De lo contrario, el valor no es el tamaño exacto que tenía el sistema de archivos en ningún momento.

Tipo: objeto [FileSystemSize](#)

Tags

Las etiquetas asociadas al sistema de archivos, presentadas como un conjunto de objetos `Tag`.

Tipo: matriz de objetos [Tag](#)

[ThroughputMode](#)

Muestra el modo de rendimiento de un sistema de archivos. Para obtener más información, consulte [Modos de rendimiento](#) en la Guía del usuario de Amazon EFS.

Tipo: cadena

Valores válidos: `bursting` | `provisioned` | `elastic`

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemAlreadyExists

Se devuelve si el sistema de archivos que está intentando crear ya existe, con el token de creación que proporcionó.

Código de estado HTTP: 409

FileSystemLimitExceeded

Se devuelve si ya Cuenta de AWS se ha creado el número máximo de sistemas de archivos permitido por cuenta.

Código de estado HTTP: 403

InsufficientThroughputCapacity

Se devuelve si no hay suficiente capacidad para aprovisionar un rendimiento adicional. Este valor puede devolverse al intentar crear un sistema de archivos en el modo de rendimiento aprovisionado, al intentar aumentar el rendimiento aprovisionado de un sistema de archivos existente o al intentar cambiar un sistema de archivos existente del modo de rendimiento de ráfaga al de rendimiento aprovisionado. Inténtelo de nuevo más tarde.

Código de estado HTTP: 503

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

ThroughputLimitExceeded

Se devuelve si el modo de rendimiento o la cantidad de rendimiento aprovisionada no se pueden cambiar porque se ha alcanzado el límite de rendimiento de 1024 MiB/s.

Código de estado HTTP: 400

UnsupportedAvailabilityZone

Se devuelve si la funcionalidad de Amazon EFS solicitada no está disponible en la zona de disponibilidad especificada.

Código de estado HTTP: 400

Ejemplos

Crear un sistema de archivos de EFS cifrado

El siguiente ejemplo envía una solicitud POST para crear un sistema de archivos en la región us-west-2 con las copias de seguridad automáticas habilitadas. La solicitud especifica myFileSystem1 como token de creación de la idempotencia.

Solicitud de muestra

```
POST /2015-02-01/file-systems HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T215117Z
Authorization: <...>
Content-Type: application/json
Content-Length: 42

{
  "CreationToken" : "myFileSystem1",
  "PerformanceMode" : "generalPurpose",
  "Backup": true,
  "Encrypted": true,
  "Tags": [
    {
```

```
        "Key": "Name",
        "Value": "Test Group1"
    }
]
}
```

Respuesta de ejemplo

```
HTTP/1.1 201 Created
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 319

{
  "ownerId":"251839141158",
  "CreationToken":"myFileSystem1",
  "Encrypted": true,
  "PerformanceMode" : "generalPurpose",
  "fileSystemId":"fs-01234567",
  "CreationTime":"1403301078",
  "LifecycleState":"creating",
  "numberOfMountTargets":0,
  "SizeInBytes":{
    "Timestamp": 1403301078,
    "Value": 29313618372,
    "ValueInArchive": 201156,
    "ValueInIA": 675432,
    "ValueInStandard": 29312741784
  },
  "Tags":[
    {
      "Key": "Name",
      "Value": "Test Group1"
    }
  ],
  "ThroughputMode": "elastic"
}
```

Crear un sistema de archivos EFS cifrado con disponibilidad One Zone

El siguiente ejemplo envía una solicitud POST para crear un sistema de archivos en la región `us-west-2` con las copias de seguridad automáticas habilitadas. El sistema de archivos tendrá almacenamiento One Zone en la zona de disponibilidad `us-west-2b`.

Solicitud de muestra

```
POST /2015-02-01/file-systems HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T215117Z
Authorization: <...>
Content-Type: application/json
Content-Length: 42
```

```
{
  "CreationToken" : "myFileSystem2",
  "PerformanceMode" : "generalPurpose",
  "Backup": true,
  "AvailabilityZoneName": "us-west-2b",
  "Encrypted": true,
  "ThroughputMode": "elastic",
  "Tags":[
    {
      "Key": "Name",
      "Value": "Test Group1"
    }
  ]
}
```

Respuesta de ejemplo

```
HTTP/1.1 201 Created
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 319
```

```
{
  "ownerId":"251839141158",
  "CreationToken":"myFileSystem1",
  "Encrypted": true,
  "AvailabilityZoneId": "usew2-az2",
  "AvailabilityZoneName": "us-west-2b",
  "PerformanceMode" : "generalPurpose",
  "fileSystemId":"fs-01234567",
  "CreationTime":"1403301078",
  "LifecycleState":"creating",
  "numberOfMountTargets":0,
  "SizeInBytes":{
```

```
    "Timestamp": 1403301078,  
    "Value": 29313618372,  
    "ValueInArchive": 201156,  
    "ValueInIA": 675432,  
    "ValueInStandard": 29312741784  
  },  
  "Tags": [  
    {  
      "Key": "Name",  
      "Value": "Test Group1"  
    }  
  ],  
  "ThroughputMode": "elastic"  
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateMountTarget

Crea un destino de montaje para un sistema de archivos. A continuación, puede montar el sistema de archivos en instancias EC2 mediante el destino de montaje.

Puede crear un destino de montaje en cada zona de disponibilidad de su VPC. Todas las instancias EC2 en una VPC dentro de una determinada zona de disponibilidad comparten un solo destino de montaje para un determinado sistema de archivos. Si tiene varias subredes en una zona de disponibilidad, puede crear un destino de montaje en tan solo una de las subredes. Las instancias EC2 no tienen por qué estar en la misma subred que el destino de montaje para acceder a su sistema de archivos.

Solo puede crear un destino de montaje para un sistema de archivos One Zone. Debe crear ese destino de montaje en la misma zona de disponibilidad en la que encuentra el sistema de archivos. Utilice las propiedades `AvailabilityZoneName` y `AvailabilityZoneId` del objeto de respuesta [DescribeFileSystems](#) para obtener esta información. Utilice el `subnetId` asociado a la zona de disponibilidad del sistema de archivos al crear el destino de montaje.

Para obtener más información, consulte [Amazon EFS: cómo funciona](#).

Para crear un destino de montaje para un sistema de archivos, el estado del ciclo de vida del sistema de archivos debe ser `available`. Para obtener más información, consulte [DescribeFileSystems](#).

En la solicitud, proporcione lo siguiente:

- ID del sistema de archivos para el que se crea el destino de montaje.
- Un identificador de subred, que determina lo siguiente:
 - La VPC en la que Amazon EFS crea el destino de montaje
 - La zona de disponibilidad en la que Amazon EFS crea el destino de montaje
 - El intervalo de direcciones IP de donde Amazon EFS selecciona la dirección IP del destino de montaje (si no especifica una dirección IP en la solicitud)

Después de crear el destino de montaje, Amazon EFS devuelve una respuesta que incluye un valor `MountTargetId` y un valor `IpAddress`. Puede utilizar esta dirección IP al montar el sistema de archivos en una instancia EC2. También puede utilizar el nombre DNS del destino de montaje al montar el sistema de archivos. La instancia EC2 en la que se monta el sistema de archivos mediante el destino de montaje puede resolver el nombre DNS del destino de montaje en su dirección IP.

Para obtener más información, consulte la sección sobre [Cómo funciona: información general de la implementación](#).

Tenga en cuenta que puede crear destinos de montaje para un sistema de archivos en una sola VPC y que solo puede haber un destino de montaje por zona de disponibilidad. Es decir, si el sistema de archivos ya tiene uno o varios destinos de montaje creados, la subred especificada en la solicitud para añadir otro destino de montaje debe cumplir los requisitos siguientes:

- Debe pertenecer a la misma VPC que las subredes de los destinos de montaje existentes
- No debe estar en la misma zona de disponibilidad que cualquiera de las subredes de los destinos de montaje existentes

Si la solicitud cumple los requisitos, Amazon EFS hace lo siguiente:

- Crea un nuevo destino de montaje en la subred especificada.
- Crea también una nueva interfaz de red en la subred como sigue:
 - Si la solicitud proporciona una `IpAddress`, Amazon EFS asigna esa dirección IP a la interfaz de red. De lo contrario, Amazon EFS asigna una dirección libre en la subred (de la misma forma que lo hace la llamada `CreateNetworkInterface` de Amazon EC2 cuando una solicitud no especifica una dirección IP privada principal).
 - Si la solicitud proporciona `SecurityGroups`, esta interfaz de red se asocia a esos grupos de seguridad. De lo contrario, pertenece al grupo de seguridad predeterminado para la VPC de la subred.
 - Asigna la descripción `Mount target fsmt-id for file system fs-id` donde *fsmt-id* es el ID del destino de montaje y *fs-id* es el `FileSystemId`.
 - Establece la propiedad `requesterManaged` de la interfaz de red en `true` y el valor `requesterId` en EFS.

Cada destino de montaje de Amazon EFS tiene la correspondiente interfaz de red de EC2 administrada por el solicitante. Después de crear la interfaz de red, Amazon EFS establece el campo `NetworkInterfaceId` de la descripción del destino de montaje en el ID de interfaz de red y el campo `IpAddress` en la dirección. Si la creación de interfaz de red produce un error, toda la operación `CreateMountTarget` fracasa.

Note

La llamada a `CreateMountTarget` realiza una devolución solo después de crear la interfaz de red pero, mientras el estado del destino sigue siendo `creating`, usted puede comprobar el estado de creación del destino de montaje llamando a la operación [DescribeMountTargets](#), que entre otras cosas devuelve el estado del destino de montaje.

Le recomendamos crear un destino de montaje en cada una de las zonas de disponibilidad. Existen consideraciones de costos al usar un sistema de archivos en una zona de disponibilidad por medio de un destino de montaje creado en otra zona de disponibilidad. Para obtener más información, consulte [Amazon EFS](#). Además, usando siempre un destino de montaje local en la zona de disponibilidad de la instancia, elimina un escenario de error parcial. Si la zona de disponibilidad en la que se crea el destino de montaje deja de funcionar, no tendrá acceso a su sistema de archivos a través de dicho destino de montaje.

Esta operación requiere permisos para las siguientes acciones en el sistema de archivos:

- `elasticfilesystem:CreateMountTarget`

Esta operación también requiere permisos para las siguientes acciones de Amazon EC2:

- `ec2:DescribeSubnets`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`

Sintaxis de la solicitud

```
POST /2015-02-01/mount-targets HTTP/1.1
Content-type: application/json
```

```
{
  "FileSystemId": "string",
  "IpAddress": "string",
  "SecurityGroups": [ "string" ],
  "SubnetId": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

FileSystemId

El ID del sistema de archivos para el que se crea el destino de montaje.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

IpAddress

Dirección IPv4 válida en el intervalo de direcciones de la subred especificada.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 7. Longitud máxima de 15.

Patrón: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Obligatorio: no

SecurityGroups

Hasta cinco ID de grupo de seguridad de la VPC, de la forma `sg-xxxxxxx`. Estos deben ser para la misma VPC que la subred especificada.

Tipo: matriz de cadenas

Miembros de la matriz: número máximo de 100 elementos.

Limitaciones de longitud: longitud mínima de 11. Longitud máxima de 43.

Patrón: `^sg-[0-9a-f]{8,40}`

Obligatorio: no

SubnetId

El ID de la subred a la que se añade el destino de montaje. Para los sistemas de archivos One Zone, utilice la subred asociada a la zona de disponibilidad del sistema de archivos.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 80.

Patrón: `^subnet-[0-9a-f]{8,40}$`

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AvailabilityZoneId": "string",
  "AvailabilityZoneName": "string",
  "FileSystemId": "string",
  "IpAddress": "string",
  "LifecycleState": "string",
  "MountTargetId": "string",
  "NetworkInterfaceId": "string",
  "OwnerId": "string",
  "SubnetId": "string",
  "VpcId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AvailabilityZoneId

El identificador único y coherente de la zona de disponibilidad en la que reside el destino de montaje. Por ejemplo, use1-az1 es un ID AZ para la región us-east-1 y tiene la misma ubicación en todas. Cuenta de AWS

Tipo: cadena

[AvailabilityZoneName](#)

El nombre de la zona de disponibilidad en la que se encuentra el destino de montaje. Las zonas de disponibilidad se asignan de forma independiente a los nombres de cada una de ellas. Cuenta de AWS Por ejemplo, es Cuenta de AWS posible que la zona us-east-1a de disponibilidad de su ubicación no sea la misma que la us-east-1a de otra Cuenta de AWS.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: .+

[FileSystemId](#)

El ID del sistema de archivos para el que se crea el destino de montaje.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[IpAddress](#)

Dirección en la que se puede montar el sistema de archivos mediante el destino de montaje.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 7. Longitud máxima de 15.

Patrón: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

[LifecycleState](#)

Estado del ciclo de vida del destino de montaje.

Tipo: cadena

Valores válidos: `creating | available | updating | deleting | deleted | error`

[MountTargetId](#)

ID de destino de montaje asignado por el sistema.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 13. Longitud máxima de 45.

Patrón: `^fsmt-[0-9a-f]{8,40}$`

[NetworkInterfaceId](#)

El ID de la interfaz de red que creó Amazon EFS cuando creó el destino de montaje.

Tipo: cadena

[OwnerId](#)

Cuenta de AWS ID propietario del recurso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

[SubnetId](#)

El ID de la subred del destino de montaje.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 80.

Patrón: `^subnet-[0-9a-f]{8,40}$`

[VpcId](#)

El ID de la nube privada virtual (VPC) en la que está configurado el destino de montaje.

Tipo: cadena

Errores

AvailabilityZonesMismatch

Se devuelve si la zona de disponibilidad que se especificó para un destino de montaje es diferente de la zona de disponibilidad que se especificó para el almacenamiento One Zone. Para obtener más información, consulte [Redundancia de almacenamiento regional y One Zone](#).

Código de estado HTTP: 400

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

IncorrectFileSystemLifecycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no “disponible”.

Código de estado HTTP: 409

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

IpAddressInUse

Se devuelve si la solicitud especificó una `IpAddress` que ya está en uso en la subred.

Código de estado HTTP: 409

MountTargetConflict

Se devuelve si el destino de montaje infringe una de las restricciones especificadas en función de los destinos de montaje existentes en el sistema de archivos.

Código de estado HTTP: 409

NetworkInterfaceLimitExceeded

La cuenta que realiza la llamada ha alcanzado el límite de interfaces de red elásticas para la Región de AWS específica. Elimine algunas interfaces de red o solicite que se aumente la cuota de la cuenta. Para obtener más información, consulte [Cuotas de Amazon VPC](#) en la Guía del

usuario de Amazon VPC (consulte la entrada Interfaces de red por región en la tabla Interfaces de red).

Código de estado HTTP: 409

NoFreeAddressesInSubnet

Se devuelve si `IpAddress` no se especificó en la solicitud y no hay direcciones IP libres en la subred.

Código de estado HTTP: 409

SecurityGroupLimitExceeded

Se devuelve si el tamaño de `SecurityGroups` especificado en la solicitud es superior a cinco.

Código de estado HTTP: 400

SecurityGroupNotFound

Se devuelve si uno de los grupos de seguridad especificados no existe en la nube privada virtual (VPC) de la subred.

Código de estado HTTP: 400

SubnetNotFound

Se devuelve si no hay ninguna subred con el ID `SubnetId` proporcionado en la solicitud.

Código de estado HTTP: 400

UnsupportedAvailabilityZone

Se devuelve si la funcionalidad de Amazon EFS solicitada no está disponible en la zona de disponibilidad especificada.

Código de estado HTTP: 400

Ejemplos

Agregue un destino de montaje a un sistema de archivos

La siguiente solicitud crea un destino de montaje para un sistema de archivos. La solicitud especifica valores únicamente para los parámetros `FileSystemId` y `SubnetId` obligatorios.

La solicitud no proporciona los parámetros `IpAddress` y `SecurityGroups` opcionales. Para `IpAddress`, la operación utiliza una de las direcciones IP disponibles en la subred especificada. Además, la operación utiliza el grupo de seguridad predeterminado asociado a la VPC para el `SecurityGroups`.

Solicitud de muestra

```
POST /2015-02-01/mount-targets HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T221118Z
Authorization: <...>
Content-Type: application/json
Content-Length: 160

{"SubnetId": "subnet-748c5d03", "FileSystemId": "fs-01234567"}
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 252

{
  "MountTargetId": "fsmt-55a4413c",
  "NetworkInterfaceId": "eni-01234567",
  "FileSystemId": "fs-01234567",
  "LifecycleState": "available",
  "SubnetId": "subnet-01234567",
  "OwnerId": "231243201240",
  "IpAddress": "172.31.22.183"
}
```

Agregue un destino de montaje a un sistema de archivos

La siguiente solicitud especifica todos los parámetros de la solicitud para crear un destino de montaje.

Solicitud de muestra

```
POST /2015-02-01/mount-targets HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
```

```
x-amz-date: 20140620T221118Z
Authorization: <...>
Content-Type: application/json
Content-Length: 160

{
  "FileSystemId":"fs-01234567",
  "SubnetId":"subnet-01234567",
  "IpAddress":"10.0.2.42",
  "SecurityGroups":[
    "sg-01234567"
  ]
}
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 252

{
  "OwnerId":"251839141158",
  "MountTargetId":"fsmt-9a13661e",
  "FileSystemId":"fs-01234567",
  "SubnetId":"subnet-fd04ff94",
  "LifecycleState":"available",
  "IpAddress":"10.0.2.42",
  "NetworkInterfaceId":"eni-1bcb7772"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateReplicationConfiguration

Crea una configuración de replicación que replica un sistema de archivos de EFS existente en un nuevo sistema de archivos de solo lectura. Para obtener más información, consulte [Replicación de Amazon EFS](#) en la Guía del usuario de Amazon EFS. La siguiente configuración de replicación básica especifica lo siguiente:

- Sistema de archivos de origen: el sistema de archivos de EFS que desea replicar. El sistema de archivos de origen no puede ser un sistema de archivos de destino en una configuración de replicación existente.
- Región de AWS — Región de AWS En el que se crea el sistema de archivos de destino. La replicación de Amazon EFS está disponible en todos los Regiones de AWS lugares en los que esté disponible EFS. Debe habilitarse la región. Para obtener más información, consulte [Administración Regiones de AWS](#) en la Guía de referencia de referencia AWS general.
- Configuración del sistema de archivos de destino: la configuración del sistema de archivos de destino en el que se replicará el sistema de archivos de origen. Solo puede haber un sistema de archivos de destino en una configuración de replicación.

Los parámetros de la configuración de replicación incluyen:

- ID del sistema de archivos: el ID del sistema de archivos de destino para la replicación. Si no se proporciona ningún ID, EFS crea un nuevo sistema de archivos con la configuración predeterminada. Para los sistemas de archivos existentes, la protección contra sobrescritura de la replicación del sistema de archivos debe estar deshabilitada. Para obtener más información, consulte [Replicación en un sistema de archivos existente](#).
- Zona de disponibilidad: si quiere que el sistema de archivos de destino utilice almacenamiento One Zone, debe especificar la zona de disponibilidad en la que crear el sistema de archivos. Para obtener más información, consulte [Tipos de sistemas de archivos de EFS](#) en la Guía del usuario de Amazon EFS.
- Cifrado: todos los sistemas de archivos de destino se crean con el cifrado en reposo activado. Puede especificar la clave AWS Key Management Service (AWS KMS) que se utiliza para cifrar el sistema de archivos de destino. Si no especifica una clave KMS, se utiliza la clave KMS administrada por el servicio para Amazon EFS.

Note

Después de crear el sistema de archivos, no se puede cambiar la clave KMS.

Para los nuevos sistemas de archivos de destino, las siguientes propiedades están configuradas de forma predeterminada:

- Modo de rendimiento: el modo de rendimiento del sistema de archivos de destino coincide con el del sistema de archivos de origen, a menos que el sistema de archivos de destino utilice el almacenamiento EFS One Zone. En ese caso, se utiliza el modo de rendimiento de uso general. El modo de rendimiento no se puede cambiar.
- Modo de rendimiento: el modo de rendimiento del sistema de archivos de destino coincide con el del sistema de archivos de origen. Después de crear el sistema de archivos, puede modificar el modo de rendimiento.
- administración del ciclo de vida: la administración del ciclo de vida no está habilitada en el sistema de archivos de destino. Una vez creado el sistema de archivos de destino, puede habilitar la administración del ciclo de vida.
- Copias de seguridad automáticas: las copias de seguridad diarias automáticas están habilitadas en el sistema de archivos de destino. Después de crear el sistema de archivos, puede cambiar esta configuración.

Para obtener más información, consulte [Replicación de Amazon EFS](#) en la Guía del usuario de Amazon EFS.

Sintaxis de la solicitud

```
POST /2015-02-01/file-systems/SourceFileSystemId/replication-configuration HTTP/1.1
Content-type: application/json
```

```
{
  "Destinations": [
    {
      "AvailabilityZoneName": "string",
      "FileSystemId": "string",
      "KmsKeyId": "string",
      "Region": "string"
    }
  ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

SourceFileSystemId

Especifica el sistema de archivos de Amazon EFS que desea replicar. Este sistema de archivos no puede ser un sistema de archivos de origen o de destino en otra configuración de replicación.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Destinations

Una gama de objetos de configuración de destino. Solo se admite un objeto de configuración de destino.

Tipo: matriz de objetos [DestinationToCreate](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "Destinations": [
    {
      "FileSystemId": "string",
      "LastReplicatedTimestamp": number,
      "Region": "string",
```

```
    "Status": "string"
  }
],
"OriginalSourceFileSystemArn": "string",
"SourceFileSystemArn": "string",
"SourceFileSystemId": "string",
"SourceFileSystemRegion": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

Describe cuándo se creó la configuración de replicación.

Tipo: marca temporal

Destinations

Una gama de objetos de destino. Solo se admite un objeto de destino.

Tipo: matriz de objetos [Destination](#)

OriginalSourceFileSystemArn

Nombre de recurso de Amazon (ARN) del sistema de archivos de EFS de origen original en la configuración de replicación.

Tipo: cadena

SourceFileSystemArn

Nombre de recurso de Amazon (ARN) del sistema de archivos de origen actual en la configuración de replicación.

Tipo: cadena

SourceFileSystemId

El ID del sistema de archivos de Amazon EFS de origen que se está replicando.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

SourceFileSystemRegion

El Región de AWS en el que se encuentra el sistema de archivos EFS de origen.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

ConflictException

Se devuelve si el sistema de archivos de origen de una replicación está cifrado pero el sistema de archivos de destino no está cifrado.

Código de estado HTTP: 409

FileSystemLimitExceeded

Se devuelve si ya Cuenta de AWS se ha creado el número máximo de sistemas de archivos permitidos por cuenta.

Código de estado HTTP: 403

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

IncorrectFileSystemLifeCycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no “disponible”.

Código de estado HTTP: 409

InsufficientThroughputCapacity

Se devuelve si no hay suficiente capacidad para aprovisionar un rendimiento adicional. Este valor puede devolverse al intentar crear un sistema de archivos en el modo de rendimiento aprovisionado, al intentar aumentar el rendimiento aprovisionado de un sistema de archivos existente o al intentar cambiar un sistema de archivos existente del modo de rendimiento de ráfaga al de rendimiento aprovisionado. Inténtelo de nuevo más tarde.

Código de estado HTTP: 503

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

ReplicationNotFound

Se devuelve si el sistema de archivos especificado no tiene una configuración de replicación.

Código de estado HTTP: 404

ThroughputLimitExceeded

Se devuelve si el modo de rendimiento o la cantidad de rendimiento aprovisionada no se pueden cambiar porque se ha alcanzado el límite de rendimiento de 1024 MiB/s.

Código de estado HTTP: 400

UnsupportedAvailabilityZone

Se devuelve si la funcionalidad de Amazon EFS solicitada no está disponible en la zona de disponibilidad especificada.

Código de estado HTTP: 400

ValidationException

Se devuelve si el AWS Backup servicio no está disponible en el lugar Región de AWS en el que se realizó la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateTags

Note

OBSOLETO: CreateTags está en desuso y no recibe mantenimiento. Para crear etiquetas para los recursos de EFS, utilice la acción [TagResource](#) de la API.

Crea o sobrescribe etiquetas asociadas a un sistema de archivos. Cada etiqueta es un par clave-valor. Si una clave de etiqueta especificada en la solicitud ya existe en el sistema de archivos, esta operación sobrescribe su valor con el valor proporcionado en la solicitud. Si añade la etiqueta Name al sistema de archivos, Amazon EFS la devuelve como respuesta a la operación [DescribeFileSystems](#).

Esta operación necesita permiso para la acción `elasticfilesystem:CreateTags`.

Sintaxis de la solicitud

```
POST /2015-02-01/create-tags/FileSystemId HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[FileSystemId](#)

El ID del sistema de archivos cuyas etiquetas desea modificar (cadena). Esta operación modifica únicamente las etiquetas, no el sistema de archivos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[Tags](#)

Una matriz de objetos Tag que añadir. Cada objeto Tag es un par clave-valor.

Tipo: matriz de objetos [Tag](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteAccessPoint

Elimina el punto de acceso especificado. Una vez completada la eliminación, los nuevos clientes ya no podrán conectarse a los puntos de acceso. Los clientes conectados al punto de acceso en el momento de la eliminación seguirán funcionando hasta que finalicen su conexión.

Esta operación necesita permisos para la acción `elasticfilesystem:DeleteAccessPoint`.

Sintaxis de la solicitud

```
DELETE /2015-02-01/access-points/AccessPointId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

AccessPointId

El ID del punto de acceso que desea eliminar.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

AccessPointNotFound

Se devuelve si el `AccessPointId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteFileSystem

Elimina un sistema de archivos, lo que corta de forma permanente el acceso a su contenido. Cuando regrese, el sistema de archivos ya no existe y no podrá acceder a ningún contenido del sistema de archivos eliminado.

Debe eliminar manualmente los destinos de montaje adjuntos a un sistema de archivos antes de poder eliminar un sistema de archivos de EFS. Este paso se realiza automáticamente cuando se utiliza la AWS consola para eliminar un sistema de archivos.

Note

No se puede eliminar un sistema de archivos que forme parte de una configuración de replicación de EFS. Debe eliminarse primero la configuración de replicación.

No se puede eliminar un sistema de archivos que esté en uso. Es decir, si el sistema de archivos tiene ningún destino de montaje, primero debe eliminarlo. Para obtener más información, consulte [DescribeMountTargets](#) y [DeleteMountTarget](#).

Note

La llamada DeleteFileSystem realiza vuelve mientras el estado del sistema de archivos siga siendo `deleting`. Puede comprobar el estado de eliminación del sistema de archivos llamando a la operación [DescribeFileSystems](#), que devuelve una lista de los sistemas de archivos de su cuenta. Si pasa el identificador del sistema de archivos o el token de creación del sistema de archivos eliminado, [DescribeFileSystems](#) devuelve un error `404 FileSystemNotFound`.

Esta operación necesita permisos para la acción `elasticfilesystem:DeleteFileSystem`.

Sintaxis de la solicitud

```
DELETE /2015-02-01/file-systems/FileSystemId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

FileSystemId

El ID del sistema de archivos que desea eliminar.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemInUse

Se devuelve si un sistema de archivos tiene objetivos de montaje.

Código de estado HTTP: 409

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Ejemplos

Eliminar un sistema de archivos

El siguiente ejemplo envía una solicitud DELETE al punto de conexión `file-systems` (`elasticfilesystem.us-west-2.amazonaws.com/2015-02-01/file-systems/fs-01234567`) para eliminar un sistema de archivos cuyo ID es `fs-01234567`.

Solicitud de muestra

```
DELETE /2015-02-01/file-systems/fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T233021Z
Authorization: <...>
```

Respuesta de ejemplo

```
HTTP/1.1 204 No Content
x-amzn-RequestId: a2d125b3-7ebd-4d6a-ab3d-5548630bff33
Content-Length: 0
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteFileSystemPolicy

Elimina el `FileSystemPolicy` del sistema de archivos especificado. `FileSystemPolicy` predeterminado entra en vigor una vez que se elimina la política existente. Para obtener más información acerca de la política del sistema de archivos predeterminada, consulte [Uso de políticas basadas en recursos con EFS](#).

Esta operación necesita permisos para la acción `elasticfilesystem:DeleteFileSystemPolicy`.

Sintaxis de la solicitud

```
DELETE /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[FileSystemId](#)

Especifica el sistema de archivos EFS del que se va a eliminar el `FileSystemPolicy`.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el FileSystemId valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

IncorrectFileSystemLifecycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no “disponible”.

Código de estado HTTP: 409

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

DeleteMountTarget

Elimina el destino de montaje especificado.

Esta operación rompe de manera forzada los montajes del sistema de archivos utilizando el destino de montaje que se está eliminando, lo que podría afectar a las instancias o a las aplicaciones que utilizan dichos montajes. Para evitar que las aplicaciones se interrumpan abruptamente, puede considerar la posibilidad de desmontar cualquier soporte del objetivo de montaje, si es posible. La operación también elimina la interfaz de red asociada. Es posible que se pierdan las escrituras no confirmadas, pero romper un objetivo de montaje mediante esta operación no daña el sistema de archivos en sí. El sistema de archivos que creó se mantiene. Puede montar una instancia de EC2 en su VPC mediante otro destino de montaje.

Esta operación requiere permisos para las siguientes acciones en el sistema de archivos:

- `elasticfilesystem>DeleteMountTarget`

Note

La llamada a `DeleteMountTarget` se devuelve mientras el estado del objetivo de montaje sigue siendo `deleting`. Puede comprobar la eliminación del objetivo de montaje llamando a la operación [DescribeMountTargets](#), que devuelve una lista de descripciones de los objetivos de montaje para el sistema de archivos en cuestión.

La operación también requiere permisos para la siguiente acción de Amazon EC2 en la interfaz de red del destino de montaje:

- `ec2>DeleteNetworkInterface`

Sintaxis de la solicitud

```
DELETE /2015-02-01/mount-targets/MountTargetId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MountTargetId

El ID del destino de montaje que se elimina (cadena).

Limitaciones de longitud: longitud mínima de 13. Longitud máxima de 45.

Patrón: `^fsmt-[0-9a-f]{8,40}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

DependencyTimeout

Se agotó el tiempo de espera del servicio al intentar tramitar la solicitud y el cliente debería volver a intentar realizar la llamada.

Código de estado HTTP: 504

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

MountTargetNotFound

Se devuelve si no hay un objetivo de montaje con el ID especificado que se encontró en la Cuenta de AWS de la persona que llama.

Código de estado HTTP: 404

Ejemplos

Eliminar el objetivo de montaje de un sistema de archivos

El siguiente ejemplo envía una solicitud DELETE para eliminar un destino de montaje específico.

Solicitud de muestra

```
DELETE /2015-02-01/mount-targets/fsmt-9a13661e HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T232908Z
Authorization: <...>
```

Respuesta de ejemplo

```
HTTP/1.1 204 No Content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteReplicationConfiguration

Elimina una configuración de replicación. La eliminación de una configuración de replicación finaliza el proceso de replicación. Tras eliminar una configuración de replicación, se puede escribir en el sistema de archivos de destino y se vuelve a habilitar su protección contra sobrescritura de la replicación. Para obtener más información, consulte [Eliminación de una configuración de replicación](#).

Esta operación necesita permisos para la acción `elasticfilesystem:DeleteReplicationConfiguration`.

Sintaxis de la solicitud

```
DELETE /2015-02-01/file-systems/SourceFileSystemId/replication-configuration HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[SourceFileSystemId](#)

El ID del sistema de archivos de origen en la configuración de replicación.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el FileSystemId valor especificado no existe en la del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

ReplicationNotFound

Se devuelve si el sistema de archivos especificado no tiene una configuración de replicación.

Código de estado HTTP: 404

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

DeleteTags

Note

OBSOLETO: DeleteTags está en desuso y no recibe mantenimiento. Para quitar etiquetas de recursos de EFS, utilice la acción de la API [UntagResource](#).

Elimina las etiquetas especificadas de un sistema de archivos. Si la solicitud DeleteTags incluye una clave de etiqueta que no existe, Amazon EFS la ignora y no provoca ningún error. Para obtener más información sobre las etiquetas y las restricciones relacionadas, consulte [Restricciones de etiquetas](#) en la Guía del AWS Billing and Cost Management usuario.

Esta operación necesita permisos para la acción `elasticfilesystem:DeleteTags`.

Sintaxis de la solicitud

```
POST /2015-02-01/delete-tags/FileSystemId HTTP/1.1
Content-type: application/json

{
  "TagKeys": [ "string" ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[FileSystemId](#)

El ID del sistema de archivos cuyas etiquetas desea eliminar(cadena).

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[TagKeys](#)

Una lista de las claves de etiqueta que se eliminarán.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: $^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_\p{.}:/=+\-@]+)\$$

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeAccessPoints

Devuelve la descripción de un punto de acceso de Amazon EFS específico, si se proporciona `AccessPointId`. Si proporciona un `FileSystemId` de EFS, devuelve descripciones de todos los puntos de acceso de ese sistema de archivos. Puede proporcionar un `AccessPointId` o un `FileSystemId` en la solicitud, pero no ambos.

Esta operación necesita permisos para la acción `elasticfilesystem:DescribeAccessPoints`.

Sintaxis de la solicitud

```
GET /2015-02-01/access-points?  
AccessPointId=AccessPointId&FileSystemId=FileSystemId&MaxResults=MaxResults&NextToken=NextToken  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

AccessPointId

(Opcional) Especifica un punto de acceso de EFS para describirlo en la respuesta; se excluye mutuamente con `FileSystemId`.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

FileSystemId

(Opcional) Si proporciona un `FileSystemId`, EFS devuelve todos los puntos de acceso de ese sistema de archivos; se excluyen mutuamente con `AccessPointId`.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[MaxResults](#)

(Opcional) Al recuperar los puntos de acceso de un sistema de archivos, si lo desea, puede especificar el parámetro `MaxItems` para limitar el número de objetos devueltos en una respuesta. El valor predeterminado es 100.

Rango válido: valor mínimo de 1.

[NextToken](#)

`NextToken` está presente si la respuesta está paginada. Puede utilizar `NextMarker` en la solicitud subsiguiente para obtener la siguiente página de descripciones del punto de acceso.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `.+`

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "AccessPoints": [
    {
      "AccessPointArn": "string",
      "AccessPointId": "string",
      "ClientToken": "string",
      "FileSystemId": "string",
      "LifecycleState": "string",
      "Name": "string",
      "OwnerId": "string",
      "PosixUser": {
        "Gid": number,
        "SecondaryGids": [ number ],
        "Uid": number
      },
      "RootDirectory": {
```

```
    "CreationInfo": {
      "OwnerGid": number,
      "OwnerUid": number,
      "Permissions": "string"
    },
    "Path": "string"
  },
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
],
"NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AccessPoints](#)

Un conjunto de descripciones de puntos de acceso.

Tipo: matriz de objetos [AccessPointDescription](#)

[NextToken](#)

Está presente si hay más puntos de acceso de los que se devuelven en la respuesta. Puede utilizarlos NextMarker en la solicitud posterior para obtener las descripciones adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

Errores

AccessPointNotFound

Se devuelve si el `AccessPointId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)

- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeAccountPreferences

Devuelve la configuración de preferencias de la cuenta Cuenta de AWS asociada al usuario que realiza la solicitud, en la versión actual Región de AWS.

Sintaxis de la solicitud

```
GET /2015-02-01/account-preferences HTTP/1.1
Content-type: application/json

{
  "MaxResults": number,
  "NextToken": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[MaxResults](#)

(Opcional) Al recuperar las preferencias de la cuenta, si lo desea, puede especificar el parámetro `MaxItems` para limitar el número de objetos devueltos en una respuesta. El valor predeterminado es 100.

Tipo: entero

Rango válido: valor mínimo de 1.

Obligatorio: no

[NextToken](#)

(Opcional) Puedes usar `NextToken` en una solicitud posterior para buscar la siguiente página de preferencias de la Cuenta de AWS si la carga útil de la respuesta estaba paginada.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "ResourceIdPreference": {
    "ResourceIdType": "string",
    "Resources": [ "string" ]
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

Está presente si hay más registros de los que se devuelven en la respuesta. Se puede utilizar NextToken en la solicitud subsiguiente para obtener las descripciones adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

[ResourceIdPreference](#)

Describe la configuración de preferencias del identificador de recurso Cuenta de AWS asociado al usuario que realiza la solicitud, en el estado actual Región de AWS.

Tipo: objeto [ResourceIdPreference](#)

Errores

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeBackupPolicy

Devuelve la política de copias de seguridad del sistema de archivos de EFS especificado.

Sintaxis de la solicitud

```
GET /2015-02-01/file-systems/FileSystemId/backup-policy HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[FileSystemId](#)

Especifica el sistema de archivos de EFS para el que se va a recuperar la BackupPolicy.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPolicy": {
    "Status": "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPolicy](#)

Describe la política de copias de seguridad del sistema de archivos e indica si las copias de seguridad automáticas están activadas o desactivadas.

Tipo: objeto [BackupPolicy](#)

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

PolicyNotFound

Se devuelve si la política del sistema de archivos predeterminada está vigente para el sistema de archivos de EFS especificado.

Código de estado HTTP: 404

ValidationException

Se devuelve si el AWS Backup servicio no está disponible en el lugar Región de AWS en el que se realizó la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeFileSystemPolicy

Devuelve la `FileSystemPolicy` del sistema de archivos de EFS especificado.

Esta operación necesita permisos para la acción `elasticfilesystem:DescribeFileSystemPolicy`.

Sintaxis de la solicitud

```
GET /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[FileSystemId](#)

Especifica el sistema de archivos EFS del que se va a recuperar el `FileSystemPolicy`.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "FileSystemId": "string",
  "Policy": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

FileSystemId

Especifica el sistema de archivos de EFS al que se aplica la `FileSystemPolicy`.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Policy

`FileSystemPolicy` con formato JSON para el sistema de archivos de EFS.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 20 000.

Patrón: `[\s\S]+`

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

PolicyNotFound

Se devuelve si la política del sistema de archivos predeterminada está vigente para el sistema de archivos de EFS especificado.

Código de estado HTTP: 404

Ejemplos

Ejemplo

Este ejemplo ilustra un uso de DescribeFileSystemPolicy.

Solicitud de muestra

```
GET /2015-02-01/file-systems/fs-01234567/policy HTTP/1.1
```

Respuesta de ejemplo

```
{
  "FileSystemId": "fs-01234567",
  "Policy": "{
    "Version": "2012-10-17",
    "Id": "efs-policy-wizard-cdef0123-aaaa-6666-5555-444455556666",
    "Statement": [
      {
        "Sid": "efs-statement-abcdef01-1111-bbbb-2222-111122224444",
        "Effect" : "Deny",
        "Principal": {
          "AWS": "*"
        },
        "Action": "*",
        "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-
system/fs-01234567",
        "Condition": {
          "Bool": {
            "aws:SecureTransport": "false"
          }
        }
      }
    ]
  }
```

```
        }
      },
    },
    {
      "Sid": "efs-statement-01234567-aaaa-3333-4444-111122223333",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Resource" : "arn:aws:elasticfilesystem:us-east-2:111122223333:file-
system/fs-01234567"
    }
  ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeFileSystems

Devuelve la descripción de un sistema de archivos de Amazon EFS específico si se proporciona `CreationToken` o `FileSystemId` del sistema de archivos. De lo contrario, devuelve las descripciones de todos los sistemas de archivos propiedad de la persona que llama Cuenta de AWS en el Región de AWS punto final al que llamas.

Al recuperar todas las descripciones de los sistemas de archivos, si lo desea, puede especificar el parámetro `MaxItems` para limitar el número de descripciones en una respuesta. Este número se establece automáticamente en 100. Si quedan más descripciones de sistemas de archivos, Amazon EFS devuelve un `NextMarker`, un token opaco, en la respuesta. En este caso, debe enviar una solicitud posterior con el parámetro de solicitud `Marker` establecido en el valor de `NextMarker`.

Para recuperar una lista de las descripciones del sistema de archivos, esta operación se utiliza en un proceso iterativo, en el que `DescribeFileSystems` se llama primero sin el `Marker` y, a continuación, la operación continúa llamándola con el parámetro `Marker` establecido en el valor de `NextMarker` de la respuesta anterior hasta que la respuesta no tenga ningún `NextMarker`.

El orden de los sistemas de archivos devueltos en la respuesta a una llamada a `DescribeFileSystems` y el orden de los sistemas de archivos devueltos en las respuestas de una iteración de varias llamadas no están especificados.

Esta operación necesita permisos para la acción `elasticfilesystem:DescribeFileSystems`.

Sintaxis de la solicitud

```
GET /2015-02-01/file-systems?  
CreationToken=CreationToken&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

CreationToken

(Opcional) Restringe la lista al sistema de archivos con este identificador de creación (cadena). Al crear un sistema de archivos de Amazon EFS, se especifica un token de creación.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: . +

FileSystemId

(Opcional) ID del sistema de archivos cuya descripción desea recuperar (cadena).

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Marker

(Opcional) Un token de paginación opaco devuelto por una operación DescribeFileSystems anterior (cadena). Si está presente, especifica continuar la lista desde donde terminó la llamada de devolución.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: . +

MaxItems

(Opcional) Especifica el número máximo de sistemas de archivos que se devuelven en una respuesta (integer). Este número se establece automáticamente en 100. La respuesta se pagina a 100 por página si tiene más de 100 sistemas de archivos.

Rango válido: valor mínimo de 1.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "FileSystems": [
    {
      "AvailabilityZoneId": "string",
      "AvailabilityZoneName": "string",
```

```

    "CreationTime": number,
    "CreationToken": "string",
    "Encrypted": boolean,
    "FileSystemArn": "string",
    "FileSystemId": "string",
    "FileSystemProtection": {
      "ReplicationOverwriteProtection": "string"
    },
    "KmsKeyId": "string",
    "LifeCycleState": "string",
    "Name": "string",
    "NumberOfMountTargets": number,
    "OwnerId": "string",
    "PerformanceMode": "string",
    "ProvisionedThroughputInMibps": number,
    "SizeInBytes": {
      "Timestamp": number,
      "Value": number,
      "ValueInArchive": number,
      "ValueInIA": number,
      "ValueInStandard": number
    },
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "ThroughputMode": "string"
  }
],
"Marker": "string",
"NextMarker": "string"
}

```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[FileSystems](#)

Conjunto de descripciones de sistemas de archivos.

Tipo: matriz de objetos [FileSystemDescription](#)

[Marker](#)

Está presente si el intermediario lo proporciona en la solicitud (cadena).

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

[NextMarker](#)

Está presente si hay más sistemas de archivos de los devueltos en la respuesta (cadena). Se puede utilizar `NextMarker` en la solicitud subsiguiente para obtener las descripciones.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Ejemplos

Recupere una lista de 10 sistemas de archivos

El siguiente ejemplo envía una solicitud GET al punto de conexión `file-systems` (`elasticfilesystem.us-west-2.amazonaws.com/2015-02-01/file-systems`). La solicitud especifica un parámetro de consulta `MaxItems` para limitar el número de descripciones del sistema de archivos a 10.

Solicitud de muestra

```
GET /2015-02-01/file-systems?MaxItems=10 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T191208Z
Authorization: <...>
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 499
{
  "FileSystems": [
    {
      "OwnerId": "251839141158",
      "CreationToken": "MyFileSystem1",
      "FileSystemId": "fs-01234567",
      "PerformanceMode": "generalPurpose",
      "CreationTime": "1403301078",
      "LifecycleState": "created",
      "Name": "my first file system",
      "NumberOfMountTargets": 1,
      "SizeInBytes": {
        "Timestamp": 1403301078,
        "Value": 29313618372,
        "ValueInArchive": 201156,
        "ValueInIA": 675432,
        "ValueInStandard": 29312741784
      }
    }
  ]
}
```

```
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLifecycleConfiguration

Devuelve el objeto `LifecycleConfiguration` actual para el sistema de archivos de Amazon EFS especificado. La administración del ciclo de vida usa el objeto `LifecycleConfiguration` para identificar cuándo se deben mover los archivos entre clases de almacenamiento. En el caso de un sistema de archivos sin un objeto `LifecycleConfiguration`, la llamada devuelve una matriz vacía en la respuesta.

Esta operación necesita permisos para la operación `elasticfilesystem:DescribeLifecycleConfiguration`.

Sintaxis de la solicitud

```
GET /2015-02-01/file-systems/FileSystemId/lifecycle-configuration HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

FileSystemId

El ID del sistema de archivos cuyo objeto `LifecycleConfiguration` desea recuperar (String).

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
```

```
"LifecyclePolicies": [  
  {  
    "TransitionToArchive": "string",  
    "TransitionToIA": "string",  
    "TransitionToPrimaryStorageClass": "string"  
  }  
]
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

LifecyclePolicies

Un conjunto de políticas de administración del ciclo de vida. EFS admite un máximo de una política por sistema de archivos.

Tipo: matriz de objetos [LifecyclePolicy](#)

Miembros de la matriz: número máximo de 3 elementos.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el FileSystemId valor especificado no existe en la del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Ejemplos

Recupera la configuración del ciclo de vida de un sistema de archivos

La siguiente solicitud recupera el objeto `LifecycleConfiguration` del sistema de archivos especificado.

Solicitud de muestra

```
GET /2015-02-01/file-systems/fs-01234567/lifecycle-configuration HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20181120T221118Z
Authorization: <...>
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
    x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
    Content-Type: application/json
    Content-Length: 86
{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "AFTER_270_DAYS"
    },
    {
      "TransitionToIA": "AFTER_14_DAYS"
    },
    {
      "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
    }
  ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeMountTargets

Devuelve las descripciones de todos los destinos de montaje actuales o un destino de montaje específico, de un sistema de archivos. Al solicitar todos los objetivos de montaje actuales, no se especifica el orden de los objetivos de montaje devueltos en la respuesta.

Esta operación requiere permisos para la acción `elasticfilesystem:DescribeMountTargets`, ya sea en el ID del sistema de archivos que especifique en `FileSystemId` o en el sistema de archivos del destino de montaje que especifique en `MountTargetId`.

Sintaxis de la solicitud

```
GET /2015-02-01/mount-targets?  
AccessPointId=AccessPointId&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems&MountTargetId=MountTargetId  
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[AccessPointId](#)

(Opcional) El ID del punto de acceso cuyos objetivos de montaje desea enumerar. Debe incluirse en la solicitud si un `FileSystemId` o `MountTargetId` no se han incluido en la solicitud. Acepta un ID de punto de acceso o un ARN como entrada.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

[FileSystemId](#)

(Opcional) ID del sistema de archivos cuyos objetivos de montaje desea enumerar (cadena). Debe incluirse en la solicitud si un `AccessPointId` o `MountTargetId` no se han incluido. Acepta un ID de sistema de archivos o un ARN como entrada.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Marker

(Opcional) Un token de paginación opaco devuelto por una operación `DescribeMountTargets` anterior (cadena). Si está presente, especifica continuar la lista desde donde terminó la llamada de devolución anterior.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `.+`

MaxItems

(Opcional) El número máximo de destinos de montaje que se devuelven en una respuesta. Actualmente, este número se establece automáticamente en 10 y el resto de valores se ignoran. La respuesta se pagina a 100 por página si tiene más de 100 destinos de montaje.

Rango válido: valor mínimo de 1.

MountTargetId

(Opcional) ID del objetivo de montaje que quiere describir (cadena). Debe incluirse en la solicitud si un `FileSystemId` no se ha incluido. Acepta un ID de destino de montaje o un ARN como entrada.

Limitaciones de longitud: longitud mínima de 13. Longitud máxima de 45.

Patrón: `^fsmt-[0-9a-f]{8,40}$`

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "Marker": "string",
  "MountTargets": [
    {
      "AvailabilityZoneId": "string",
      "AvailabilityZoneName": "string",
```

```
    "FileSystemId": "string",
    "IpAddress": "string",
    "LifecycleState": "string",
    "MountTargetId": "string",
    "NetworkInterfaceId": "string",
    "OwnerId": "string",
    "SubnetId": "string",
    "VpcId": "string"
  }
],
"NextMarker": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Marker

Si la solicitud incluía un `Marker`, la respuesta devuelve ese valor en este campo.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

MountTargets

Devuelve los objetivos de montaje del sistema de archivos como un conjunto de objetos `MountTargetDescription`.

Tipo: matriz de objetos [MountTargetDescription](#)

NextMarker

Si hay un valor, hay más objetivos de montaje que devolver. En una solicitud posterior, puede proporcionar `Marker` en su solicitud para recuperar el siguiente conjunto de objetivos de montaje.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: . +

Errores

AccessPointNotFound

Se devuelve si el `AccessPointId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

MountTargetNotFound

Se devuelve si no hay un objetivo de montaje con el ID especificado que se encontró en la Cuenta de AWS de la persona que llama.

Código de estado HTTP: 404

Ejemplos

Recupera las descripciones de los objetivos de montaje creados para un sistema de archivos

La siguiente solicitud recupera las descripciones de los objetivos de montaje creados para el sistema de archivos especificado.

Solicitud de muestra

```
GET /2015-02-01/mount-targets?FileSystemId=fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T191252Z
Authorization: <...>
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 357

{
  "MountTargets": [
    {
      "OwnerId": "251839141158",
      "MountTargetId": "fsmt-01234567",
      "FileSystemId": "fs-01234567",
      "SubnetId": "subnet-01234567",
      "LifecycleState": "added",
      "IpAddress": "10.0.2.42",
      "NetworkInterfaceId": "eni-1bcb7772"
    }
  ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)

- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeMountTargetSecurityGroups

Devuelve los grupos de seguridad actualmente en vigor de un destino de montaje. Esta operación requiere que se haya creado la interfaz de red del objetivo de montaje y que no el estado del ciclo de vida del destino de montaje no sea `deleted`.

Esta operación necesita permisos para las siguientes acciones:

- Acción de `elasticfilesystem:DescribeMountTargetSecurityGroups` en el sistema de archivos del objetivo de montaje.
- Acción de `ec2:DescribeNetworkInterfaceAttribute` en la interfaz de red del objetivo de montaje.

Sintaxis de la solicitud

```
GET /2015-02-01/mount-targets/MountTargetId/security-groups HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MountTargetId

El ID del objetivo de montaje cuyos grupos de seguridad desea recuperar.

Limitaciones de longitud: longitud mínima de 13. Longitud máxima de 45.

Patrón: `^fsmt-[0-9a-f]{8,40}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200  
Content-type: application/json
```



```
{  
  "SecurityGroups": [ "string" ]  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

SecurityGroups

Un conjunto de grupos de seguridad

Tipo: matriz de cadenas

Miembros de la matriz: número máximo de 100 elementos.

Limitaciones de longitud: longitud mínima de 11. Longitud máxima de 43.

Patrón: `^sg-[0-9a-f]{8,40}`

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

IncorrectMountTargetState

Se devuelve si el objetivo de montaje no tiene el estado correcto para la operación.

Código de estado HTTP: 409

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

MountTargetNotFound

Se devuelve si no hay un objetivo de montaje con el ID especificado que se encontró en la Cuenta de AWS de la persona que llama.

Código de estado HTTP: 404

Ejemplos

Recuperar grupos de seguridad en vigor de un sistema de archivos

El siguiente ejemplo recupera los grupos de seguridad vigentes para la interfaz de red asociada a un objetivo de montaje.

Solicitud de muestra

```
GET /2015-02-01/mount-targets/fsmt-9a13661e/security-groups HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T223513Z
Authorization: <...>
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Length: 57

{
  "SecurityGroups" : [
    "sg-188d9f74"
  ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)

- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeReplicationConfigurations

Recupera la configuración de replicación de un sistema de archivos específico. Si no se especifica un sistema de archivos, se recuperan todas las configuraciones de replicación del Cuenta de AWS in Región de AWS an.

Sintaxis de la solicitud

```
GET /2015-02-01/file-systems/replication-configurations?  
FileSystemId=FileSystemId&MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[FileSystemId](#)

Puede recuperar la configuración de replicación de un sistema de archivos específico proporcionando su ID de sistema de archivos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[MaxResults](#)

(Opcional) Puede especificar el parámetro `MaxItems` para limitar el número de objetos devueltos en una respuesta. El valor predeterminado es 100.

Rango válido: valor mínimo de 1.

[NextToken](#)

`NextToken` está presente si la respuesta está paginada. Se puede utilizar `NextToken` en una solicitud posterior para buscar la siguiente página de resultados.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `.+`

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Replications": [
    {
      "CreationTime": number,
      "Destinations": [
        {
          "FileSystemId": "string",
          "LastReplicatedTimestamp": number,
          "Region": "string",
          "Status": "string"
        }
      ],
      "OriginalSourceFileSystemArn": "string",
      "SourceFileSystemArn": "string",
      "SourceFileSystemId": "string",
      "SourceFileSystemRegion": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Se puede utilizar NextToken de la respuesta anterior en la solicitud subsiguiente para obtener las descripciones adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: . +

Replications

El conjunto de configuraciones de replicación que se devuelve.

Tipo: matriz de objetos [ReplicationConfigurationDescription](#)

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

ReplicationNotFound

Se devuelve si el sistema de archivos especificado no tiene una configuración de replicación.

Código de estado HTTP: 404

ValidationException

Se devuelve si el AWS Backup servicio no está disponible en el lugar Región de AWS en el que se realizó la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeTags

Note

OBSOLETO: la acción `DescribeTags` está en desuso y no recibe mantenimiento. Para ver las etiquetas asociadas a los recursos de EFS, utilice la acción `ListTagsForResource` de la API.

Devuelve las etiquetas asociadas a un sistema de archivos. El orden de las etiquetas devueltas en la respuesta a una llamada a `DescribeTags` y el orden de las etiquetas devueltas en las respuestas de una iteración de varias llamadas (cuando se utiliza la paginación) no están especificados.

Esta operación necesita permisos para la acción `elasticfilesystem:DescribeTags`.

Sintaxis de la solicitud

```
GET /2015-02-01/tags/FileSystemId?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

FileSystemId

El ID del sistema de archivos cuya conjunto de etiquetas desea recuperar.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Marker

(Opcional) Un token de paginación opaco devuelto por una operación `DescribeTags` anterior (cadena). Si está presente, especifica continuar la lista desde donde terminó la llamada anterior.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: . +

[MaxItems](#)

(Opcional) El número máximo de etiquetas del sistema de archivos que se devuelven en una respuesta. Actualmente, este número se establece automáticamente en 100 y el resto de valores se ignoran. La respuesta se pagina a 100 por página si tiene más de 100 etiquetas.

Rango válido: valor mínimo de 1.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "Marker": "string",
  "NextMarker": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Marker](#)

Si la solicitud incluía un `Marker`, la respuesta devuelve ese valor en este campo.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

[NextMarker](#)

Si hay un valor, hay más etiquetas que devolver. En una solicitud posterior, puede proporcionar el valor de `NextMarker` como valor del parámetro `Marker` en la siguiente solicitud para recuperar el siguiente conjunto de etiquetas.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

[Tags](#)

Devuelve las etiquetas asociadas al sistema de archivos como un conjunto de objetos `Tag`.

Tipo: matriz de objetos [Tag](#)

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Ejemplos

Recuperar etiquetas asociadas a un sistema de archivos

La siguiente solicitud recupera etiquetas (pares de clave-valor) asociadas al sistema de archivos especificado.

Solicitud de muestra

```
GET /2015-02-01/tags/fs-01234567/ HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T215404Z
Authorization: <...>
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 288

{
  "Tags": [
    {
      "Key": "Name",
      "Value": "my first file system"
    },
    {
      "Key": "Fleet",
      "Value": "Development"
    },
    {
      "Key": "Developer",
      "Value": "Alice"
    }
  ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListTagsForResource

Muestra una lista de todas las etiquetas de un recurso de EFS de nivel superior. Debe proporcionar el ID del recurso para el que quiera recuperar las etiquetas.

Esta operación necesita permisos para la acción `elasticfilesystem:DescribeAccessPoints`.

Sintaxis de la solicitud

```
GET /2015-02-01/resource-tags/ResourceId?MaxResults=MaxResults&NextToken=NextToken
HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MaxResults](#)

(Opcional) Especifica la cantidad máxima de objetos de etiqueta que se devuelven en la respuesta. El valor predeterminado es 100.

Rango válido: valor mínimo de 1.

[NextToken](#)

(Opcional) Puede usar `NextToken` en una solicitud posterior para buscar la siguiente página de descripciones de puntos de acceso si la carga útil de la respuesta estaba paginada.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `.+`

[ResourceId](#)

Especifica el recurso de EFS para el que desea recuperar las etiquetas. Puede recuperar etiquetas para los puntos de acceso y los sistemas de archivos de EFS mediante este punto de conexión de API.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

NextToken está presente si la carga útil de la respuesta está paginada. Puede utilizar NextToken en la solicitud subsiguiente para obtener la siguiente página de descripciones del punto de acceso.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: .+

[Tags](#)

Un conjunto de las etiquetas del recurso de EFS especificado.

Tipo: matriz de objetos [Tag](#)

Errores

AccessPointNotFound

Se devuelve si el `AccessPointId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ModifyMountTargetSecurityGroups

Modifica el conjunto de grupos de seguridad en vigor de un destino de montaje.

Al crear un destino de montaje, Amazon EFS también crea una nueva interfaz de red. Para obtener más información, consulte [CreateMountTarget](#). Esta operación reemplaza los grupos de seguridad vigentes para la interfaz de red asociada a un destino de montaje, por los SecurityGroups proporcionados en la solicitud. Esta operación requiere que se haya creado la interfaz de red del destino de montaje y que no el estado del ciclo de vida del destino de montaje no sea `deleted`.

La operación necesita permisos para las siguientes acciones:

- Acción de `elasticfilesystem:ModifyMountTargetSecurityGroups` en el sistema de archivos del objetivo de montaje.
- Acción de `ec2:ModifyNetworkInterfaceAttribute` en la interfaz de red del objetivo de montaje.

Sintaxis de la solicitud

```
PUT /2015-02-01/mount-targets/MountTargetId/security-groups HTTP/1.1
Content-type: application/json

{
  "SecurityGroups": [ "string" ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[MountTargetId](#)

El ID del objetivo de montaje cuyos grupos de seguridad desea modificar.

Limitaciones de longitud: longitud mínima de 13. Longitud máxima de 45.

Patrón: `^fsmt-[0-9a-f]{8,40}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

SecurityGroups

Un conjunto de hasta cinco ID de grupo de seguridad de la VPC.

Tipo: matriz de cadenas

Miembros de la matriz: número máximo de 100 elementos.

Limitaciones de longitud: longitud mínima de 11. Longitud máxima de 43.

Patrón: `^sg-[0-9a-f]{8,40}`

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

IncorrectMountTargetState

Se devuelve si el objetivo de montaje no tiene el estado correcto para la operación.

Código de estado HTTP: 409

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

MountTargetNotFound

Se devuelve si no hay un objetivo de montaje con el ID especificado que se encontró en la Cuenta de AWS de la persona que llama.

Código de estado HTTP: 404

SecurityGroupLimitExceeded

Se devuelve si el tamaño de SecurityGroups especificado en la solicitud es superior a cinco.

Código de estado HTTP: 400

SecurityGroupNotFound

Se devuelve si uno de los grupos de seguridad especificados no existe en la nube privada virtual (VPC) de la subred.

Código de estado HTTP: 400

Ejemplos

Sustituya los grupos de seguridad de un objetivo de montaje

El siguiente ejemplo sustituye los grupos de seguridad vigentes para la interfaz de red asociada a un destino de montaje.

Solicitud de muestra

```
PUT /2015-02-01/mount-targets/fsmt-9a13661e/security-groups HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T223446Z
Authorization: <...>
Content-Type: application/json
Content-Length: 57

{
  "SecurityGroups" : [
```

```
"sg-188d9f74"  
]  
}
```

Respuesta de ejemplo

```
HTTP/1.1 204 No Content  
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

PutAccountPreferences

Utilice esta operación para establecer la preferencia de la cuenta en la Región de AWS actual para utilizar identificadores de recursos largos de 17 caracteres (63 bits) o cortos de 8 caracteres (32 bits) para el nuevo sistema de archivos de EFS y montar los recursos de destino. Los cambios que realice no afectarán a todos los identificadores de recursos existentes. Puede establecer la preferencia de ID durante el período de suscripción a medida que EFS pasa a identificadores de recursos largos. Para obtener más información, consulte [Administración de los ID de recursos de Amazon EFS](#).

Note

A partir de octubre de 2021, recibirá un mensaje de error si intenta configurar la preferencia de la cuenta para utilizar el ID de recurso corto en formato de 8 caracteres. Póngase en contacto con el servicio de AWS asistencia si recibe un error y debe utilizar identificadores abreviados para el sistema de archivos y el montaje de los recursos de destino.

Sintaxis de la solicitud

```
PUT /2015-02-01/account-preferences HTTP/1.1
Content-type: application/json
```

```
{
  "ResourceIdType": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[ResourceIdType](#)

Especifica la preferencia de ID de recurso de EFS que se debe establecer para el usuario Cuenta de AWS Región de AWS, en la versión actual LONG_ID (17 caracteres) u SHORT_ID (8 caracteres).

Note

A partir de octubre de 2021, recibirá un error al establecer la preferencia de cuenta en SHORT_ID. Póngase en contacto con el servicio de AWS asistencia si recibe un error y debe utilizar identificadores abreviados para el sistema de archivos y el montaje de los recursos de destino.

Tipo: cadena

Valores válidos: LONG_ID | SHORT_ID

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "ResourceIdPreference": {
    "ResourceIdType": "string",
    "Resources": [ "string" ]
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ResourceIdPreference

Describe el tipo de recurso y su preferencia de ID para el usuario Cuenta de AWS, en la versión actual Región de AWS.

Tipo: objeto [ResourceIdPreference](#)

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

PutBackupPolicy

Actualiza la política de copias de seguridad del sistema de archivos. Utilice esta acción para iniciar o detener las copias de seguridad automáticas del sistema de archivos.

Sintaxis de la solicitud

```
PUT /2015-02-01/file-systems/FileSystemId/backup-policy HTTP/1.1
Content-type: application/json

{
  "BackupPolicy": {
    "Status": "string"
  }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

FileSystemId

Especifica el sistema de archivos de EFS para el que se debe actualizar la política de copias de seguridad.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupPolicy

La política de copias de seguridad incluida en la solicitud de PutBackupPolicy.

Tipo: objeto BackupPolicy

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPolicy": {
    "Status": "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[BackupPolicy](#)

Describe la política de copias de seguridad del sistema de archivos e indica si las copias de seguridad automáticas están activadas o desactivadas.

Tipo: objeto [BackupPolicy](#)

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el FileSystemId valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

IncorrectFileSystemLifecycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no “disponible”.

Código de estado HTTP: 409

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

ValidationException

Se devuelve si el AWS Backup servicio no está disponible en el lugar Región de AWS en el que se realizó la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

PutFileSystemPolicy

Aplica un `FileSystemPolicy` de Amazon EFS a un sistema de archivos de Amazon EFS. Una política de sistema de archivos es una política de IAM basada en recursos y puede contener varias declaraciones de política. Un sistema de archivos siempre tiene exactamente una política de sistema de archivos, que puede ser la política predeterminada o una política explícita establecida o actualizada mediante esta operación de API. Las políticas del sistema de archivos de EFS tienen un límite de 20 000 caracteres. Cuando se establece una política explícita, se anula la política predeterminada. Para obtener más información acerca de la política de sistema de archivos predeterminada, consulte [Política de sistema de archivos de EFS predeterminada](#).

Note

Las políticas del sistema de archivos de EFS tienen un límite de 20 000 caracteres.

Esta operación necesita permisos para la acción `elasticfilesystem:PutFileSystemPolicy`.

Sintaxis de la solicitud

```
PUT /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
Content-type: application/json

{
  "BypassPolicyLockoutSafetyCheck": boolean,
  "Policy": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

FileSystemId

El ID del sistema de archivos de EFS para el que se desea crear o actualizar `FileSystemPolicy`.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[BypassPolicyLockoutSafetyCheck](#)

(Opcional) Un valor booleano que especifica si se omite o no el control de seguridad de bloqueo de `FileSystemPolicy`. La comprobación de seguridad de bloqueo determina si la política de la solicitud bloqueará, o impedirá, que la entidad principal de seguridad de IAM que realiza la solicitud haga futuras solicitudes de `PutFileSystemPolicy` en este sistema de archivos. Establezca `BypassPolicyLockoutSafetyCheck` en `True` solo cuando pretenda evitar que la entidad principal de IAM que realiza la solicitud haga solicitudes posteriores de `PutFileSystemPolicy` en este sistema de archivos. El valor predeterminado es `False`.

Tipo: Booleano

Obligatorio: no

[Policy](#)

La `FileSystemPolicy` que está creando. Acepta una definición de política con formato JSON. Las políticas del sistema de archivos de EFS tienen un límite de 20 000 caracteres. Para obtener más información sobre los elementos que componen una política de sistema de archivos, consulte [Políticas basadas en recursos de Amazon EFS](#).

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 20 000.

Patrón: `[\s\S]+`

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
```

```
"FileSystemId": "string",  
"Policy": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

FileSystemId

Especifica el sistema de archivos de EFS al que se aplica la `FileSystemPolicy`.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Policy

`FileSystemPolicy` con formato JSON para el sistema de archivos de EFS.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 20 000.

Patrón: `[\s\S]+`

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

IncorrectFileSystemLifecycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no “disponible”.

Código de estado HTTP: 409

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

InvalidPolicyException

Se devuelve si `FileSystemPolicy` tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio. Se devuelve en el caso de un error en la comprobación de seguridad relacionada con el bloqueo de la política.

Código de estado HTTP: 400

Ejemplos

Crear un EFS `FileSystemPolicy`

La siguiente solicitud crea una `FileSystemPolicy` que permite a todos los AWS principales montar el sistema de archivos EFS especificado con permisos de lectura y escritura.

Solicitud de muestra

```
PUT /2015-02-01/file-systems/fs-01234567/file-system-policy HTTP/1.1
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Principal": {
        "AWS": ["*"]
      }
    }
  ],
}
```

```
    }  
  ]  
}
```

Respuesta de ejemplo

```
{  
  "Version": "2012-10-17",  
  "Id": "1",  
  "Statement": [  
    {  
      "Sid": "efs-statement-abcdef01-1111-bbbb-2222-111122224444",  
      "Effect": "Allow",  
      "Action": [  
        "elasticfilesystem:ClientMount",  
        "elasticfilesystem:ClientWrite"  
      ],  
      "Principal": {  
        "AWS": ["*"]  
      },  
      "Resource": "arn:aws:elasticfilesystem:us-east-1:1111222233334444:file-  
system/fs-01234567"  
    }  
  ]  
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

PutLifecycleConfiguration

Utilice esta acción para gestionar el almacenamiento de su sistema de archivos. A `LifecycleConfiguration` consta de uno o más objetos `LifecyclePolicy` que definen lo siguiente:

- **TransitionToIA:** Cuándo mover los archivos del sistema de archivos del almacenamiento principal (clase de almacenamiento Estándar) al almacenamiento de Acceso poco frecuente (IA).
- **TransitionToArchive:** Cuándo mover los archivos del sistema de archivos de su clase de almacenamiento actual (clase de almacenamiento IA o Estándar) al almacenamiento Archivado.

Los sistemas de archivos no pueden realizar la transición al almacenamiento Archivado antes de pasar al almacenamiento IA. Por lo tanto, `TransitionToArchive` debe configurarse o debe ser posterior a `TransitionTo IA`.

Note

La clase de almacenamiento Archive solo está disponible para los sistemas de archivos que utilizan el modo de rendimiento elástico y el modo de rendimiento de uso general.

- **TransitionToPrimaryStorageClass:** si se deben volver a mover los archivos del sistema de archivos al almacenamiento principal (clase de almacenamiento Estándar) una vez que se haya accedido a ellos en almacenamiento IA o Archivado.

Para obtener más información, consulte [Administración del almacenamiento del sistema de archivos](#).

Cada sistema de archivos de Amazon EFS admite una configuración de ciclo de vida, que se aplica a todos los archivos del sistema de archivos. Si ya existe un objeto `LifecycleConfiguration` para el sistema de archivos especificado, una llamada a `PutLifecycleConfiguration` modifica la configuración existente. Una llamada `PutLifecycleConfiguration` con una matriz `LifecyclePolicies` vacía en el cuerpo de la solicitud elimina cualquier otra `LifecycleConfiguration` existente. En la solicitud, especifique lo siguiente:

- El ID del sistema de archivos para el que va a habilitar, deshabilitar o modificar la administración del ciclo de vida.

- Una matriz `LifecyclePolicies` de objetos `LifecyclePolicy` que definen cuándo mover los archivos al almacenamiento de IA, al almacenamiento Archivado y de vuelta al almacenamiento principal.

Note

Amazon EFS requiere que cada objeto `LifecyclePolicy` tenga una sola transición, por lo que la matriz `LifecyclePolicies` debe estar estructurada con objetos `LifecyclePolicy` independientes. Para más información, consulte los ejemplos de solicitudes en la siguiente sección.

Esta operación necesita permisos para la operación `elasticfilesystem:PutLifecycleConfiguration`.

Para aplicar un `LifecycleConfiguration` objeto a un sistema de archivos cifrados, necesita los mismos AWS Key Management Service permisos que cuando creó el sistema de archivos cifrados.

Sintaxis de la solicitud

```
PUT /2015-02-01/file-systems/FileSystemId/lifecycle-configuration HTTP/1.1
Content-type: application/json
```

```
{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "string",
      "TransitionToIA": "string",
      "TransitionToPrimaryStorageClass": "string"
    }
  ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

FileSystemId

El ID del sistema de archivos para el que crea el objeto `LifecycleConfiguration` (cadena).

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[LifecyclePolicies](#)

Una matriz de objetos de `LifecyclePolicy` que definen el objeto del sistema de archivos de `LifecycleConfiguration`. Un `LifecycleConfiguration` objeto informa a la administración del ciclo de vida de lo siguiente:

- **TransitionToIA:** Cuándo mover los archivos del sistema de archivos del almacenamiento principal (clase de almacenamiento Estándar) al almacenamiento de Acceso poco frecuente (IA).
- **TransitionToArchive:** Cuándo mover los archivos del sistema de archivos de su clase de almacenamiento actual (clase de almacenamiento IA o Estándar) al almacenamiento Archivado.

Los sistemas de archivos no pueden realizar la transición al almacenamiento Archivado antes de pasar al almacenamiento IA. Por lo tanto, no `TransitionToArchive` debe configurarse o debe ser posterior a `TransitionTo IA`.

Note

La clase de almacenamiento Archive solo está disponible para los sistemas de archivos que utilizan el modo de rendimiento elástico y el modo de rendimiento de uso general.

- **TransitionToPrimaryStorageClass:** si se deben volver a mover los archivos del sistema de archivos al almacenamiento principal (clase de almacenamiento Estándar) una vez que se haya accedido a ellos en almacenamiento IA o Archivado.

Note

Cuando se utiliza el comando `put-lifecycle-configuration` de la CLI o la acción `PutLifecycleConfiguration` de la API, Amazon EFS requiere que cada objeto `LifecyclePolicy` tenga una sola transición. Esto significa que en un órgano de solicitud, `LifecyclePolicies` debe estructurarse como una matriz de objetos `LifecyclePolicy`, un objeto para cada transición de almacenamiento. Para más información, consulte los ejemplos de solicitudes en la siguiente sección.

Tipo: matriz de objetos [LifecyclePolicy](#)

Miembros de la matriz: número máximo de 3 elementos.

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "string",
      "TransitionToIA": "string",
      "TransitionToPrimaryStorageClass": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LifecyclePolicies](#)

Un conjunto de políticas de administración del ciclo de vida. EFS admite un máximo de una política por sistema de archivos.

Tipo: matriz de objetos [LifecyclePolicy](#)

Miembros de la matriz: número máximo de 3 elementos.

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

IncorrectFileSystemLifecycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no “disponible”.

Código de estado HTTP: 409

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Ejemplos

Crear una configuración de ciclo de vida

En el siguiente ejemplo, se crea un objeto `LifecyclePolicy` mediante la acción `PutLifecycleConfiguration`. En este ejemplo se crea una política de ciclo de vida que indica a EFS que haga lo siguiente:

- Mover todos los archivos del sistema de archivos a los que no se haya accedido en almacenamiento Estándar en los últimos 30 días a la clase de almacenamiento IA.

- Mover todos los archivos del sistema de archivos a los que no se haya accedido en almacenamiento Estándar en los últimos 90 días a la clase de almacenamiento Archivado.
- Vuelva a mover los archivos al almacenamiento Estándar una vez que se haya accedido a ellos en almacenamiento IA o Archivado. La clase de almacenamiento Archive solo está disponible para los sistemas de archivos que utilizan el modo de rendimiento elástico y el modo de rendimiento de uso general.

Para obtener más información, consulte [Clases de almacenamiento de EFS](#) y [Administración del almacenamiento del sistema de archivos](#).

Solicitud de muestra

```
PUT /2015-02-01/file-systems/fs-0123456789abcdefb/lifecycle-configuration HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20181122T232908Z
Authorization: <...>
Content-type: application/json
Content-Length: 86
```

```
{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "AFTER_90_DAYS"
    },
    {
      "TransitionToIA": "AFTER_30_DAYS"
    },
    {
      "TransitionToPrimaryStorage": "AFTER_1_ACCESS"
    }
  ]
}
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-type: application/json
Content-Length: 86
```

```
{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "AFTER_90_DAYS"
    },
    {
      "TransitionToIA": "AFTER_30_DAYS"
    },
    {
      "TransitionToPrimaryStorage": "AFTER_1_ACCESS"
    }
  ]
}
```

Ejemplo de solicitud put-lifecycle-configuration CLI

Este ejemplo ilustra un uso de PutLifecycleConfiguration.

Solicitud de muestra

```
aws efs put-lifecycle-configuration \
  --file-system-id fs-0123456789abcdefb \
  --lifecycle-policies [{"TransitionToArchive":"AFTER_90_DAYS"},
  {"TransitionToIA":"AFTER_30_DAYS"},
  {"TransitionToPrimaryStorageClass":"AFTER_1_ACCESS"}]
  --region us-west-2 \
  --profile adminuser
```

Respuesta de ejemplo

```
{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "AFTER_90_DAYS"
    },
    {
      "TransitionToIA": "AFTER_30_DAYS"
    },
    {
      "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
    }
  ]
}
```

```
}
```

Deshabilitar la administración del ciclo de vida

En el siguiente ejemplo, se deshabilita la administración del ciclo de vida del sistema de archivos especificado.

Solicitud de muestra

```
PUT /2015-02-01/file-systems/fs-01234567/lifecycle-configuration HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20181122T232908Z
Authorization: <...>
Content-type: application/json
Content-Length: 86

{
  "LifecyclePolicies": [ ]
}
```

Respuesta de ejemplo

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-type: application/json
Content-Length: 86

{
  "LifecyclePolicies": [ ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)

- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

TagResource

Creación de una etiqueta para un recurso de EFS. Puede crear etiquetas para los puntos de acceso y los sistemas de archivos EFS mediante esta operación de API.

Esta operación necesita permisos para la acción `elasticfilesystem:TagResource`.

Sintaxis de la solicitud

```
POST /2015-02-01/resource-tags/ResourceId HTTP/1.1
Content-type: application/json
```

```
{
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ResourceId

El ID que especifica el recurso de EFS para el que desea crear una etiqueta.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Tags

Una matriz de objetos Tag que añadir. Cada objeto Tag es un par clave-valor.

Tipo: matriz de objetos [Tag](#)

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

AccessPointNotFound

Se devuelve si el `AccessPointId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Ejemplos

Crear etiquetas en un sistema de archivos

La siguiente solicitud crea tres etiquetas ("key1", "key2" y "key3") en el sistema de archivos especificado.

Solicitud de muestra

```
POST /2015-02-01/tag-resource/fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T221118Z
Authorization: <...>
Content-Type: application/json
Content-Length: 160
```

```
{
  "Tags": [
    {
      "Key": "key1",
      "Value": "value1"
    },
    {
      "Key": "key2",
      "Value": "value2"
    },
    {
      "Key": "key3",
      "Value": "value3"
    }
  ]
}
```

Respuesta de ejemplo

```
HTTP/1.1 204 no content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UntagResource

Elimina etiquetas de un recurso de EFS. Puede eliminar etiquetas para los puntos de acceso y los sistemas de archivos EFS mediante esta operación de API.

Esta operación necesita permisos para la acción `elasticfilesystem:UntagResource`.

Sintaxis de la solicitud

```
DELETE /2015-02-01/resource-tags/ResourceId?tagKeys=TagKeys HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[ResourceId](#)

Especifica el recurso de EFS para el que desea eliminar las etiquetas.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})$`

Obligatorio: sí

[TagKeys](#)

Las claves de los pares de etiquetas de clave-valor que se van a eliminar del recurso de EFS especificado.

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]+)$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

AccessPointNotFound

Se devuelve si el `AccessPointId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateFileSystem

Actualiza el modo de rendimiento o la cantidad de rendimiento aprovisionado de un sistema de archivos existente.

Sintaxis de la solicitud

```
PUT /2015-02-01/file-systems/FileSystemId HTTP/1.1
Content-type: application/json

{
  "ProvisionedThroughputInMibps": number,
  "ThroughputMode": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

FileSystemId

El ID del sistema de archivos que desea actualizar.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

ProvisionedThroughputInMibps

(Opcional) El rendimiento, medido en mebibytes por segundo (MiBps), que desea aprovisionar para el sistema de archivos que está creando. Obligatorio si `ThroughputMode` se establece en `provisioned`. Los valores válidos son del 1 al 3414 MiBps, y el límite superior depende de la región. Para aumentar este límite, póngase en contacto con AWS Support. Para obtener más

información, consulte [Cuotas de Amazon EFS que puede incrementar](#) en la Guía del usuario de Amazon EFS.

Tipo: Doble

Rango válido: valor mínimo de 1.0.

Obligatorio: no

ThroughputMode

(Opcional) Actualiza el modo de rendimiento del sistema de archivos. Si no va a actualizar el modo de rendimiento, no necesita proporcionar este valor en la solicitud. Si cambia ThroughputMode a provisioned, también debe establecer un valor para ProvisionedThroughputInMibps.

Tipo: cadena

Valores válidos: bursting | provisioned | elastic

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 202
Content-type: application/json

{
  "AvailabilityZoneId": "string",
  "AvailabilityZoneName": "string",
  "CreationTime": number,
  "CreationToken": "string",
  "Encrypted": boolean,
  "FileSystemArn": "string",
  "FileSystemId": "string",
  "FileSystemProtection": {
    "ReplicationOverwriteProtection": "string"
  },
  "KmsKeyId": "string",
  "LifecycleState": "string",
  "Name": "string",
  "NumberOfMountTargets": number,
```

```
"OwnerId": "string",
"PerformanceMode": "string",
"ProvisionedThroughputInMibps": number,
"SizeInBytes": {
  "Timestamp": number,
  "Value": number,
  "ValueInArchive": number,
  "ValueInIA": number,
  "ValueInStandard": number
},
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"ThroughputMode": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 202.

El servicio devuelve los datos siguientes en formato JSON.

AvailabilityZoneId

El identificador único y coherente de la zona de disponibilidad en la que se encuentra el sistema de archivos y solo es válido para los sistemas de archivos One Zone. Por ejemplo, use1-az1 es un identificador de zona de disponibilidad para el Región de AWS us-east-1 y tiene la misma ubicación en todas. Cuenta de AWS

Tipo: cadena

AvailabilityZoneName

Describe la zona de AWS disponibilidad en la que se encuentra el sistema de archivos y solo es válido para los sistemas de archivos de una zona. Para obtener más información, consulte [Uso de clases de almacenamiento de EFS](#) en la Guía del usuario de Amazon EFS.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: . +

CreationTime

Hora en que se creó el sistema de archivos, en segundos (desde 1970-01-01T 00:00:00 Z).

Tipo: marca temporal

CreationToken

La cadena opaca especificada en la solicitud.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: . +

Encrypted

Un valor booleano que, si es verdadero, indica que el sistema de archivos está cifrado.

Tipo: Booleano

FileSystemArn

Nombre de recurso de Amazon (ARN) para el sistema de archivos de EFS en el formato `arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id` . Ejemplo con datos de muestra: `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Tipo: cadena

FileSystemId

El ID del sistema de archivos, asignado por Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

FileSystemProtection

Describe la protección del sistema de archivos.

Tipo: objeto [FileSystemProtectionDescription](#)

[KmsKeyId](#)

El identificador de un sistema de archivos cifrado que AWS KMS key se utiliza para proteger el sistema de archivos cifrados.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

[LifecycleState](#)

La fase del ciclo de vida del sistema de archivos.

Tipo: cadena

Valores válidos: `creating | available | updating | deleting | deleted | error`

[Name](#)

Puede añadir etiquetas a un sistema de archivos, incluida una etiqueta Name. Para obtener más información, consulte [CreateFileSystem](#). Si el sistema de archivos tiene una etiqueta Name, Amazon EFS devuelve el valor de este campo.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 256.

Patrón: `^[\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*$`

[NumberOfMountTargets](#)

El número actual de destinos de montaje que tiene el sistema de archivos. Para obtener más información, consulte [CreateMountTarget](#).

Tipo: entero

Rango válido: valor mínimo de 0.

[OwnerId](#)

El Cuenta de AWS que creó el sistema de archivos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

[PerformanceMode](#)

El modo de desempeño del sistema de archivos.

Tipo: cadena

Valores válidos: `generalPurpose` | `maxIO`

[ProvisionedThroughputInMibps](#)

La cantidad de rendimiento aprovisionada, medida en MiBps, para el sistema de archivos. Válido para los sistemas de archivos que utilizan `ThroughputMode` establecido en `provisioned`.

Tipo: Doble

Rango válido: valor mínimo de 0.0.

[SizeInBytes](#)

El último tamaño medido conocido (en bytes) de los datos almacenados en el sistema de archivos, en su campo `Value`, y el momento en que se determinó ese tamaño en su campo `Timestamp`. El valor de `Timestamp` es el número entero de segundos transcurridos desde 1970-01-01T 00:00:00 Z. El valor de `SizeInBytes` no representa el tamaño de una instantánea coherente del sistema de archivos, pero en última instancia es coherente cuando no hay escrituras en el sistema de archivos. Es decir, `SizeInBytes` representa el tamaño real solo si el sistema de archivos no se modifica durante un período superior a un par de horas. De lo contrario, el valor no es el tamaño exacto que tenía el sistema de archivos en ningún momento.

Tipo: objeto [FileSystemSize](#)

[Tags](#)

Las etiquetas asociadas al sistema de archivos, presentadas como un conjunto de objetos `Tag`.

Tipo: matriz de objetos [Tag](#)

ThroughputMode

Muestra el modo de rendimiento de un sistema de archivos. Para obtener más información, consulte [Modos de rendimiento](#) en la Guía del usuario de Amazon EFS.

Tipo: cadena

Valores válidos: `bursting` | `provisioned` | `elastic`

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del solicitante. Cuenta de AWS

Código de estado HTTP: 404

IncorrectFileSystemLifecycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no "disponible".

Código de estado HTTP: 409

InsufficientThroughputCapacity

Se devuelve si no hay suficiente capacidad para aprovisionar un rendimiento adicional. Este valor puede devolverse al intentar crear un sistema de archivos en el modo de rendimiento aprovisionado, al intentar aumentar el rendimiento aprovisionado de un sistema de archivos existente o al intentar cambiar un sistema de archivos existente del modo de rendimiento de ráfaga al de rendimiento aprovisionado. Inténtelo de nuevo más tarde.

Código de estado HTTP: 503

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

ThroughputLimitExceeded

Se devuelve si el modo de rendimiento o la cantidad de rendimiento aprovisionada no se pueden cambiar porque se ha alcanzado el límite de rendimiento de 1024 MiB/s.

Código de estado HTTP: 400

TooManyRequests

Se devuelve si no esperas al menos 24 horas antes de cambiar el modo de rendimiento o reducir el valor del rendimiento aprovisionado.

Código de estado HTTP: 429

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateFileSystemProtection

Actualiza la protección del sistema de archivos.

Esta operación necesita permisos para la acción `elasticfilesystem:UpdateFileSystemProtection`.

Sintaxis de la solicitud

```
PUT /2015-02-01/file-systems/FileSystemId/protection HTTP/1.1
Content-type: application/json

{
  "ReplicationOverwriteProtection": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

[FileSystemId](#)

El ID del sistema de archivos que vaya a actualizar.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

[ReplicationOverwriteProtection](#)

El estado de la protección contra sobrescritura de la replicación del sistema de archivos.

- **ENABLED**: el sistema de archivos no puede utilizarse como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos se puede escribir. La protección contra sobrescritura de la replicación es **ENABLED** de forma predeterminada.

- **DISABLED**: el sistema de archivos puede utilizarse como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos es de solo lectura y solo puede modificarse mediante replicación de EFS.
- **REPLICATING**: el sistema de archivos se utiliza como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos es de solo lectura y solo se modifica mediante replicación de EFS.

Si se elimina la configuración de replicación, se vuelve a activar la protección contra sobrescritura de la replicación del sistema de archivos y se puede escribir en este.

Tipo: cadena

Valores válidos: ENABLED | DISABLED | REPLICATING

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
  "ReplicationOverwriteProtection": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[ReplicationOverwriteProtection](#)

El estado de la protección contra sobrescritura de la replicación del sistema de archivos.

- **ENABLED**: el sistema de archivos no puede utilizarse como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos se puede escribir. La protección contra sobrescritura de la replicación es **ENABLED** de forma predeterminada.
- **DISABLED**: el sistema de archivos puede utilizarse como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos es de solo lectura y solo puede modificarse mediante replicación de EFS.

- **REPLICATING**: el sistema de archivos se utiliza como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos es de solo lectura y solo se modifica mediante replicación de EFS.

Si se elimina la configuración de replicación, se vuelve a activar la protección contra sobrescritura de la replicación del sistema de archivos y se puede escribir en este.

Tipo: cadena

Valores válidos: **ENABLED** | **DISABLED** | **REPLICATING**

Errores

BadRequest

Se devuelve si la solicitud tiene un formato incorrecto o contiene un error, como un valor de parámetro no válido, o falta un parámetro obligatorio.

Código de estado HTTP: 400

FileSystemNotFound

Se devuelve si el `FileSystemId` valor especificado no existe en el del Cuenta de AWS solicitante.

Código de estado HTTP: 404

IncorrectFileSystemLifecycleState

Se devuelve si el estado del ciclo de vida del sistema de archivos es no “disponible”.

Código de estado HTTP: 409

InsufficientThroughputCapacity

Se devuelve si no hay suficiente capacidad para aprovisionar un rendimiento adicional. Este valor puede devolverse al intentar crear un sistema de archivos en el modo de rendimiento aprovisionado, al intentar aumentar el rendimiento aprovisionado de un sistema de archivos existente o al intentar cambiar un sistema de archivos existente del modo de rendimiento de ráfaga al de rendimiento aprovisionado. Inténtelo de nuevo más tarde.

Código de estado HTTP: 503

InternalServerError

Se devuelve si se ha producido un error en el servidor.

Código de estado HTTP: 500

ReplicationAlreadyExists

Se devuelve si el sistema de archivos ya está incluido en una configuración de replicación.>

Código de estado HTTP: 409

ThroughputLimitExceeded

Se devuelve si el modo de rendimiento o la cantidad de rendimiento aprovisionada no se pueden cambiar porque se ha alcanzado el límite de rendimiento de 1024 MiB/s.

Código de estado HTTP: 400

TooManyRequests

Se devuelve si no esperas al menos 24 horas antes de cambiar el modo de rendimiento o reducir el valor del rendimiento aprovisionado.

Código de estado HTTP: 429

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

Data Types

Los siguientes tipos de datos son compatibles:

- [AccessPointDescription](#)
- [BackupPolicy](#)
- [CreationInfo](#)
- [Destination](#)
- [DestinationToCreate](#)
- [FileSystemDescription](#)
- [FileSystemProtectionDescription](#)
- [FileSystemSize](#)
- [LifecyclePolicy](#)
- [MountTargetDescription](#)
- [PosixUser](#)
- [ReplicationConfigurationDescription](#)
- [ResourceIdPreference](#)
- [RootDirectory](#)
- [Tag](#)

AccessPointDescription

Proporciona una descripción de un punto de acceso del sistema de archivos de EFS.

Contenido

AccessPointArn

El nombre de recurso de Amazon (ARN) único asociado al punto de acceso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}$`

Obligatorio: no

AccessPointId

El ID del punto de acceso, asignado por Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

Obligatorio: no

ClientToken

La cadena opaca especificada en la solicitud para garantizar la creación de idempotentes.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `.+`

Obligatorio: no

FileSystemId

El ID del sistema de archivos de EFS al que se aplica el punto de acceso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: no

LifeCycleState

Identifica la fase del ciclo de vida del punto de acceso.

Tipo: cadena

Valores válidos: `creating | available | updating | deleting | deleted | error`

Obligatorio: no

Name

El nombre del punto de acceso. Este es el valor de la etiqueta Name.

Tipo: cadena

Requerido: no

OwnerId

Identifica al Cuenta de AWS propietario del recurso del punto de acceso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

Obligatorio: no

PosixUser

La identidad POSIX completa, incluido el ID de usuario, el ID de grupo y los ID de grupo secundarios en el punto de acceso que se utiliza para todas las operaciones de archivos por los clientes de NFS que utilizan el punto de acceso.

Tipo: objeto [PosixUser](#)

Obligatorio: no

RootDirectory

El directorio del sistema de archivos de EFS que el punto de acceso expone como directorio raíz a los clientes de NFS que utilizan el punto de acceso.

Tipo: objeto [RootDirectory](#)

Obligatorio: no

Tags

Las etiquetas asociadas al punto de acceso, presentadas como una matriz de objetos Tag.

Tipo: matriz de objetos [Tag](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

BackupPolicy

La política de copias de seguridad del sistema de archivos que se utiliza para crear copias de seguridad diarias automáticas. Si el estado tiene un valor de **ENABLED**, se realizará una copia de seguridad automática del sistema de archivos. Para obtener más información, consulte [Copias de seguridad automáticas](#).

Contenido

Status

Describe el estado de la política de copia de seguridad del sistema de archivos.

- **ENABLED** : EFS realiza automáticamente una copia de seguridad del sistema de archivos.
- **ENABLING** : EFS activa las copias de seguridad automáticas para el sistema de archivos.
- **DISABLED** : se desactivan las copias de seguridad automáticas para el sistema de archivos.
- **DISABLING** : EFS desactiva las copias de seguridad automáticas para el sistema de archivos.

Tipo: cadena

Valores válidos: **ENABLED** | **ENABLING** | **DISABLED** | **DISABLING**

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CreationInfo

Obligatorio si el `RootDirectory` especificado > `Path` no existe. Especifica los ID de POSIX y los permisos que se aplicarán al `RootDirectory` > `Path` del punto de acceso. Si el directorio raíz del punto de acceso no existe, EFS lo crea con esta configuración cuando un cliente se conecta al punto de acceso. Al especificar `CreationInfo`, debe incluir valores para todas las propiedades.

Amazon EFS crea un directorio raíz solo si ha proporcionado `CreationInfo`: `OwnUid`, `OwnGID` y los permisos para el directorio. Si no proporciona dicha información, Amazon EFS no creará el directorio raíz. Si el directorio raíz no existe, los intentos de montaje utilizando el punto de acceso fallarán.

Important

Si no proporciona `CreationInfo` y el `RootDirectory` especificado no existe, los intentos de montar el sistema de archivos utilizando el punto de acceso producirán un error.

Contenido

OwnerGid

Especifica el ID de grupo de POSIX que se va a aplicar a `RootDirectory`. Acepta valores de 0 a 2^{32} (4294967295).

Tipo: largo

Rango válido: valor mínimo de 0. Valor máximo de 4294967295.

Obligatorio: sí

OwnerUid

Especifica el ID de usuario de POSIX que se va a aplicar a `RootDirectory`. Acepta valores de 0 a 2^{32} (4294967295).

Tipo: largo

Rango válido: valor mínimo de 0. Valor máximo de 4294967295.

Obligatorio: sí

Permissions

Especifica los permisos de POSIX que se aplicarán a `RootDirectory`, en el formato de un número octal que representa los bits de modo del archivo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 4 caracteres.

Patrón: `^[0-7]{3,4}$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Destination

Describe el sistema de archivos de destino en la configuración de replicación.

Contenido

FileSystemId

El ID del sistema de archivos de Amazon EFS de destino.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

Region

Región de AWS En el que se encuentra el sistema de archivos de destino.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Obligatorio: sí

Status

Describe el estado del sistema de archivos de EFS de destino.

- El estado de Paused se produce como resultado de la exclusión voluntaria de la región de origen o destino después de crear la configuración de replicación. Para reanudar la replicación del sistema de archivos, debe volver a inscribirse en la Región de AWS. Para obtener más información, consulte [Administración Regiones de AWS](#) en la Guía de referencia AWS general.
- El estado de Error se produce cuando el sistema de archivos de origen o de destino (o ambos) se encuentra en un estado de error e irrecuperable. Para obtener más información, consulte [Supervisión de estado de replicación](#) en la Guía del usuario de Amazon EFS. Debe eliminar la configuración de replicación y, a continuación, restaurar la copia de seguridad más

reciente del sistema de archivos defectuoso (ya sea el de origen o el de destino) en un nuevo sistema de archivos.

Tipo: cadena

Valores válidos: ENABLED | ENABLING | DELETING | ERROR | PAUSED | PAUSING

Obligatorio: sí

LastReplicatedTimestamp

La hora en la que la sincronización más reciente se completó correctamente en el sistema de archivos de destino. Todos los cambios en los datos del sistema de archivos de origen que se hayan producido antes de esa hora se han replicado correctamente en el sistema de archivos de destino. Es posible que cualquier cambio que se haya producido después de este tiempo no se haya replicado por completo.

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

DestinationToCreate

Describe el sistema de archivos de destino nuevo o existente para la configuración de replicación.

Contenido

AvailabilityZoneName

Para crear un sistema de archivos que utilice el almacenamiento One Zone, especifique la zona de disponibilidad en la que desea crear el sistema de archivos.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: .+

Obligatorio: no

FileSystemId

El ID del sistema de archivos que se usa para el destino. La protección contra sobrescritura de la replicación del sistema de archivos debe estar deshabilitada. Si no proporciona un ID, EFS crea un nuevo sistema de archivos para el destino de la replicación.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: no

KmsKeyId

Especifique la clave AWS Key Management Service (AWS KMS) que desee utilizar para cifrar el sistema de archivos de destino. Si no especifica una clave de KMS, Amazon EFS utiliza su clave de KMS predeterminada para Amazon EFS, `/aws/elasticfilesystem`. Este ID puede tener uno de los siguientes formatos:

- ID de clave: un identificador único de la clave, por ejemplo `1234abcd-12ab-34cd-56ef-1234567890ab`.

- ARN: un nombre de recurso de Amazon (ARN) para la clave, por ejemplo `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- Alias de clave: un nombre de visualización creado con anterioridad para una clave, por ejemplo `alias/projectKey1`.
- ARN de alias de clave: un ARN para un alias de clave, por ejemplo `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-zA-Z0-9-]+\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

Obligatorio: no

Region

Para crear un sistema de archivos que utilice el almacenamiento regional, especifique Región de AWS en qué se va a crear el sistema de archivos de destino.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FileSystemDescription

Descripción del sistema de archivos.

Contenido

CreationTime

Hora en que se creó el sistema de archivos, en segundos (desde 1970-01-01T 00:00:00 Z).

Tipo: marca temporal

Obligatorio: sí

CreationToken

La cadena opaca especificada en la solicitud.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: .+

Obligatorio: sí

FileSystemId

El ID del sistema de archivos, asignado por Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

LifeCycleState

La fase del ciclo de vida del sistema de archivos.

Tipo: cadena

Valores válidos: `creating` | `available` | `updating` | `deleting` | `deleted` | `error`

Obligatorio: sí

NumberOfMountTargets

El número actual de destinos de montaje que tiene el sistema de archivos. Para obtener más información, consulte [CreateMountTarget](#).

Tipo: entero

Rango válido: valor mínimo de 0.

Obligatorio: sí

OwnerId

El Cuenta de AWS que creó el sistema de archivos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

Obligatorio: sí

PerformanceMode

El modo de desempeño del sistema de archivos.

Tipo: cadena

Valores válidos: `generalPurpose` | `maxIO`

Obligatorio: sí

SizeInBytes

El último tamaño medido conocido (en bytes) de los datos almacenados en el sistema de archivos, en su campo `Value`, y el momento en que se determinó ese tamaño en su campo `Timestamp`. El valor de `Timestamp` es el número entero de segundos transcurridos desde 1970-01-01T 00:00:00 Z. El valor de `SizeInBytes` no representa el tamaño de una instantánea coherente del sistema de archivos, pero en última instancia es coherente cuando no hay escrituras en el sistema de archivos. Es decir, `SizeInBytes` representa el tamaño real solo

si el sistema de archivos no se modifica durante un período superior a un par de horas. De lo contrario, el valor no es el tamaño exacto que tenía el sistema de archivos en ningún momento.

Tipo: objeto [FileSystemSize](#)

Obligatorio: sí

Tags

Las etiquetas asociadas al sistema de archivos, presentadas como un conjunto de objetos Tag.

Tipo: matriz de objetos [Tag](#)

Obligatorio: sí

AvailabilityZoneId

El identificador único y coherente de la zona de disponibilidad en la que se encuentra el sistema de archivos y solo es válido para los sistemas de archivos One Zone. Por ejemplo, use1-az1 es un identificador de zona de disponibilidad para el Región de AWS us-east-1 y tiene la misma ubicación en todas. Cuenta de AWS

Tipo: cadena

Requerido: no

AvailabilityZoneName

Describe la zona de AWS disponibilidad en la que se encuentra el sistema de archivos y solo es válido para los sistemas de archivos de una zona. Para obtener más información, consulte [Uso de clases de almacenamiento de EFS](#) en la Guía del usuario de Amazon EFS.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: .+

Obligatorio: no

Encrypted

Un valor booleano que, si es verdadero, indica que el sistema de archivos está cifrado.

Tipo: Booleano

Obligatorio: no

FileSystemArn

Nombre de recurso de Amazon (ARN) para el sistema de archivos de EFS en el formato `arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id` . Ejemplo con datos de muestra: `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Tipo: cadena

Requerido: no

FileSystemProtection

Describe la protección del sistema de archivos.

Tipo: objeto [FileSystemProtectionDescription](#)

Obligatorio: no

KmsKeyId

El identificador de un sistema de archivos cifrado que AWS KMS key se utiliza para proteger el sistema de archivos cifrados.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

Obligatorio: no

Name

Puede añadir etiquetas a un sistema de archivos, incluida una etiqueta Name. Para obtener más información, consulte [CreateFileSystem](#). Si el sistema de archivos tiene una etiqueta Name, Amazon EFS devuelve el valor de este campo.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 256.

Patrón: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Obligatorio: no

ProvisionedThroughputInMibps

La cantidad de rendimiento aprovisionada, medida en MiBps, para el sistema de archivos. Válido para los sistemas de archivos que utilizan `ThroughputMode` establecido en `provisioned`.

Tipo: Doble

Rango válido: valor mínimo de 1.0.

Obligatorio: no

ThroughputMode

Muestra el modo de rendimiento de un sistema de archivos. Para obtener más información, consulte [Modos de rendimiento](#) en la Guía del usuario de Amazon EFS.

Tipo: cadena

Valores válidos: `bursting` | `provisioned` | `elastic`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FileSystemProtectionDescription

Describe la protección del sistema de archivos.

Contenido

ReplicationOverwriteProtection

El estado de la protección contra sobrescritura de la replicación del sistema de archivos.

- **ENABLED:** el sistema de archivos no puede utilizarse como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos se puede escribir. La protección contra sobrescritura de la replicación es ENABLED de forma predeterminada.
- **DISABLED:** el sistema de archivos puede utilizarse como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos es de solo lectura y solo puede modificarse mediante replicación de EFS.
- **REPLICATING:** el sistema de archivos se utiliza como el sistema de archivos de destino en una configuración de replicación. El sistema de archivos es de solo lectura y solo se modifica mediante replicación de EFS.

Si se elimina la configuración de replicación, se vuelve a activar la protección contra sobrescritura de la replicación del sistema de archivos y se puede escribir en este.

Tipo: cadena

Valores válidos: ENABLED | DISABLED | REPLICATING

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FileSystemSize

El último tamaño medido conocido (en bytes) de los datos almacenados en el sistema de archivos, en su campo `Value`, y el momento en que se determinó ese tamaño en su campo `Timestamp`. El valor de no representa el tamaño de una instantánea coherente del sistema de archivos, pero en última instancia es coherente cuando no hay escrituras en el sistema de archivos. Es decir, el valor representa el tamaño real solo si el sistema de archivos no se modifica durante un período superior a un par de horas. De lo contrario, el valor no es necesariamente el tamaño exacto que tenía el sistema de archivos en un momento dado.

Contenido

Value

El último tamaño medido conocido (en bytes) de los datos almacenados en el sistema de archivos.

Tipo: largo

Rango válido: valor mínimo de 0.

Obligatorio: sí

Timestamp

Hora en la que se determinó el tamaño de los datos devueltos en el campo `Value`. El valor de es el número entero de segundos transcurridos desde 1970-01-01T 00:00:00 Z.

Tipo: marca temporal

Obligatorio: no

ValueInArchive

El último tamaño medido conocido (en bytes) de los datos almacenados en la clase de almacenamiento Archivado.

Tipo: largo

Rango válido: valor mínimo de 0.

Obligatorio: no

ValueInIA

El último tamaño medido conocido (en bytes) de los datos almacenados en la clase de almacenamiento Infrequent Access.

Tipo: largo

Rango válido: valor mínimo de 0.

Obligatorio: no

ValueInStandard

El último tamaño medido conocido (en bytes) de los datos almacenados en la clase de almacenamiento Standard.

Tipo: largo

Rango válido: valor mínimo de 0.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LifecyclePolicy

Describe una política utilizada por la administración del ciclo de vida que especifica cuándo hacer la transición de los archivos hacia y desde las clases de almacenamiento. Para obtener más información, consulte [Administración del almacenamiento del sistema de archivos](#).

Note

Cuando se utiliza el comando `put-lifecycle-configuration` de la CLI o la acción `PutLifecycleConfiguration` de la API, Amazon EFS requiere que cada objeto `LifecyclePolicy` tenga una sola transición. Esto significa que en un órgano de solicitud, `LifecyclePolicies` debe estructurarse como una matriz de objetos de `LifecyclePolicy`, un objeto para cada transición. Para obtener más información, consulte la solicitud de ejemplo en [PutLifecycleConfiguration](#).

Contenido

TransitionToArchive

El número de días transcurridos desde la última vez que se accedió a los archivos en el almacenamiento principal (la clase de almacenamiento Estándar) para moverlos al almacenamiento Archivado. Las operaciones de metadatos como enumerar el contenido de un directorio no cuentan como eventos de acceso a un archivo.

Tipo: cadena

Valores válidos: `AFTER_1_DAY` | `AFTER_7_DAYS` | `AFTER_14_DAYS` | `AFTER_30_DAYS` | `AFTER_60_DAYS` | `AFTER_90_DAYS` | `AFTER_180_DAYS` | `AFTER_270_DAYS` | `AFTER_365_DAYS`

Obligatorio: no

TransitionToIA

El número de días transcurridos desde la última vez que se accedió a los archivos en el almacenamiento principal (la clase de almacenamiento Estándar) para moverlos al almacenamiento de Acceso poco frecuente (IA). Las operaciones de metadatos como enumerar el contenido de un directorio no cuentan como eventos de acceso a un archivo.

Tipo: cadena

Valores válidos: AFTER_7_DAYS | AFTER_14_DAYS | AFTER_30_DAYS | AFTER_60_DAYS
| AFTER_90_DAYS | AFTER_1_DAY | AFTER_180_DAYS | AFTER_270_DAYS |
AFTER_365_DAYS

Obligatorio: no

TransitionToPrimaryStorageClass

Si se deben volver a mover los archivos al almacenamiento principal (estándar) después de acceder a ellos en el almacenamiento IA o Archivado. Las operaciones de metadatos como enumerar el contenido de un directorio no cuentan como eventos de acceso a un archivo.

Tipo: cadena

Valores válidos: AFTER_1_ACCESS

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

MountTargetDescription

Proporciona una descripción de un destino de montaje.

Contenido

FileSystemId

El ID del sistema de archivos para el que se crea el destino de montaje.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

LifeCycleState

Estado del ciclo de vida del destino de montaje.

Tipo: cadena

Valores válidos: `creating | available | updating | deleting | deleted | error`

Obligatorio: sí

MountTargetId

ID de destino de montaje asignado por el sistema.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 13. Longitud máxima de 45.

Patrón: `^fsmt-[0-9a-f]{8,40}$`

Obligatorio: sí

SubnetId

El ID de la subred del destino de montaje.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 80.

Patrón: `^subnet-[0-9a-f]{8,40}$`

Obligatorio: sí

AvailabilityZoneId

El identificador único y coherente de la zona de disponibilidad en la que reside el destino de montaje. Por ejemplo, `use1-az1` es un ID AZ para la región `us-east-1` y tiene la misma ubicación en todas. Cuenta de AWS

Tipo: cadena

Requerido: no

AvailabilityZoneName

El nombre de la zona de disponibilidad en la que se encuentra el destino de montaje. Las zonas de disponibilidad se asignan de forma independiente a los nombres de cada una de ellas. Cuenta de AWS Por ejemplo, es Cuenta de AWS posible que la zona `us-east-1a` de disponibilidad de su ubicación no sea la misma que la `us-east-1a` de otra Cuenta de AWS.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `.+`

Obligatorio: no

IpAddress

Dirección en la que se puede montar el sistema de archivos mediante el destino de montaje.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 7. Longitud máxima de 15.

Patrón: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Obligatorio: no

NetworkInterfaceId

El ID de la interfaz de red que creó Amazon EFS cuando creó el destino de montaje.

Tipo: cadena

Requerido: no

OwnerId

Cuenta de AWS ID propietario del recurso.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

Obligatorio: no

VpcId

El ID de la nube privada virtual (VPC) en la que está configurado el destino de montaje.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

PosixUser

La identidad POSIX completa, incluido el ID de usuario, el ID de grupo y cualquier ID de grupo secundario, en el punto de acceso que se utiliza para todas las operaciones del sistema de archivos realizadas por los clientes de NFS que utilizan el punto de acceso.

Contenido

Gid

El ID de grupo de POSIX utilizado para todas las operaciones del sistema de archivos que utilizan este punto de acceso.

Tipo: largo

Rango válido: valor mínimo de 0. Valor máximo de 4294967295.

Obligatorio: sí

Uid

El ID de usuario de POSIX utilizado para todas las operaciones del sistema de archivos que utilizan este punto de acceso.

Tipo: largo

Rango válido: valor mínimo de 0. Valor máximo de 4294967295.

Obligatorio: sí

SecondaryGids

Los ID de grupo de POSIX secundarios utilizados para todas las operaciones del sistema de archivos que utilizan este punto de acceso.

Tipo: matriz de longitudes

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 16 elementos.

Rango válido: valor mínimo de 0. Valor máximo de 4294967295.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReplicationConfigurationDescription

Describe la configuración de replicación de un sistema de archivos específico.

Contenido

CreationTime

Describe cuándo se creó la configuración de replicación.

Tipo: marca temporal

Obligatorio: sí

Destinations

Una gama de objetos de destino. Solo se admite un objeto de destino.

Tipo: matriz de objetos [Destination](#)

Obligatorio: sí

OriginalSourceFileSystemArn

Nombre de recurso de Amazon (ARN) del sistema de archivos de EFS de origen original en la configuración de replicación.

Tipo: cadena

Obligatorio: sí

SourceFileSystemArn

Nombre de recurso de Amazon (ARN) del sistema de archivos de origen actual en la configuración de replicación.

Tipo: cadena

Obligatorio: sí

SourceFileSystemId

El ID del sistema de archivos de Amazon EFS de origen que se está replicando.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatorio: sí

SourceFileSystemRegion

El Región de AWS en el que se encuentra el sistema de archivos EFS de origen.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ResourceIdPreference

Describe el tipo de recurso y su preferencia de ID para el usuario Cuenta de AWS, en el estado actual Región de AWS.

Contenido

ResourceIdType

Identifica la preferencia de ID de recurso de EFS, ya sea LONG_ID (17 caracteres) o SHORT_ID (8 caracteres).

Tipo: cadena

Valores válidos: LONG_ID | SHORT_ID

Obligatorio: no

Resources

Identifica los recursos de Amazon EFS a los que se aplica la configuración de preferencias de ID, FILE_SYSTEM y MOUNT_TARGET.

Tipo: matriz de cadenas

Valores válidos: FILE_SYSTEM | MOUNT_TARGET

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

RootDirectory

Especifica el directorio del sistema de archivos de Amazon EFS al que el punto de acceso proporciona acceso. El punto de acceso expone la ruta del sistema de archivos especificada como directorio raíz del sistema de archivos a las aplicaciones que utilizan el punto de acceso. Los clientes de NFS que utilizan el punto de acceso solo pueden acceder a los datos en los puntos de acceso `RootDirectory` y sus subdirectorios.

Contenido

CreationInfo

(Opcional) Especifica los ID de POSIX y los permisos que se van a aplicar a los puntos de acceso `RootDirectory`. Si `RootDirectory` especificado > `Path` no existe, EFS crea el directorio raíz utilizando la configuración de `CreationInfo` cuando un cliente se conecta a un punto de acceso. Al especificar `CreationInfo`, debe proporcionar valores para todas las propiedades.

Important

Si no proporciona `CreationInfo` y `RootDirectory` especificado > `Path` no existe, los intentos de montar el sistema de archivos utilizando el punto de acceso producirán un error.

Tipo: objeto [CreationInfo](#)

Obligatorio: no

Path

Especifica la ruta en el sistema de archivos de EFS que se va a exponer como directorio raíz a los clientes de NFS mediante el punto de acceso para acceder al sistema de archivos de EFS. Una ruta puede tener hasta cuatro subdirectorios. Si la ruta de acceso especificada no existe, deberá proporcionar `CreationInfo`.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^(\\|\\(?:!\\.)+[^\$#<>;`|&?{}^*\/\n]+){1,4}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Tag

Una etiqueta es un par clave-valor. Los caracteres permitidos son letras, espacios en blanco y números que se pueden representar en UTF-8, y los siguientes caracteres: + - = . _ : /.

Contenido

Key

La clave de la etiqueta (cadena). La clave no pueden comenzar por aws :.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Obligatorio: sí

Value

El valor de la clave de etiqueta.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 256.

Patrón: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Historial de documentos

- Versión de la API: 01-02-2015
- Última actualización de la documentación: 15 de mayo de 2024

En la siguiente tabla se describen los cambios importantes en la Guía del usuario de sistema de archivos elástico de Amazon a partir de julio de 2018. Para obtener notificaciones sobre las actualizaciones de la documentación, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
Se aumentó la cuota de objetivos de montura	El número máximo de objetivos de montaje para cada nube privada virtual (VPC) aumentó de 400 a 1400. Para obtener más información, consulte las cuotas de recursos de Amazon EFS que no puede cambiar .	15 de mayo de 2024
Se aumentó el límite de rendimiento combinado para los sistemas de archivos de Elastic	El rendimiento máximo combinado de lectura y escritura es de 1500 MiBps para los sistemas de archivos que utilizan Elastic Throughput y se montan con la versión 2.0 o posterior del cliente Amazon EFS (amazon-efs-utils versión) o el controlador CSI de Amazon EFS (aws-efs-csi-driver). Para obtener más información, consulte la tabla de resumen del rendimiento de Amazon EFS .	30 de abril de 2024

[Se ha incrementado el límite de rendimiento de Elastic](#)

El límite de rendimiento elástico ha aumentado en algunos casos. Regiones de AWS Para obtener más información, consulte [Rendimiento elástico total predeterminado para todos los clientes conectados en](#) cada uno de ellos. Región de AWS

13 de marzo de 2024

[IOPS mayor](#)

Los sistemas de archivos que utilizan Elastic Throughput pueden generar un máximo de 90 000 lecturas para los datos a los que se accede con poca frecuencia. Para obtener más información, consulte [Resumen de rendimiento.](#)

22 de enero de 2024

[Se actualizó la política gestionada existente AWS](#)

elasticfilesystem: UpdateFileSystemProtection Se agregó un permiso a la AmazonElasticFileSystemFullAccess política existente para permitir a los directores actualizar la protección en un sistema de archivos. Para obtener más información, consulte [Actualizaciones de Amazon EFS a las políticas AWS gestionadas.](#)

27 de noviembre de 2023

[Replicar en el sistema de archivos existente](#)

Ya se pueden replicar sistemas de archivos en los sistemas existentes, lo que facilita la sincronización de cambios entre los sistemas de archivos con fines de conmutación por recuperación. Para obtener más información, consulte [Sistemas de archivos de destino](#).

27 de noviembre de 2023

[Se agregó protección del sistema de archivos](#)

La protección contra sobrescritura de la replicación se ha agregado a los sistemas de archivos y está habilitada de forma predeterminada. La protección evita que los sistemas de archivos se utilicen como destino en una configuración de replicación. Para obtener más información, consulte [Protección del sistema de archivos](#).

27 de noviembre de 2023

[Nueva clase de almacenamiento, tipos de sistemas de archivos y política de ciclo de vida](#)

Amazon EFS ahora ofrece la clase de almacenamiento Archivado de EFS, tipos de sistemas de archivos y la política de ciclo de vida de Transición a Archivado. Para obtener más información, consulte [Tipos de sistemas de archivos y clases de almacenamiento](#).

26 de noviembre de 2023

[IOPS mayor](#)

Los sistemas de archivos de rendimiento elástico ahora admiten un máximo de 65 000 IOPS de operaciones de lectura y 50 000 operaciones de escritura para los datos a los que se accede con poca frecuencia, y también admiten 250 000 IOPS de lectura para los datos a los que se accede con frecuencia. Para obtener más información, consulte [Resumen de rendimiento](#).

26 de noviembre de 2023

[Eliminar la configuración de replicación del sistema de archivos de origen](#)

Eliminar la configuración de replicación del sistema de archivos de origen Para obtener más información, consulte [Eliminación de una configuración de replicación](#).

19 de septiembre de 2023

[Se agregó Región de AWS soporte adicional](#)

Amazon EFS ya está disponible en la región de Israel (Tel Aviv).

7 de agosto de 2023

[Aumento del rendimiento de los sistemas de archivos en modo de uso general](#)

Los sistemas de archivos en modo de uso general de Amazon EFS ahora admiten hasta 55 000 operaciones de lectura por segundo y 25 000 operaciones de escritura. Para obtener más información, consulte [Cuotas para los sistemas de archivos de Amazon EFS](#).

3 de agosto de 2023

[Se aumentó el límite de rendimiento aprovisionado](#)

El límite de rendimiento aprovisionado ha aumentado en algunos casos. Regiones de AWS Para obtener más información, consulte [Rendimiento total aprovisionado predeterminado para todos los clientes conectados](#) en cada uno de ellos. Región de AWS

21 de junio de 2023

[Soporte regional ampliado para la replicación de EFS](#)

La replicación de EFS ahora está disponible en todos los Regiones de AWS lugares en los que esté disponible EFS. Para obtener más información, consulte [Replicación de Amazon EFS](#).

28 de abril de 2023

[Aumento del límite de rendimiento elástico](#)

El límite de rendimiento elástico ha aumentado en algunos casos. Regiones de AWS Para obtener más información, consulta la tabla [Rendimiento elástico total predeterminado para todos los clientes conectados en](#) cada uno de ellos. Región de AWS

17 de abril de 2023

[Elastic reemplaza a Bursting como modo de rendimiento predeterminado](#)

El modo de rendimiento predeterminado (y recomendado) para los sistemas de archivos ahora es Elastic en lugar de Bursting. Para obtener más información, consulte [Modos de rendimiento](#).

13 de abril de 2023

Se agregó soporte adicional Región de AWS	Amazon EFS está disponible ahora en la región de Asia-Pacífico (Melbourne).	12 de abril de 2023
Se ha agregado compatibilidad con macOS Ventura	Amazon EFS ahora se puede instalar en instancias Mac EC2 que se ejecuten en macOS Ventura. Para obtener más información, consulte Distribuciones compatibles .	10 de abril de 2023
Se agregó Región de AWS soporte adicional	Amazon EFS está disponible e ahora en la región de Asia-Pacífico (Hyderabad).	16 de febrero de 2023
Se agregó Región de AWS soporte adicional	Amazon EFS ya está disponible e para todos los usuarios en la Región de AWS Europa (España).	19 de enero de 2023
El límite de puntos de acceso para los sistemas de archivos ha aumentado	El número máximo de puntos de acceso que puede tener un solo sistema de archivos ha aumentado de 120 a 1000. Para obtener más información, consulte Cuotas de recursos .	17 de enero de 2023
Se agregó Región de AWS soporte adicional	Amazon EFS ya está disponible e para todos los usuarios de Europa (Zúrich) Región de AWS.	15 de diciembre de 2022
Se agregó soporte para políticas de ciclo de vida de un día	Ahora puede seleccionar un día para la política de ciclo de vida de transición a la IA. Para obtener más información, consulte Trabajo con políticas de ciclo de vida .	27 de noviembre de 2022

[Latencias de lectura y escritura reducidas](#)

Las latencias de lectura y escritura de datos de archivos se han reducido tanto en los sistemas de archivos de almacenamiento One Zone como en los de almacenamiento estándar. Para obtener más información, consulte [Resumen de rendimiento](#).

27 de noviembre de 2022

[Se ha añadido un modo de rendimiento adicional](#)

El modo de rendimiento elástico se añade como opción de rendimiento para los sistemas de archivos de Amazon EFS. Para obtener más información, consulte [Elastic throughput](#).

27 de noviembre de 2022

[Se agregó Región de AWS soporte adicional](#)

Amazon EFS está disponible ahora en la región de Medio Oriente (EAU).

17 de octubre de 2022

[Soporte agregado para la replicación de EFS](#)

Amazon EFS ha eliminado un límite anterior en el que la replicación de EFS no admite sockets ni canalizaciones con nombre (FIFOs).

15 de septiembre de 2022

[Se ha incrementado el límite de bloqueos de archivos por conexión](#)

Se ha incrementado el límite de bloqueos de archivos por conexión de 8192 a 65 536. Para obtener más información, consulte [Cuotas para clientes de NFS](#).

4 de mayo de 2022

<u>Se ha eliminado el límite para los procesos que utilizan bloqueos de archivos</u>	Amazon EFS ha eliminado un límite anterior según el cual un máximo de 256 procesos de una sola instancia podían utilizar bloqueos de archivos al mismo tiempo. Para obtener más información, consulte <u>Cuotas para clientes de NFS</u> .	4 de mayo de 2022
<u>Se agregó Región de AWS soporte adicional</u>	Amazon EFS ya está disponible para todos los usuarios en la Región de AWS de Asia-Pacífico (Yakarta).	27 de enero de 2022
<u>Soporte agregado para la replicación de EFS</u>	Utilice la replicación de EFS para replicar los datos y los metadatos de un sistema de archivos EFS en otro sistema Región de AWS de archivos EFS que elija. Para obtener más información, consulte <u>Replicación de Amazon EFS</u> .	25 de enero de 2022
<u>El sistema de archivos y los recursos de destino de montaje utilizan un formato de ID de recurso de 17 caracteres</u>	Ahora se asignan ID de 17 caracteres al nuevo sistema de archivos de Amazon EFS y a los recursos de destino de montaje. Para obtener más información, consulte <u>Uso de los recursos de Amazon EFS</u> .	22 de octubre de 2021

[Soporte agregado para EFS Intelligent-Tiering \(capas avanzadas\)](#)

EFS Intelligent-Tiering utiliza EFS Lifecycle Management para supervisar los patrones de acceso a los archivos y está diseñado para realizar la transición automática de los archivos hacia y desde las clases de almacenamiento de acceso poco frecuente (IA) correspondientes. Para obtener más información, consulte [EFS Intelligent-Tiering y Lifecycle Management](#).

2 de septiembre de 2021

[Soporte agregado para probar el formato de ID de recurso de 17 caracteres](#)

Amazon EFS pasará de utilizar identificadores de 8 caracteres a identificadores de 17 caracteres para sistemas de archivos y objetivos de montaje el 1 de octubre de 2021. Durante esta transición, puede optar por utilizar identificadores de recursos de 17 caracteres por separado y empezar a utilizarlos Región de AWS . Para obtener más información, consulte [ID de recurso](#).

5 de mayo de 2021

[Soporte agregado para montar sistemas de archivos One Zone desde una zona de disponibilidad diferente mediante el asistente de montaje de Amazon EFS](#)

Ahora puede usar el asistente de montaje de EFS para montar un sistema de archivos de Amazon EFS que utilice clases de almacenamiento de One Zone en una instancia EC2 que se encuentre en una zona de disponibilidad diferente. Puede usar la nueva opción de az para especificar la zona de disponibilidad del sistema de archivos Amazon EFS. Para obtener más información, consulte [Montaje de sistemas de archivos con clases de almacenamiento de One Zone](#).

6 de abril de 2021

[Soporte agregado para clases de almacenamiento EFS de One Zone](#)

Las clases de almacenamiento de Amazon EFS One Zone almacenan los datos en una única zona de disponibilidad de Región de AWS. Las clases de almacenamiento EFS One Zone y One Zone-Infrequent Access (One Zone-IA) son una opción rentable para almacenar datos que no requieren la resiliencia Multi-AZ de las clases de almacenamiento EFS Standard y Standard-IA. Para obtener más información, consulte [Trabajo con clases de almacenamiento de EFS](#).

9 de marzo de 2021

[Se agregó Región de AWS soporte adicional](#)

Amazon EFS ya está disponible para todos los usuarios en la Región de AWS de Asia-Pacífico (Osaka).

3 de marzo de 2021

[Soporte añadido para instancias de Mac de Amazon EC2 que ejecutan macOS Big Sur](#)

Ahora puede montar su sistema de archivos Amazon EFS desde instancias macOS EC2 que ejecutan macOS Big Sur mediante el asistente de montaje de EFS o mediante el comando mount de NFS. Para obtener más información, consulte [Montaje con el asistente de montaje de EFS](#) o [Montaje de sistemas de archivos sin el asistente de montaje de EFS](#).

23 de febrero de 2021

[La nueva consola Amazon EFS está disponible en AWS GovCloud \(US\) la región](#)

La nueva consola Amazon EFS ya está disponible en AWS GovCloud (US) Región de AWS.

10 de febrero de 2021

[Support agregado para la nueva CloudWatch métrica de Amazon EFS MeteredIO Bytes](#)

Puede usar MeteredIO Bytes para medir el número de bytes de cada operación del sistema de archivos, incluida las operaciones de lectura de datos, escritura de datos y metadatos. Las operaciones de lectura se miden a un tercio del ritmo de las demás operaciones. Para obtener más información, consulte [CloudWatch las métricas de Amazon para Amazon EFS.](#)

28 de enero de 2021

[Amazon EFS aumenta el rendimiento de lectura del sistema de archivos en un 300%](#)

Los sistemas de archivos Amazon EFS ahora miden las solicitudes de lectura a un tercio de la velocidad de otras solicitudes.

28 de enero de 2021

[Support agregado para la nueva CloudWatch métrica de Amazon EFS StorageBytes](#)

Puede utilizar StorageBytes para medir y supervisar el tamaño del sistema de archivos en bytes, incluida la cantidad de datos almacenados en las clases de almacenamiento de acceso estándar y de acceso poco frecuente. Para obtener más información, consulte [CloudWatch las métricas de Amazon para Amazon EFS.](#)

11 de enero de 2021

[Úselo AWS Transfer Family para acceder a los sistemas de archivos Amazon EFS](#)

Puede utilizarlos AWS Transfer Family para transferir archivos dentro y fuera de sus sistemas de archivos de Amazon EFS. Para obtener más información, consulte [Utilización AWS Transfer Family para acceder a los archivos del sistema de archivos EFS](#).

6 de enero de 2021

[Se utiliza AWS Systems Manager para administrar el cliente Amazon EFS \(amazon-efs-utils \)](#)

Puede utilizarlos AWS Systems Manager para instalar o actualizar automáticamente los clientes de Amazon EFS (amazon-efs-utils) en sus instancias EC2. Para obtener más información, consulte [Uso de AWS Systems Manager para instalar o actualizar automáticamente los clientes de Amazon EFS](#).

29 de septiembre de 2020

[Aplicación de la creación de sistemas de archivos EFS cifrados](#)

Puede usar la clave de condición `elasticfilesystem:Encrypted` de AWS Identity and Access Management (IAM) para obligar a los usuarios a crear sistemas de archivos Amazon EFS cifrados en reposo. Para obtener más información, consulte [Aplicación de la creación de un sistema de archivos de Amazon EFS cifrado en reposo](#).

16 de septiembre de 2020

[El rendimiento por cliente de Amazon EFS aumentó un 100 %](#)

EFS ahora admite un rendimiento de hasta 500 MB/s por cliente, lo que supone un aumento del 100 % con respecto al límite anterior de 250 MB/s. Para obtener más información, consulte [Cuotas para los sistemas de archivos de Amazon EFS](#).

23 de julio de 2020

[Soporte agregado para copias de seguridad diarias automáticas de los sistemas de archivos de Amazon EFSs](#)

Las copias de seguridad diarias automáticas ahora están habilitadas de forma predeterminada cuando crea un sistema de archivos mediante la consola de EFS. Para obtener más información, consulte [Uso AWS Backup con Amazon EFS](#).

16 de julio de 2020

[El nuevo flujo de trabajo Creación rápida simplifica la creación de sistemas de archivos Amazon EFS](#)

Con la opción Creación rápida de la consola EFS, puede crear un sistema de archivos EFS con la configuración recomendada por el servicio con un solo botón. Para obtener más información, consulte [Sistema de archivos CreateYour Amazon EFS](#).

16 de julio de 2020

[La nueva consola de Amazon EFS ya está disponible](#)

La nueva consola de EFS le facilita el uso de Amazon EFS y simplifica la administración de sus sistemas de archivos de EFS.

16 de julio de 2020

[Amazon EFS aumenta el rendimiento mínimo del sistema de archivos](#)

Los sistemas de archivos Amazon EFS que utilizan un rendimiento en ráfaga ahora tienen un rendimiento mínimo de 1 MiB/s. Para obtener más información, consulte [Modos de rendimiento](#).

30 de junio de 2020

[Aumento del rendimiento de los sistemas de archivos en modo de uso general](#)

Los sistemas de archivos del modo de uso general de Amazon EFS admiten ahora hasta un total de 35 000 operaciones de lectura por segundo, un aumento del 400 % respecto al límite anterior de 7000. Para obtener más información, consulte [Cuotas para los sistemas de archivos de Amazon EFS](#).

1 de abril de 2020

<u>Región de AWS Se ha añadido soporte adicional</u>	Amazon EFS ya está disponible para todos los usuarios de Beijing y Ningxia Regiones de AWS.	22 de enero de 2020
<u>Soporte añadido para la autorización de IAM para clientes de NFS</u>	Ahora puede usar AWS Identity and Access Management (IAM) para administrar el acceso de NFS a un sistema de archivos Amazon EFS. Para obtener más información, consulte <u>Uso de AWS IAM para controlar el acceso de NFS a Amazon EFS</u> .	13 de enero de 2020
<u>Compatibilidad añadida para los puntos de acceso de EFS</u>	Los puntos de acceso de Amazon EFS son puntos de entrada específicos que la aplicación utiliza para acceder a un sistema de archivos de Amazon EFS y que facilitan la administración del acceso de las aplicaciones a conjuntos de datos compartidos. Para obtener más información, consulte <u>Uso de puntos de acceso de Amazon EFS</u> .	13 de enero de 2020

[Support agregado para la restauración AWS Backup parcial.](#)

Ahora puede restaurar archivos y directorios específicos mediante una restauración parcial, además de restaurar un punto de recuperación completo. Para obtener más información, consulte [Uso AWS Backup con Amazon EFS](#).

13 de enero de 2020

[Soporte añadido para roles vinculados a servicios de IAM](#)

Ahora Amazon EFS utiliza un rol vinculado a servicios basado en IAM, lo que facilita la configuración de EFS mediante la adición automática de los permisos necesarios. Para obtener más información, consulte [Uso de roles vinculados a servicios para Amazon EFS](#).

10 de diciembre de 2019

[Se agregó Región de AWS soporte adicional](#)

Amazon EFS ya está disponible para todos los usuarios de Europa (Estocolmo) Región de AWS.

20 de noviembre de 2019

[Se ha añadido Región de AWS soporte adicional](#)

Amazon EFS ya está disponible para todos los usuarios de Asia Pacífico (Hong Kong) Región de AWS.

20 de noviembre de 2019

[Se ha añadido Región de AWS soporte adicional](#)

Amazon EFS ya está disponible para todos los usuarios de Sudamérica (São Paulo) Región de AWS.

20 de noviembre de 2019

[Se agregó Región de AWS soporte adicional](#)

Amazon EFS ya está disponible para todos los usuarios de Oriente Medio (Bahrén) Región de AWS.

20 de noviembre de 2019

[Nueva política de administración del ciclo de vida de 7 días añadida](#)

La administración del ciclo de vida cuenta ahora con una política adicional para mover datos a la clase de almacenamiento rentable de acceso infrecuente después de 7 días. Para obtener más información, consulte [Administración del ciclo de vida de EFS](#).

6 de noviembre de 2019

[Se ha añadido compatibilidad para los puntos de conexión de VPC de tipo interfaz](#)

Puede establecer una conexión privada entre la nube virtual privada y Amazon EFS para llamar a la API de EFS. Para obtener más información, consulte [Trabajo con puntos de enlace de la VPC](#).

22 de octubre de 2019

[Monte un sistema de archivos de EFS al lanzar una nueva instancia EC2.](#)

Ahora puede configurar nuevas instancias Amazon EC2 para que monten sus sistemas de archivos de EFS al iniciarse en el Asistente de la instancia de lanzamiento de EC2. Para obtener más información, consulte [Paso 2. Crear sus recursos de EC2 y lanzar la instancia EC2](#).

17 de octubre de 2019

[Se ha añadido compatibilidad con Service Quotas](#)

Ahora puede ver todos los límites de Amazon EFS en la consola de cuotas de servicio. Para obtener más información, consulte [Límites de Amazon EFS](#).

10 de septiembre de 2019

[Nuevas políticas de administración del ciclo de vida añadidas](#)

Ahora, al utilizar la administración del ciclo de vida, puede elegir una de las cuatro políticas de ciclo de vida para definir cuándo se pasan los archivos a la clase de almacenamiento de Acceso poco frecuente, más rentable. Para obtener más información, consulte [Administración del ciclo de vida de EFS](#).

9 de julio de 2019

[Administración del ciclo de vida de EFS ahora disponible en todos los sistemas de archivos de EFS.](#)

La característica Administración del ciclo de vida de EFS está ahora disponible en todos los sistemas de archivos de EFS. Se ha eliminado una restricción anterior basada en la fecha en la que se creó un sistema de archivos. Para obtener más información, consulte [Administración del ciclo de vida de EFS](#).

9 de julio de 2019

[Se agregó Región de AWS soporte adicional](#)

Amazon EFS ya está disponible para todos los usuarios de Europa (París) Región de AWS.

12 de junio de 2019

Se ha añadido Región de AWS soporte adicional	Amazon EFS ya está disponible para todos los usuarios de Asia Pacífico (Bombay) Región de AWS.	5 de junio de 2019
Se agregó Región de AWS soporte adicional	Amazon EFS ya está disponible para todos los usuarios de Canadá (centro) Región de AWS.	1 de mayo de 2019
Actualización de la API: las etiquetas ahora forman parte de la carga útil de la CreateFileSystem operación	Ahora puede incluir etiquetas cuando utilice la CreateFileSystem operación de AWS API y CLI para crear un sistema de archivos Amazon EFS. Para obtener más información, consulte CreateFileSystem y creación de un sistema de archivos mediante la AWS CLI .	19 de febrero de 2019
Nuevas características: clase de almacenamiento de acceso poco frecuente de EFS y administración del ciclo de vida de EFS	El acceso poco frecuente de Amazon EFS es una clase de almacenamiento económica para los archivos a los que no se obtiene acceso con frecuencia. La administración del ciclo de vida de EFS cambia automáticamente los archivos del almacenamiento estándar al almacenamiento de acceso poco frecuente. Para obtener más información, consulte Clases de almacenamiento de EFS .	13 de febrero de 2019

[Se agregó Región de AWS soporte adicional](#)

Amazon EFS ya está disponible para todos los usuarios de Europa (Londres) Región de AWS.

23 de enero de 2019

[AWS Backup Integración de servicios con Amazon EFS](#)

Se pueden realizar copias de seguridad de los sistemas de archivos Amazon EFS mediante AWS Backup un servicio de copia de seguridad automatizado, centralizado y totalmente gestionado para realizar copias de seguridad de los datos de todos los AWS servicios en la nube y en las instalaciones. Para obtener más información, consulte [AWS Backup y Amazon EFS](#).

16 de enero de 2019

[Se ha añadido soporte de conexión de Transit Gateway para sistemas de almacenamiento en las instalaciones.](#)

Los sistemas de archivos de Amazon EFS ahora son accesibles utilizando o conexiones de Transit Gateway a sistemas de almacenamiento en las instalaciones. Para obtener más información, consulte [Montaje de otra cuenta o VPC](#) y [Tutorial: Montar un sistema de archivos desde una VPC distinta](#).

6 de diciembre de 2018

[La sincronización de archivos EFS ahora forma parte del nuevo AWS DataSync servicio.](#)

AWS DataSync es un servicio de transferencia de datos gestionado que simplifica la sincronización de grandes cantidades de datos entre los sistemas de almacenamiento locales y AWS los servicios de almacenamiento. Para obtener más información, consulte [Transferir archivos de sistemas de archivos locales a Amazon EFS mediante AWS DataSync.](#)

26 de noviembre de 2018

Se ha añadido compatibilidad con la conexión VPN y la interconexión con VPC entre regiones

Ya se puede acceder a Amazon EFS a través de conexiones de VPN y conexión de emparejamiento de VPC entre regiones. Para obtener más información, consulte [Transferir archivos de sistemas de archivos locales a Amazon EFS mediante AWS DataSync.](#)

23 de octubre de 2018

Se ha añadido compatibilidad con la conexión VPN y la interconexión con VPC entre regiones

Ya se puede acceder a los sistemas de archivos de Amazon EFS a través de conexiones de VPN conexión de emparejamiento de VPC entre regiones. Para obtener más información, consulte las secciones [Montaje desde otra cuenta o VPC](#) y [Funcionamiento de Amazon EFS con Direct Connect y VPN.](#)

23 de octubre de 2018

Se agregó Región de AWS soporte adicional	Amazon EFS ya está disponible para todos los usuarios en la Región de AWS de Asia-Pacífico (Singapur).	13 de julio de 2018
Presentación del modo de rendimiento aprovisionado	Ahora puede aprovisionar el desempeño para sistemas de archivos nuevos o existentes con el nuevo modo de desempeño aprovisionado. Para obtener más información, consulte Modos de rendimiento .	12 de julio de 2018
Se agregó Región de AWS soporte adicional	Amazon EFS ya está disponible para todos los usuarios en la Región de AWS de Asia-Pacífico (Tokio).	11 de julio de 2018

En la siguiente tabla se describen los cambios importantes en la Guía del usuario de sistema de archivos elástico de Amazon antes de julio de 2018.

Cambio	Descripción	Fecha de modificación
Se agregó Región de AWS soporte adicional	Amazon EFS ya está disponible para todos los usuarios en la AWS de Asia-Pacífico (Seúl).	30 de mayo de 2018
Se agregó soporte para matemáticas CloudWatch métricas	La matemática métrica te permite consultar múltiples CloudWatch métricas y usar expresiones matemáticas para crear nuevas series temporales basadas en estas métricas. Para obtener más información, consulte Uso de cálculos de métricas con Amazon EFS .	4 de abril de 2018
Añadido el conjunto de	Las herramientas de amazon-efs-utils son un conjunto de archivos ejecutables de código abierto	4 de abril de 2018

Cambio	Descripción	Fecha de modificación
herramientas de código abierto <code>amazon-efs-utils</code> y el cifrado en movimiento	<p>que simplifican aspectos del uso de Amazon EFS, por ejemplo, el montaje. Su uso <code>amazon-efs-utils</code> no supone ningún coste adicional y puedes descargar estas herramientas desde GitHub. Para obtener más información, consulte Instalación de las herramientas de Amazon EFS.</p> <p>También en esta versión, Amazon EFS admite el cifrado en tránsito usando el túnel de TLS (Transport Layer Security). Para obtener más información, consulte Cifrado de datos en Amazon EFS.</p>	
Límites actualizados del sistema de archivos por Región de AWS	Amazon EFS ha aumentado el límite del número de sistemas de archivos de todas las cuentas de todas las Región de AWS. Para obtener más información, consulte Cuotas de recursos de Amazon EFS que no puede cambiar .	15 de marzo de 2018
Se agregó Región de AWS soporte adicional	Amazon EFS ya está disponible para todos los usuarios del oeste de EE. UU. (norte de California) Región de AWS.	14 de marzo de 2018
Cifrado de datos en reposo	Amazon ES ahora admite el cifrado de datos en reposo. Para obtener más información, consulte Cifrado de datos en Amazon EFS .	14 de agosto de 2017
Añadida compatibilidad con más regiones	Amazon EFS ya está disponible en la región de Europa (Fráncfort).	20 de julio de 2017

Cambio	Descripción	Fecha de modificación
Nombres de sistema de archivos que utilizan sistema de nombres de dominio (DNS)	Amazon EFS ahora es compatible con nombres de DNS para sistemas de archivos. Un nombre de DNS de un sistema de archivos resuelve automáticamente la dirección IP de un destino de montaje en la zona de disponibilidad para la conexión de instancia Amazon EC2. Para obtener más información, consulte Montaje en Amazon EC2 con un nombre de DNS .	20 de diciembre de 2016
Mayor compatibilidad con etiquetas para sistemas de archivos	Amazon EFS ahora es compatible con 50 etiquetas por sistema de archivos. Para obtener más información sobre las etiquetas en Amazon EFS, consulte Etiquetado de los recursos de Amazon EFS .	29 de agosto de 2016
Disponibilidad general	Disponibilidad general de Amazon ECS en las regiones de Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón) y Europa (Irlanda).	28 de junio de 2016
Aumento del límite del sistema de archivos	El número de sistemas de archivos de Amazon EFS que se pueden crear por cada cuenta para cada Región de AWS aumentó de 5 a 10.	21 de agosto de 2015
Ejercicio de introducción actualizado	El ejercicio de introducción se ha actualizado para simplificar el proceso de introducción.	17 de agosto de 2015
Nueva guía	Esta es la primera versión de la Guía del usuario de sistema de archivos elásticos de Amazon.	26 de mayo de 2015

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.