aws

Guida per l'utente

# Amazon Elastic File System

# Amazon Elastic File System: Guida per l'utente

# Table of Contents

# Cos’è Amazon Elastic File System?

Amazon Elastic File System (Amazon EFS) fornisce un'archiviazione di file serverless e completamente elastica in modo da poter condividere i dati dei file senza dover fornire o gestire la capacità e le prestazioni di archiviazione. Amazon EFS è progettato per eseguire il dimensionamento on-demand fino a svariati petabyte senza interrompere le applicazioni, aumentando e riducendo automaticamente le dimensioni man mano che aggiungi e rimuovi i file. Dal momento che Amazon EFS ha una semplice interfaccia di servizi Web, puoi creare e configurare i file system in modo rapido e semplice. Il servizio gestisce tutta l'infrastruttura di storage dei file per conto dell'utente, il che significa che è possibile evitare attività complesse come la distribuzione, l'applicazione di patch e la manutenzione di complesse configurazioni di file system.

Amazon EFS supporta il protocollo Network File System versione 4 (NFSv4.1 e NFSv4.0). Pertanto, le applicazioni e gli strumenti attualmente in uso potranno continuare a funzionare correttamente con Amazon EFS. Amazon EFS è accessibile dalla maggior parte dei tipi di istanze di calcolo di Amazon Web Services, tra cui Amazon EC2, Amazon ECS, Amazon AWS Lambda EKS e. AWS Fargate

Il servizio è stato progettato per essere altamente scalabile, a disponibilità elevata ed estremamente durevole. Amazon EFS offre i seguenti tipi di file system per soddisfare le tue esigenze di disponibilità e durabilità:

- Regionale (consigliato): i file system regionali (consigliato) archiviano i dati in modo ridondante su più zone di disponibilità geograficamente separate all'interno di un. Regione AWS L'archiviazione dei dati su più zone di disponibilità garantisce la disponibilità continua dei dati, anche quando una o più zone di disponibilità in una non sono disponibili. Regione AWS
- One Zone: i file system One Zone archiviano i dati all'interno di una singola zona di disponibilità in una Regione AWS. L'archiviazione dei dati in una singola zona di disponibilità garantisce la disponibilità continua dei dati. Nel caso improbabile di perdita o danneggiamento totale o parziale della zona di disponibilità, tuttavia, i dati archiviati in questi tipi di file system potrebbero andare persi.

Per ulteriori informazioni sui tipi di file system, consulta Tipi di file system EFS.

Amazon EFS è stato progettato per fornire i livelli di throughput, IOPS e bassa latenza necessari per un'ampia gamma di carichi di lavoro. I file system EFS possono crescere fino a dimensioni dell'ordine dei petabyte, offrire alti livelli di throughput e consentire alle istanze un accesso ai dati

altamente parallelizzato. Per la maggior parte dei carichi di lavoro, consigliamo di utilizzare le modalità predefinite, ovvero la modalità prestazioni General Purpose e le modalità Elastic throughput.

- Scopo generale: la modalità prestazionale General Purpose è ideale per applicazioni sensibili alla latenza, come ambienti di server Web, sistemi di gestione dei contenuti, home directory e server di file in generale.
- Elastico: la modalità Elastic throughput è progettata per aumentare o ridurre automaticamente le prestazioni di throughput per soddisfare le esigenze dell'attività del carico di lavoro.

Per ulteriori informazioni sulle prestazioni e sulle modalità di throughput EFS, vedere Prestazioni Amazon EFS.

Amazon EFS fornisce file-system-access semantica, ad esempio una forte coerenza dei dati e il blocco dei file. Per ulteriori informazioni, consulta Coerenza dei dati in Amazon EFS. Amazon EFS consente inoltre di controllare l'accesso ai file system tramite le autorizzazioni POSIX (Portable Operating System Interface). Per ulteriori informazioni, consulta Sicurezza in Amazon EFS.

Amazon EFS supporta funzionalità di autenticazione, autorizzazione e crittografia per aiutarti a soddisfare i requisiti di sicurezza e conformità. Amazon EFS supporta due forme di crittografia per i file system, la crittografia dei dati in transito e la crittografia dei dati memorizzati su disco. Alla creazione di un file system Amazon EFS, è possibile abilitare la crittografia dei dati memorizzati su disco. Facendolo, tutti i dati e i metadati vengono crittografati. Al montaggio del file system è possibile abilitare la crittografia dei dati in transito. L'accesso del client NFS a EFS è controllato sia da policy AWS Identity and Access Management (IAM) che da policy di sicurezza di rete, come i gruppi di sicurezza. Per ulteriori informazioni, consulta Crittografia dei dati in Amazon EFS, Gestione dell'identità e degli accessi per Amazon Elastic File System e Controllo dell'accesso di rete ai file system Amazon EFS per i client NFS.

> **Note**
>
> L'utilizzo di Amazon EFS con istanze Amazon EC2 basate su Microsoft Windows non è supportato.

# È la prima volta che utilizzi Amazon EFS?

Se è la prima volta che utilizzi Amazon EFS, ti consigliamo di leggere le seguenti sezioni in ordine:

1. Per una panoramica sul prodotto e sui prezzi di Amazon EFS, consulta Amazon EFS.
2. Per una panoramica tecnica di Amazon EFS, consulta Amazon EFS: come funziona.
3. Segui le esercitazioni introduttive:
   - Nozioni di base
   - Procedure guidate

Per ulteriori informazioni su Amazon EFS, i seguenti argomenti esaminano il servizio in modo più dettagliato:

- Utilizzo delle risorse Amazon EFS
- Gestione dei file system Amazon EFS
- API EFS

# Amazon EFS: come funziona

Qui di seguito, è possibile trovare una descrizione su come funziona Amazon EFS, sui dettagli implementativi e sulle considerazioni di sicurezza.

Argomenti



## Panoramica

Amazon Elastic File System fornisce un file system semplice, senza server set-and-forget ed elastico. Con Amazon EFS, è possibile creare un file system, montarlo su un'istanza Amazon EC2, quindi leggere e scrivere dati su e dal file system. È possibile montare un file system Amazon EFS all'interno della propria VPC utilizzando il protocollo Network File System versione 4.0 e 4.1 (NFSv4). Si consiglia di utilizzare un client NFSv4.1 di Linux di ultima generazione, come quelli presenti nelle ultime AMI di Amazon Linux, Amazon Linux 2, Red Hat, Ubuntu e macOS Big Sur, insieme all'helper di montaggio Amazon EFS. Per istruzioni, consulta Utilizzo degli amazon-efs-utils strumenti.

Per un elenco di AMI (Amazon Machine Image) Linux per Amazon EC2 che supportano questo protocollo, consulta Supporto per NFS. Per alcune AMI, è necessario installare un client NFS prima di montare il file system su un'istanza Amazon EC2. Per istruzioni, consulta Installazione del client NFS.

È possibile accedere al file system Amazon EFS contemporaneamente da più client NFS, in modo che le applicazioni che scalano oltre una singola connessione possano accedere a un file system. Le istanze Amazon EC2 e altre AWS in esecuzione in più zone di disponibilità all'interno della stessa Regione AWS possono accedere al file system, consentendo a più utenti di accedere e condividere un'origine dati comune.

Per un elenco di Regioni AWS in cui è possibile creare file system Amazon EFS, consulta Riferimenti generali di Amazon Web Services.

Per accedere al file system Amazon EFS in una VPC, è necessario creare una o più destinazioni di montaggio nella VPC.

- Per i file system regionali, puoi creare una destinazione di montaggio in ogni zona di disponibilità di Regione AWS.
- Per i file system a zona singola, si crea solo una singola destinazione di montaggio che si trova nella stessa zona di disponibilità del file system.

Per ulteriori informazioni, consulta Classi di storage EFS.

Una destinazione di montaggio fornisce un indirizzo IP per un endpoint NFSv4 in cui è possibile montare un file system Amazon EFS. Montare il file system utilizzando il nome Domain Name Service (DNS), che si risolve nell'indirizzo IP della destinazione di montaggio di EFS nella stessa zona di disponibilità dell'istanza EC2. È possibile creare una destinazione di montaggio per ogni zona di disponibilità in Regione AWS. Se la VPC dispone di più sottoreti in una zona di disponibilità, è possibile creare una destinazione di montaggio in una di tali sottoreti. Tutte le istanze EC2 nella zona di disponibilità condividono quella destinazione di montaggio.

> **Note**
>
> Un file system Amazon EFS può avere destinazioni di montaggio solo in un VPC alla volta.

i target di montaggio stesse sono progettate per offrire elevata disponibilità. Durante la progettazione di disponibilità elevata e il failover ad altre zone di disponibilità, tenere presente che mentre gli indirizzi IP e il DNS per le destinazioni di montaggio in ogni zona di disponibilità sono statici, sono componenti ridondanti supportati da più risorse.

Dopo aver montato il file system utilizzando il suo nome DNS, utilizzarlo come qualsiasi altro file system compatibile con POSIX. Per ulteriori informazioni sulle autorizzazioni a livello di NFS e sulle considerazioni correlate, vedere Utilizzo di utenti, gruppi e autorizzazioni a livello di Network File System (NFS).

È possibile montare i file system AWS Direct Connect su server di data center on-premise quando sono connessi alla VPC Amazon con o AWS VPN. È possibile montare i file system EFS su server

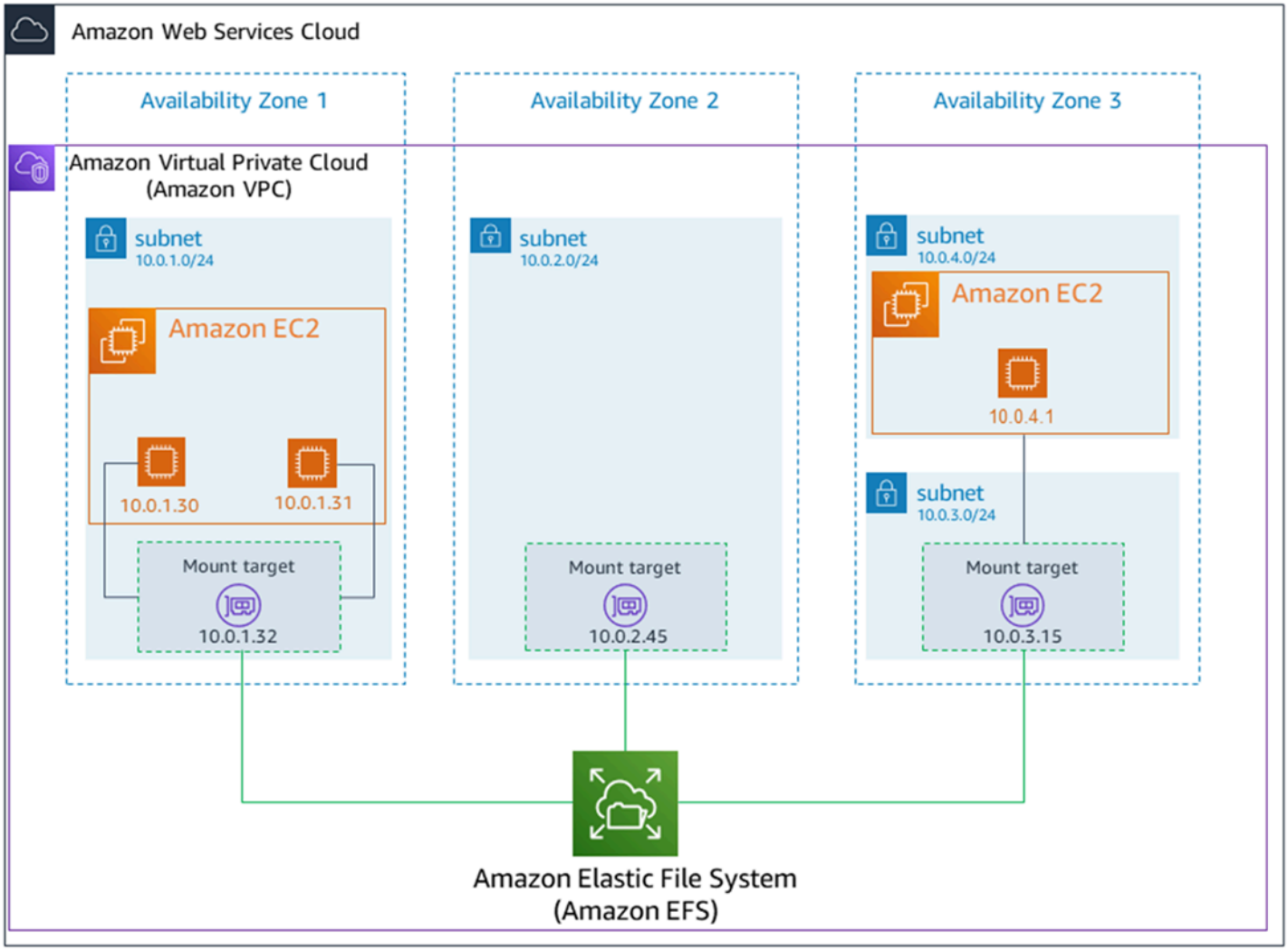
on-premise per eseguire la migrazione di set di dati a EFS, abilitare scenari di espansione del cloud o eseguire il backup dei dati locali su EFS.

# Utilizzo di Amazon EFS con Amazon EC2

Questa sezione spiega come i file system Amazon EFS regionali e a zona singola vengono montati su istanze EC2 in un Amazon VPC.

## File system Amazon EFS regionali

La seguente illustrazione mostra più istanze EC2 che accedono a un file system Amazon EFS configurato per più zone di disponibilità in Regione AWS.

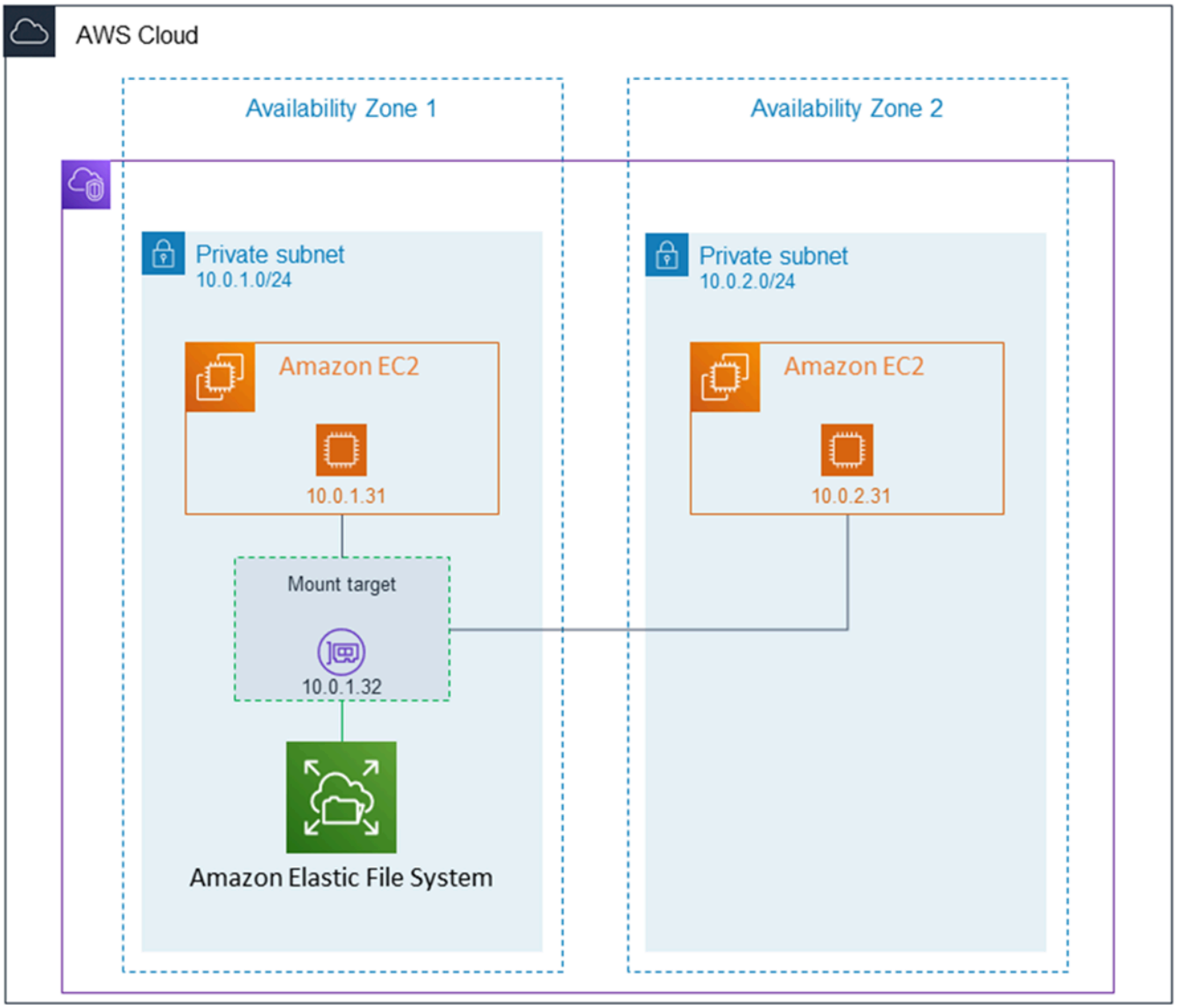



In questa illustrazione, il cloud privato virtuale (VPC) ha tre zone di disponibilità. Poiché il file system è regionale, è stato creato un target di montaggio in ogni zona di disponibilità. Consigliamo di

accedere al file system da una destinazione di montaggio situata all'interno della stessa zona di disponibilità per motivi prestazionali e di costi. Una delle zone di disponibilità dispone di due sottoreti. Tuttavia, viene creata una destinazione di montaggio in una sola delle sottoreti. Per ulteriori informazioni, consulta Monta il file system utilizzando l'helper di montaggio di EFS Montaggio su istanze Amazon EC2 Linux utilizzando l'helper di montaggio EFS.

## File system Amazon EFS a zona singola

La seguente illustrazione mostra più istanze EC2 che accedono a un file system a zona singola da diverse zone di disponibilità in un'unica Regione AWS.



In questa illustrazione, il VPC ha due zone di disponibilità, ciascuna con una sottorete. Poiché il tipo di file system è a zona singola, può avere una sola destinazione di montaggio. Per migliorare le prestazioni e i costi, ti consigliamo di accedere al file system da un target di montaggio nella stessa zona di disponibilità dell'istanza EC2 su cui lo stai montando.

In questo esempio, l'istanza EC2 nella zona di disponibilità us-west-2c pagherà i costi di accesso ai dati EC2 per l'accesso a un target di montaggio in una zona di disponibilità diversa. Per ulteriori informazioni, consulta Montaggio dei file system a zona singola.

# Come funziona Amazon EFS con AWS Direct Connect e VPN gestite da AWS

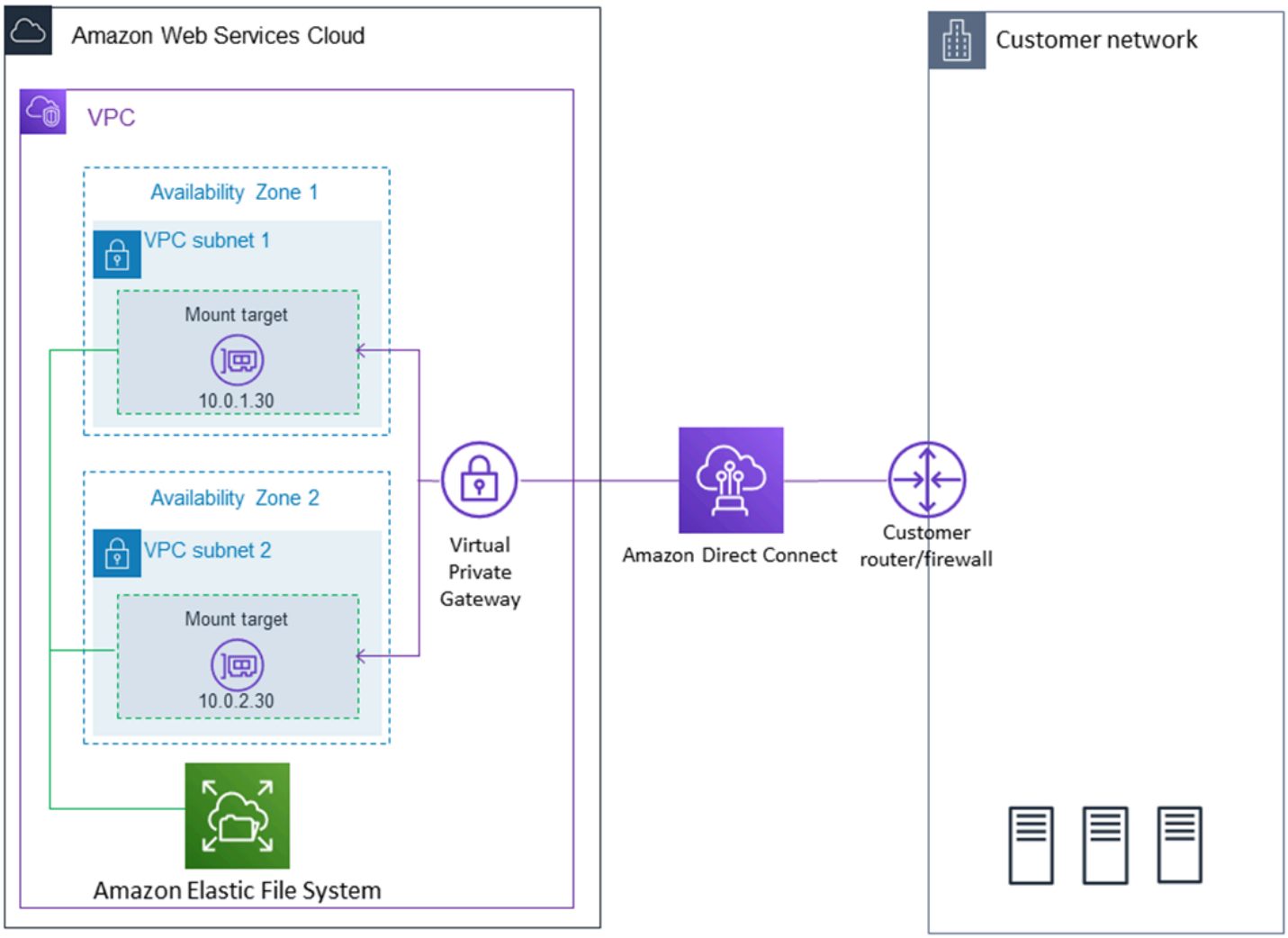
Utilizzando un file system Amazon EFS montato su un server on-premise, è possibile eseguire la migrazione dei dati on-premise in Cloud AWS su un file system Amazon EFS. È inoltre possibile usufruire del bursting. In altre parole, puoi spostare i dati dai server on-premise in Amazon EFS e analizzarli su un parco istanze Amazon EC2 nella VPC Amazon. È quindi possibile archiviare i risultati definitivamente nel file system o spostare i risultati nel server locale.

Tenere a mente le considerazioni seguenti durante l'uso di Amazon EFS con un server on-premise:

- Il server locale deve disporre di un sistema operativo basato su Linux. Consigliamo un kernel Linux 4.0 o versioni successive.
- Per semplicità, consigliamo di montare un file system Amazon EFS su un server on-premise utilizzando l'indirizzo IP di una destinazione di montaggio invece di un nome DNS.

Non vi è alcun costo aggiuntivo per l'accesso on-premise ai file system Amazon EFS. Viene addebitato il costo per la connessione AWS Direct Connect alla VPC Amazon. Per ulteriori informazioni, consulta Prezzi di AWS Direct Connect.

La figura seguente mostra un esempio di come accedere a un file system Amazon EFS on-premise (i server on-premise hanno il file system montato).




È possibile utilizzare qualsiasi destinazione di montaggio nel VPC se si possono raggiungere le sottoreti della destinazione di montaggio utilizzando una connessione AWS Direct Connect tra il server locale e il VPC. Per accedere ad Amazon EFS da un server on-premise, aggiungere una regola al gruppo di sicurezza della destinazione di montaggio per consentire il traffico in ingresso sulla porta NFS (2049) proveniente dal server on-premise. Per ulteriori informazioni, comprese le procedure dettagliate, consulta Procedura dettagliata: creare e montare un file system in locale con una VPN AWS Direct Connect.

# Come funziona Amazon EFS con AWS Backup

Per un backup completo dell'implementazione per i file system, è possibile utilizzare Amazon EFS con AWS Backup. AWS Backup è un servizio di backup completamente gestito che consente di centralizzare e automatizzare il backup dei dati su tutti i servizi AWS nel cloud e on-premise. Utilizzando AWS Backup, puoi configurare le policy di backup e monitorare l'attività delle tue risorse

AWS per il backup. Amazon EFS dà sempre la priorità alle operazioni di file system rispetto alle operazioni di backup. Per ulteriori informazioni sul backup dei file system EFS utilizzando AWS Backup, consultare Backup dei file system di Amazon EFS.

## Riepilogo dell'implementazione

In Amazon EFS, la risorsa principale è un file system. Ad ogni file system sono associate proprietà, come ID, token di creazione, istante di creazione, dimensioni del file system in byte, il numero di destinazioni di montaggio create per il file system e stato del ciclo di vita del file system. Per ulteriori informazioni, consulta CreateFileSystem.

Amazon EFS supporta anche altre risorse per configurare la risorsa principale. Queste includono destinazioni di montaggio e punti di accesso:

- Destinazione di montaggio - Per accedere al file system, è necessario creare delle destinazioni di montaggio nella VPC. Ogni destinazione di montaggio possiede le seguenti proprietà: ID della destinazione di montaggio, ID della sottorete in cui viene creata, ID del file system per cui è stata creata, un indirizzo IP in corrispondenza del quale il file system potrebbe essere montato, gruppi di sicurezza VPC e stato della destinazione di montaggio. Nel comando `mount` è possibile utilizzare l'indirizzo IP o il nome DNS.

  Ogni file system dispone di un nome DNS nel seguente formato.

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

  È possibile specificare il nome DNS nel comando `mount` usato per montare il file system . Si supponga di creare una sottocartella `efs-mount-point` all'interno della cartella principale dell'istanza EC2 o del server locale. È possibile utilizzare il comando mount per montare il file system. Ad esempio, su un'AMI Amazon Linux, è possibile utilizzare il seguente comando `mount`.

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

  Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza. In primo luogo, è necessario installare il client NFS sull'istanza di EC2. L'Nozioni di baseesercizio fornisce step-by-step istruzioni.

- Access Points – Un punto di accesso applica un utente del sistema operativo, gruppo e percorso del file system a qualsiasi richiesta di file system effettuata utilizzando il punto di accesso. L'utente e il gruppo per sistema operativo del punto di accesso sostituiscono le eventuali informazioni di identità fornite dal client NFS. Il percorso file system viene esposto al client come la directory radice del punto di accesso. In questo modo ogni applicazione utilizza sempre l'identità del sistema operativo corretta e la directory corretta durante l'accesso a set di dati basati su file condivisi. Le applicazioni che utilizzano il punto di accesso possono accedere ai dati solo nella propria directory e sotto a questa. Per ulteriori informazioni, consulta Utilizzo dei punti di accesso Amazon EFS.

Le destinazioni di montaggio e i tag sono risorse secondarie associate a un file system. Possono essere creati solo nel contesto di un file system esistente.

Amazon EFS fornisce delle operazioni API che permettono di creare e gestire queste risorse. Oltre alle operazioni di creazione ed eliminazione di ciascuna risorsa, Amazon EFS supporta anche un'operazione di descrizione che consente di recuperare le informazioni sulla risorsa. Per la creazione e la gestione di queste risorse sono messe a disposizione le seguenti alternative:

- Utilizzo della console Amazon EFS - Per un esempio, consulta Nozioni di base.
- Utilizzo dell'interfaccia a riga di comando (Command Line Interface - CLI) di Amazon EFS - Per un esempio, consulta Procedura dettagliata: Creazione di un file system Amazon EFS e montarlo su un'istanza Amazon EC2 utilizzandoAWS CLI.
- È inoltre possibile gestire queste risorse in modo programmatico come segue:
  - Utilizzare gli SDK AWS Gli SDK AWSsemplificano le attività di programmazione tramite il wrapping dell'API sottostante. Inoltre, i client degli SDK autenticano le richieste utilizzando le chiavi di accesso fornite dall'utente. Per ulteriori informazioni, consultare Librerie e codice di esempio.
  - Richiamare l'API Amazon EFS direttamente dall'applicazione - Se non è possibile utilizzare gli SDK per qualsiasi motivo, è possibile effettuare le chiamate API Amazon EFS direttamente dall'applicazione. Tuttavia, scegliendo questa opzione è necessario scrivere il codice di autenticazione delle richieste. Per ulteriori informazioni sull'API Amazon EFS, consulta API EFS.

# Autenticazione e controllo degli accessi

Per eseguire richieste verso l'API di Amazon EFS, come ad esempio quella di creazione di un file system, è necessario disporre di credenziali valide. Inoltre, è necessario disporre delle autorizzazioni per creare o accedere alle risorse.

Agli utenti e ai ruoli creati in AWS Identity and Access Management (IAM) devono essere concesse le autorizzazioni per creare o accedere alle risorse. Per ulteriori informazioni sulle autorizzazioni, consultare Gestione dell'identità e degli accessi per Amazon Elastic File System.

L'autorizzazione IAM per i client NFS è un'opzione di protezione aggiuntiva di Amazon EFS che utilizza IAM per semplificare la gestione degli accessi per i client NFS (Network File System) su larga scala. Con l'autorizzazione IAM per i client NFS, puoi utilizzare IAM per gestire l'accesso a un file system EFS in modo intrinsecamente scalabile. L'autorizzazione IAM per i client NFS è ottimizzata anche per gli ambienti cloud. Per ulteriori informazioni sull'utilizzo dell'autorizzazione IAM per i client NFS, consulta Utilizzo di IAM per controllare l'accesso ai dati del file system.

# Coerenza dei dati in Amazon EFS

Amazon EFS fornisce la semantica di close-to-open coerenza che le applicazioni si aspettano da NFS.

In Amazon EFS, le operazioni di scrittura per file system regionali vengono memorizzate in modo persistente tra le zone di disponibilità in questi scenari:

- Un'applicazione esegue un'operazione di scrittura sincrona (per esempio, utilizzando il comando Linux `open` con il flag `O_DIRECT` o il comando Linux `fsync`).
- Un'applicazione chiude un file.

A seconda del modello di accesso, Amazon EFS può fornire garanzie di coerenza più forti rispetto alla close-to-open semantica. Le applicazioni che eseguono l'accesso sincrono ai dati ed eseguono scritture senza aggiunta hanno read-after-write coerenza per quanto riguarda l'accesso ai dati.

## Blocco dei file

Le applicazioni client NFS possono utilizzare il blocco dei file NFS versione 4 (incluso il blocco per intervallo di byte) per operazioni di lettura e scrittura sui file Amazon EFS.

Ricorda quanto segue su come Amazon EFS blocca i file:

- Amazon EFS supporta solo il blocco consultivo e le operazioni di lettura/scrittura, non verificano la presenza di blocchi in conflitto prima dell'esecuzione. Ad esempio, per evitare problemi di sincronizzazione dei file con operazioni atomiche, l'applicazione deve conoscere la semantica NFS (come la coerenza). close-to-open

- Ogni specifico file può sostenere fino a 512 blocchi in tutte le istanze connesse e gli utenti che accedono al file.

# Classi di storage EFS

Amazon EFS offre diverse classi di storage per diverse esigenze di archiviazione di dati. Standard è la prima classe di storage in cui vengono scritti i dati ed è la classe di storage per i dati a cui si accede frequentemente. Per i file ad accesso meno frequente, Amazon EFS offre le classi di storage EFS Infrequent Access (IA) ed EFS Archive. La classe di storage IA è ottimizzata in termini di costi per i dati a cui si accede poche volte ogni trimestre e la classe di storage Archive è ottimizzata in termini di costi per i dati a cui si accede solo poche volte all'anno o meno. Per ulteriori informazioni sulle classi di storage Amazon EFS, consulta Classi di storage EFS.

## gestione del ciclo di vita

Per gestire i file system in modo che vengano archiviati in modo conveniente per tutto il loro ciclo di vita, utilizza la gestione del ciclo di vita. La gestione del ciclo di vita trasferisce automaticamente i dati tra le classi di storage in base alla configurazione del ciclo di vita definita per il file system. La configurazione del ciclo di vita è un insieme di policy del ciclo di vita che definiscono quando trasferire i dati del file system a un'altra classe di storage.

Per ulteriori informazioni, consulta Gestione dello storage del file system.

# Replica EFS

Puoi creare una replica del tuo file system Amazon EFS nel modo che preferisci utilizzando la Regione AWS replica. La replica replica automaticamente e in modo trasparente i dati e i metadati del tuo file system EFS in un nuovo file system EFS di destinazione creato in un file system EFS a tua scelta. Regione AWS

Con la replica, EFS mantiene automaticamente sincronizzati i file system di origine e di destinazione. La replica è continua e progettata per fornire un obiettivo del punto di ripristino (RTO) e un obiettivo del tempo di ripristino (RTO) di minuti. Queste funzionalità consentono di raggiungere gli obiettivi di conformità e continuità aziendale. Per ulteriori informazioni, consulta Replica dei file system.

# Configurazione

Prima di utilizzare Amazon EFS per la prima volta, è necessario completare le seguenti operazioni:

1. Registrarsi per creare un Account AWS
2. Creazione di un utente amministratore

## Registrarsi per creare un Account AWS

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

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

   Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Al termine del processo di registrazione, riceverai un'e-mail di conferma da AWS. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

## Creazione di un utente amministratore

Dopo aver effettuato la registrazione di un Account AWS, proteggi Utente root dell'account AWS, abilita AWS IAM Identity Center e crea un utente amministratore in modo da non utilizzare l'utente root per le attività quotidiane.

### Protezione dell'Utente root dell'account AWS

1. Accedi alla AWS Management Console come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email del Account AWS. Nella pagina successiva, inserisci la password.

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

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

### Creazione di un utente amministratore

1. Abilita IAM Identity Center.

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

   Per un tutorial sull'utilizzo di IAM Identity Center directory come origine di identità, consulta Configurazione dell'accesso utente con IAM Identity Center directory predefinito nella Guida per l'utente di AWS IAM Identity Center.

### Accesso come utente amministratore

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

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

# Guida introduttiva ad Amazon Elastic File System

In questa esercitazione sulle nozioni di base potrai apprendere come creare rapidamente un file system Amazon Elastic File System (Amazon EFS). Per eseguire il processo, è necessario montare il file system su un'istanza Amazon Elastic Compute Cloud (Amazon EC2) nel cloud privato virtuale (VPC, Virtual Private Cloud), Puoi anche testare la end-to-end configurazione.

Per creare e utilizzare il tuo primo file system Amazon EFS, dovrai eseguire quattro passaggi:

- Creare un file system Amazon EFS.
- Creare le risorse Amazon EC2, avviare l'istanza e montare il file system.
- Trasferire i file al file system EFS utilizzando AWS DataSync.
- Eliminare le risorse e proteggere Account AWS.

Argomenti



## Presupposti

Per questa esercitazione, facciamo le seguenti assunzioni:

- L'utente ha già familiarità con l'utilizzo della console Amazon EC2 per avviare le istanze.
- Le tue risorse Amazon VPC, Amazon EC2 e Amazon EFS sono tutte in Regione AWS. Questa guida utilizza la regione Stati Uniti occidentali (Oregon) (us-west-2).
- All’interno di Regione AWS in uso per questa esercitazione sulle nozioni di base è disponibile una VPC di default. Se non si dispone di una VPC di default oppure se si desidera installare il file system su una nuova VPC con gruppi di sicurezza nuovi o esistenti, è possibile continuare a utilizzare questa esercitazione sulle nozioni di base. Per farlo, configura Utilizzo di gruppi di sicurezza VPC per istanze Amazon EC2 e destinazioni di montaggio.

- Non è stata modificata la regola di autorizzazione in ingresso predefinita per il gruppo di sicurezza di predefinito.
- Hai creato un utente amministratore nel tuo account Account AWS e stai utilizzando le relative credenziali per gestire le risorse del tuo account. Per ulteriori informazioni, consulta Configurazione.

## Argomenti correlati

Questa guida fornisce inoltre una procedura dettagliata per eseguire un'analoga esercitazione sulle nozioni di base utilizzando i comandi AWS Command Line Interface (AWS CLI) per eseguire le chiamate alle API Amazon EFS. Per ulteriori informazioni, consulta Procedura dettagliata: Creazione di un file system Amazon EFS e montarlo su un'istanza Amazon EC2 utilizzandoAWS CLI.

## Fase 1: Creazione di un file system Amazon EFS

In questa fase, utilizza la console Amazon EFS per creare un file system Amazon EFS con le impostazioni consigliate dal servizio.

Se desideri creare un file system con una configurazione personalizzata, consulta Creazione di un file system con impostazioni personalizzate utilizzando la console Amazon EFS.

Creazione del file system Amazon EFS

1. Accedi a AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Scegli Crea file system per aprire la finestra di dialogo Crea file system.
3. (Facoltativo) Immetti un Nome per il file system.
4. Per Virtual Private Cloud (VPC), scegli il tuo VPC o mantienilo impostato sul tuo VPC predefinito.
5. Scegli Crea per creare un file system che utilizzi le seguenti impostazioni consigliate dal servizio:
   - Backup automatici attivati. Per ulteriori informazioni, consulta Backup dei file system di Amazon EFS.
   - Installa i target configurati con le seguenti impostazioni:
     - Creato in ogni zona di disponibilità Regione AWS in cui viene creato il file system.
     - Si trova nelle sottoreti predefinite del VPC selezionato.

    - Utilizzo del gruppo di sicurezza predefinito del VPC: puoi gestire i gruppi di sicurezza dopo la creazione del file system.

  Per ulteriori informazioni, consulta Gestione dell'accessibilità del file system dalla rete.

- Per ulteriori informazioni sui tipi di file system regionali, consulta Tipi di file system EFS.
- Per ulteriori informazioni sulle prestazioni a scopi generali, consulta Modalità prestazionali.
- Per ulteriori informazioni sul Throughput Elastic, consulta Modalità di velocità di trasmissione effettiva.
- Crittografia dei dati inattivi abilitata utilizzando la chiave predefinita per Amazon EFS (`aws/elasticfilesystem`) — Per ulteriori informazioni, consultaCrittografia dei dati a riposo.
- gestione del ciclo di vita: Amazon EFS crea il file system con le seguenti politiche del ciclo di vita:
    - Transizione a IA impostata su 30 giorni dall'ultimo accesso.
    - TransitionToArchiveimpostato su 90 giorni dall'ultimo accesso.
    - Transizione a standard impostato su Nessuno.

  Per ulteriori informazioni, consulta Gestione dello storage del file system.

Dopo avere creato il file system, puoi personalizzare le impostazioni del file system ad eccezione di disponibilità e durabilità, crittografia e modalità a prestazioni.

La pagina File system viene visualizzata con un banner nella parte superiore che mostra lo stato del file system creato. Quando il file system diventa disponibile, nel banner viene visualizzato un collegamento per accedere alla pagina dei dettagli del file system.

Per ulteriori informazioni sullo stato dei file system, consulta Stato del file system.

## Fase 2: Creazione delle risorse EC2 e avvio dell'istanza EC2

> **Note**
>
> Amazon EFS non può essere utilizzato con istanze Amazon EC2 basate su Microsoft Windows.

In questo passaggio creerai una nuova istanza Amazon EC2 con Amazon Linux 2 e la configurerai per montare automaticamente il file system EFS appena creato nella Fase 1.

Prima di poter avviare e connettersi a un'istanza Amazon EC2, è necessario creare una coppia di chiavi, a meno che non sia già disponibile. È possibile creare una coppia di chiavi utilizzando la console Amazon EC2, quindi è possibile avviare l'istanza di EC2.

Creazione di una coppia di chiavi

- Segui i passaggi in Configurazione con Amazon EC2 nella Guida per l'utente di Amazon EC2 per le istanze Linux per creare una coppia di chiavi. Se si dispone già di una coppia di chiavi, non è necessario crearne una nuova. Per questo esercizio puoi utilizzare la coppia di chiavi esistente.

Per avviare l'istanza EC2 e montare un file system EFS

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. In Fase 1: Scelta di una Amazon Machine Image (AMI), trova un'AMI Amazon Linux 2 all'inizio dell'elenco e scegli Seleziona.
4. In Fase 2: Scelta di un tipo di istanza scegli Passaggio successivo: Configura i dettagli dell'istanza.
5. In Fase 3: Configurazione dei dettagli dell'istanza, fornisci le seguenti informazioni:
   - Lascia il Numero di istanze uguale a uno.
   - Lascia Acquisto sull'impostazione predefinita.
   - Per Rete, scegli la voce per lo stesso VPC annotato al momento della creazione del file system EFS in Fase 1: Creazione di un file system Amazon EFS.
   - Per Sottorete, scegli una sottorete predefinita in qualsiasi zona di disponibilità.
   - Per File system, assicurati che sia selezionato il file system EFS creato in Fase 1: Creazione di un file system Amazon EFS. Il percorso mostrato accanto all'ID del file system è il punto di montaggio che verrà utilizzato dall'istanza EC2, che è possibile modificare.
   - I Dati utente includono automaticamente i comandi per il montaggio del file system Amazon EFS.
6. Scegli Passaggio successivo: aggiunta dello storage.
7. Scegliere Passaggio successivo: aggiunta di tag.
8. Denomina l'istanza e scegli Passaggio successivo: configurazione del gruppo di sicurezza.

9. In Fase 6: Configurazione del gruppo di sicurezza, imposta Assegna un gruppo di sicurezza su Seleziona un gruppo di sicurezza esistente. Scegli il gruppo di sicurezza predefinito per assicurarti che possa accedere al file system EFS.
10. Scegli Analizza e avvia.
11. Scegli Avvia.
12. Seleziona la casella di controllo relativa alla coppia di chiavi creata e scegli Avvia istanze.

    Una volta creata e resa disponibile, l'istanza EC2 verrà montata sul file system EFS. A questo punto, sarai in grado di trasferire file sul tuo file system EFS.

# Fase 3: Trasferimento dei file ad Amazon EFS utilizzando AWS DataSync

Ora che è stato creato un file system EFS funzionante, è possibile utilizzare AWS DataSync per trasferire i file da un file system esistente ad Amazon EFS. AWS DataSync è un servizio di trasferimento dei dati che semplifica, automatizza e accelera lo spostamento e la replica dei dati tra sistemi di storage on-premise e servizi di storage AWS su Internet AWS Direct Connect. AWS DataSync può trasferire i dati del file e anche i metadati del file system come proprietà, timestamp e autorizzazioni di accesso.

## Prima di iniziare

In questa fase, è necessario disporre di quanto segue:

- Un file system NFS sorgente dal quale è possibile trasferire file. Questo file system di origine deve essere accessibile con NFS versione 3, versione 4 o 4.1. File system di esempio includono quelli situati in un data center on-premise, in file system auto gestiti nel cloud e file system Amazon EFS.
- Un file system EFS su cui trasferire file. Se non si dispone di un file system EFS, creane uno. Per ulteriori informazioni, consulta Guida introduttiva ad Amazon Elastic File System.
- Il server e la rete soddisfano i requisiti AWS DataSync. Per ulteriori informazioni, consulta Requisiti di AWS DataSync.

Per trasferire i file da una posizione di origine a una destinazione utilizzando AWS DataSync, effettua le seguenti operazioni:

- Scaricare e distribuire un agente nell'ambiente e attivarlo.

- Creare e configurare una posizione di origine e di destinazione.
- Creare e configurare un'attività.
- Eseguire l'attività per trasferire i file dall'origine alla destinazione.

Per informazioni su come trasferire i file da un file system on-premise esistente al file system EFS, consultare Nozioni di base su AWS DataSync nella Guida per l'utente di AWS DataSync. Per ulteriori informazioni su come trasferire i file da un file system esistente nel cloud in un file system EFS, consulta Implementazione dell'agent AWS DataSync come istanza Amazon EC2 nella Guida per l'utente di AWS DataSync e Amazon EFS AWS DataSync In-Cloud Transfer Quick Start and Scheduler.

## Fase 4: Eliminazione delle risorse e protezione dell'account AWS

Questa guida include scenari che è possibile utilizzare per esplorare ulteriormente Amazon EFS. Prima di eseguire questa fase di pulizia, è possibile utilizzare le risorse create e a cui ci si è connessi durante questa esercitazione per ulteriori esplorazioni. Per ulteriori informazioni, consulta Procedure guidate. Al completamento dell'esplorazione ulteriore oppure qualora non si desideri esplorare gli scenari aggiuntivi, è necessario seguire questi passaggi per eliminare le risorse e proteggere l'account Account AWS.

Eliminazione delle risorse e protezione dell'account

1. Esegui la connessione all'istanza Amazon EC2.
2. Disinstalla il file system Amazon EFS con il seguente comando.

   ```
   $ sudo umount efs
   ```

3. Apri la console EFS all'indirizzo https://console.aws.amazon.com/efs/.
4. Scegli il file system EFS che si desidera eliminare dall'elenco dei file system.
5. In Azioni, seleziona Elimina file system.
6. Nella finestra di dialogo Eliminazione definitiva del file system, immetti l'ID del file system Amazon EFS da eliminare e scegli Elimina file system.
7. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
8. Scegli l'istanza Amazon EC2 da terminare nell'elenco delle istanze.
9. In Azioni, seleziona Stato istanza e scegli Termina.

10. In Termina istanze, scegli Sì, termina per terminare l'istanza creata per questa esercitazione sulle nozioni di base.
11. Fai clic su Gruppi di sicurezza nel riquadro di navigazione.
12. Seleziona il nome del gruppo di sicurezza creato per questa esercitazione sulle nozioni di base in Fase 2: Creazione delle risorse EC2 e avvio dell'istanza EC2 all'interno della procedura guidata di avvio dell'istanza Amazon EC2.

    > **Warning**
    >
    > Non eliminare il gruppo di sicurezza predefinito della VPC.

13. In Azioni, scegli Elimina gruppo di sicurezza.
14. In Elimina gruppo di sicurezza, scegli Sì, elimina per eliminare il gruppo di sicurezza creato per questa esercitazione sulle nozioni di base.

# Tipi di file system e classi di storage Amazon EFS

Questa sezione descrive i tipi di file system e le opzioni della classe di storage per i file system Amazon Elastic File System (Amazon EFS).

## Tipi di file system EFS

Amazon EFS offre tipi di file system regionali e a zona singola.

- Regionale: i file system regionali (consigliato) archiviano i dati in modo ridondante su più zone di disponibilità geograficamente separate all'interno di un. Regione AWS L'archiviazione dei dati su più zone di disponibilità garantisce la disponibilità continua dei dati, anche quando una o più zone di disponibilità in una non sono disponibili. Regione AWS
- One Zone: i file system One Zone archiviano i dati all'interno di una singola zona di disponibilità in una Regione AWS. L'archiviazione dei dati in una singola zona di disponibilità garantisce la disponibilità continua dei dati. Nel caso improbabile di perdita o danneggiamento totale o parziale della zona di disponibilità, tuttavia, i dati archiviati in questi tipi di file system potrebbero andare persi.

  Nell'improbabile eventualità di perdita o danneggiamento totale o parziale di una zona di AWS disponibilità, i dati in una classe di storage One Zone potrebbero andare persi. Ad esempio, eventi come incendi e inondazioni potrebbero causare la perdita di dati. Oltre a questi tipi di eventi, le nostre classi di storage a zona singola utilizzano design ingegneristici simili a quelli delle nostre classi di storage regionali per proteggere gli oggetti da guasti indipendenti a livello di disco, host e rack, e ciascuna è progettata per offrire una durabilità dei dati del 99.999999999%.

  Per una maggiore protezione dei dati, Amazon EFS esegue automaticamente il backup dei file system One Zone con AWS Backup. Puoi ripristinare i backup del file system in qualsiasi zona di disponibilità operativa all'interno di una Regione AWS o puoi ripristinarli in un'altra Regione AWS. I backup del file system EFS creati e gestiti utilizzando AWS Backup vengono replicati in tre zone di disponibilità e sono progettati per durare a lungo. Per ulteriori informazioni, vedere Resilience in. AWS Backup

> **Note**
>
> I file system One Zone sono disponibili solo per determinate zone di disponibilità. Per una tabella che elenca le zone di disponibilità in cui è possibile utilizzare i file system One Zone, vedereZone di disponibilità supportate per i file system a zona singola.

Nella tabella seguente vengono confrontati i tipi di file system con disponibilità, durata e altre considerazioni.

| Tipo di file system | Sviluppato per | Durabilità (in base alla progettazione) | Disponibilità | Zone di disponibilità | Altre considerazioni |
|---|---|---|---|---|---|
| Regionale | Dati che richiedono la massima durabilità e disponibilità. | 99,999999999% (11 9 s) | 99,99% | >=3 | Nessuno |
| Zona singola | Dati che richiedono la massima durabilità e disponibilità. | 99,999999999% (11 9 s) | 99,99% | 1 | Non resiliente alla perdita della zona di disponibilità |

## Zone di disponibilità supportate per i file system a zona singola

I file system One Zone sono disponibili solo per determinate zone di disponibilità. La tabella seguente elenca gli ID AZ Regione AWS e gli ID AZ per ogni zona di disponibilità in cui è possibile utilizzare i file system One Zone. Per vedere la mappatura degli ID AZ alle zone di disponibilità nel tuo account, consulta gli ID delle zone di disponibilità per AWS le tue risorse nella Guida per l'utente di AWS Resource Access Manager.

Zone di disponibilità che supportano i file system One Zone

| Regione AWS Nome | Regione AWS Codice | ID AZ supportati |
|---|---|---|
| Stati Uniti orientali (Ohio) | us-east-2 | use2-az1, use2-az2, use2-az3 |
| Stati Uniti orientali (Virginia settentrionale) | us-east-1 | use1-az1, use1-az2, use1-az4, use1-az5, use1-az6 |
| US West (N. California) | us-west-1 | usw1-az1, usw1-az3 |
| Stati Uniti occidentali (Oregon) | us-west-2 | usw2-az1, usw2-az2, usw2-az3, usw2-az4 |
| Africa (Cape Town) | af-south-1 | afs1-az1, afs1-az2, afs1-az3 |
| Asia Pacifico (Hong Kong) | ap-east-1 | ape1-az1, ape1-az2, ape1-az3 |
| Asia Pacific (Mumbai) | ap-south-1 | aps1-az1, aps1-az2, aps1-az3 |
| Asia Pacifico (Osaka-Locale) | ap-northeast-3 | apne3-az1, apne3-az2, apne3-az3 |
| Asia Pacifico (Seoul) | ap-northeast-2 | apne2-az1, apne2-az2, apne2-az3 |
| Asia Pacific (Singapore) | ap-southeast-1 | apse1-az1, apse1-az2 |
| Asia Pacific (Sydney) | ap-southeast-2 | apse2-az1, apse2-az2, apse2-az3 |
| Asia Pacifico (Tokyo) | ap-northeast-1 | apne1-az1, apne1-az4 |
| Canada (Central) | ca-central-1 | cac1-az1, cac1-az2 |
| China (Beijing) | cn-north-1 | cnn1-az1, cnn1-az2 |
| Cina (Ningxia) | cn-northwest-1 | cnnw1-az1, cnnw1-az2, cnnw1-az3 |
| Europe (Frankfurt) | eu-central-1 | euc1-az1, euc1-az2, euc1-az3 |

| Regione AWS Nome | Regione AWS Codice | ID AZ supportati |
|---|---|---|
| Europa (Irlanda) | eu-west-1 | euw1-az1, euw1-az2, euw1-az3 |
| Europe (London) | eu-west-2 | euw2-az1, euw2-az2 |
| Europa (Milano) | eu-south-1 | eus1-az1, eus1-az2, eus1-az3 |
| Europe (Paris) | eu-west-3 | euw3-az1, euw3-az3 |
| Europa (Stoccolma) | eu-north-1 | eun1-az1, eun1-az2, eun1-az3 |
| Medio Oriente (Bahrein) | me-south-1 | mes1-az1, mes1-az2, mes1-az3 |
| Sud America (São Paulo) | sa-east-1 | sae1-az1, sae1-az2, sae1-az3 |
| AWS GovCloud (Stati Uniti orientali) | us-gov-east-1 | usge1-az1, usge1-az2, usge1-az3 |
| AWS GovCloud (Stati Uniti occidentali) | us-gov-west-1 | usgw1-az1, usgw1-az2, usgw1-az3 |

# Classi di storage EFS

Le diverse classi di storage Amazon EFS sono progettate per lo storage più efficace a seconda dei casi d'uso.

- EFS Standard: la classe di storage EFS Standard utilizza storage SSD (Solid State Drive) per offrire i livelli di latenza più bassi per i file a cui si accede di frequente. I nuovi dati del file system vengono prima scritti nella classe di storage EFS Standard e quindi possono essere trasferiti su più livelli nelle classi di storage EFS Infrequent Access ed EFS Archive utilizzando la gestione del ciclo di vita.
- EFS Infrequent Access (IA): una classe di storage a costi ottimizzati per i dati a cui si accede solo poche volte al trimestre.
- EFS di archivio: una classe di storage ottimizzata in termini di costi per i dati a cui si accede poche volte all'anno o meno.

La classe di storage EFS Archive è supportata sui file system EFS con throughput elastico. Non è possibile aggiornare la velocità effettiva del file system a Bursting o Con provisioning una volta che il file system contiene dati nella classe di storage di archivio.

## Ottimizzazione dei costi di archiviazione

Le classi di storage IA e Archive sono ottimizzate in termini di costi per i file che non richiedono le prestazioni di latenza dello storage Standard. La latenza al primo byte durante la lettura da una delle classi di storage ad accesso infrequente è superiore a quella della classe di storage standard.

Utilizzando la gestione del ciclo di vita, è possibile ottimizzare i costi di storage suddividendo automaticamente i dati tra le classi di storage in base ai modelli di accesso del carico di lavoro. È possibile spostare i file dalle classi di storage IA o Archive alla classe di storage Standard impostando la politica del ciclo di vita Transition to Standard sul file system. Questa impostazione trasferisce i file da IA o Archive a Standard al momento dell'accesso. Se desideri che i tuoi file rimangano nella classe di storage Standard a cui si accede di frequente, disattiva la gestione del ciclo di vita sul file system. Per ulteriori informazioni, consulta Gestione dello storage del file system.

## Confronto delle classi di storage

La tabella seguente confronta le classi di storage. Per ulteriori dettagli sulle prestazioni di ogni classe di storage, vedi Prestazioni Amazon EFS.

| Classe di storage | Sviluppato per | Latenza di lettura del primo byte | Durabilità (progettata per) 1 | Disponibilità (SLA) | Zone di disponibilità | Costo di fatturazione minimo per file 2 | Durat di archiv ione minim |
|---|---|---|---|---|---|---|---|
| EFS Standard | Dati attivi che richiedono prestazioni di latenza inferiori al millisecondo | Meno di millisecondo | 99,999999999%<br>(11 anni e 9) | 99,99% (regionale)<br>99,9% (una zona) | =>3 (regionale)<br>1 (Una zona) | Non applicabile | Non applic le |

| Classe di storage | Sviluppato per | Latenza di lettura del primo byte | Durabilità (progettata per) 1 | Disponibilità (SLA) | Zone di disponibilità | Costo di fatturazione minimo per file 2 | Durata di archiviazione minim |
|---|---|---|---|---|---|---|---|
| Accesso non frequente a EFS | Dati inattivi a cui si accede solo poche volte ogni trimestre. | Decine di millisecondi | | | | 128 KiB | Non applicabile |
| EFS di archivio | Dati inattivi a cui si accede poche volte all'anno o meno | Decine di millisecondi | | 99,9% (regionale) | =>3 (regionale) | 128 KiB | 90 giorni |

Note

[1] Poiché i file system One Zone archiviano i dati in un'unica zona di AWS disponibilità, i dati archiviati in questi tipi di file system potrebbero andare persi in caso di emergenza o altro errore che influisca su tutte le copie dei dati all'interno della zona di disponibilità o in caso di distruzione della zona di disponibilità.

[2] Le policy relative al ciclo di vita aggiornate a partire dalle 12:00 PT del 26 novembre 2023 trasferiranno i file di < 128 KB alla classe IA. Per ulteriori informazioni su come Amazon EFS contabilizza e fattura singoli file e metadati, consulta. Misurazione: come Amazon EFS calcola le dimensioni di file system e oggetti

## Prezzi della classe di storage

La fatturazione avviene in base alla quantità di dati in ogni classe di storage, Ti vengono inoltre addebitati i costi di accesso ai dati quando vengono letti i file nello storage IA o Archive o per i dati che passano da una classe di storage all'altra utilizzando la gestione del ciclo di vita. La fattura AWS mostra la capacità per ogni classe di storage e l'accesso calcolato rispetto alla classe di storage del file system. Per ulteriori informazioni, consulta Prezzi di Amazon EFS.

Inoltre, le classi di storage Infrequent Access (IA) e Archive hanno un costo di fatturazione minimo per file di 128 KB. Il supporto per file di dimensioni inferiori a 128 KiB è disponibile solo per le politiche relative al ciclo di vita aggiornate a partire dalle 12:00 PT del 26 novembre 2023. Per ulteriori informazioni su come Amazon EFS contabilizza e fattura singoli file e metadati, consulta. Misurazione: come Amazon EFS calcola le dimensioni di file system e oggetti

Si applicano prezzi aggiuntivi per i file system che utilizzano il throughput Con provisioning o Bursting.

- Per i file system che utilizzano il Throughput con provisioning, la fatturazione avviene per il throughput con provisioning, oltre a ciò che viene fornito in base alla quantità di dati presenti nella classe di storage EFS Standard.
- Per i file system che utilizzano Bursting, il throughput consentito è determinato in base alla quantità di dati archiviati solo nella classe di storage EFS Standard.

Per ulteriori informazioni sulle modalità di throughput EFS, vedereModalità di velocità di trasmissione effettiva.

> **Note**
>
> Non sono previsti costi di accesso ai dati quando si utilizza AWS Backup per eseguire il backup di file system EFS abilitati alla gestione del ciclo di vita. Per ulteriori informazioni sulla gestione del ciclo di vita e sulla gestione del ciclo di vita, consulta. AWS Backup Classi di storage EFS

## Visualizzazione della dimensione della classe di storage

Puoi visualizzare la quantità di dati archiviata in ogni classe di storage del tuo file system utilizzando la console Amazon EFS AWS CLI, o l'API EFS.

Visualizzazione delle dimensioni dei dati di storage nella console Amazon EFS

La scheda Dimensioni misurate nella pagina dei Dettagli del file system mostra la dimensione misurata corrente del file system in multipli binari di byte (kibibyte, mebibyte, gibibyte e tebibyte). La metrica viene emessa ogni 15 minuti e consente di visualizzare la dimensione misurata del file system nel tempo. La Dimensione misurata visualizza le seguenti informazioni sulla dimensione di archiviazione del file system:

- La Dimensione totale è la dimensione (in byte binari) dei dati memorizzati nel file system, incluse tutte le classi di archiviazione.
- La Dimensione in Standard è la dimensione (in byte binari) dei dati archiviati nella classe di storage EFS Standard.
- La Dimensione in IA è la dimensione (in byte binari) dei dati archiviati nella classe di storage EFS ad accesso infrequente. I file di dimensioni inferiori a 128 KiB vengono arrotondati a 128 KiB.
- La Dimensione in archivio è la dimensione (in byte binari) dei dati archiviati nella classe di storage di archivio EFS. I file di dimensioni inferiori a 128 KiB vengono arrotondati a 128 KiB.

Puoi anche visualizzare la metrica `Storage bytes` nella scheda Monitoraggio nella pagina dei Dettagli del file system nella console Amazon EFS. Per ulteriori informazioni, consulta Accesso alle CloudWatch metriche.

Visualizzazione delle dimensioni dei dati di archiviazione utilizzando il AWS CLI

È possibile visualizzare la quantità di dati archiviata in ciascuna classe di storage del file system utilizzando l'API AWS CLI o EFS. Visualizza i dettagli di archiviazione dei dati chiamando il comando `describe-file-systems` CLI (l'operazione API corrispondente è DescribeFileSystems).

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

Nella risposta, `ValueInIA` visualizza l'ultima dimensione misurata in byte nella classe di storage ad accesso infrequente del file system. `ValueInStandard` visualizza l'ultima dimensione misurata in byte nella classe di storage Standard. `ValueInArchive` visualizza l'ultima dimensione misurata in byte nella classe di storage di archivio. La somma dei tre valori è uguale alla dimensione dell'intero file system, visualizzato in. `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"
      }
   ]
}
```

Per ulteriori metodi per visualizzare e misurare l'utilizzo del disco, consulta Misurazione degli oggetti di un file system Amazon EFS.

# Utilizzo delle risorse Amazon EFS

Amazon EFS fornisce un sistema di memorizzazione dei file elastico e condiviso compatibile con POSIX. Il file system che crei supporta l'accesso simultaneo in lettura e scrittura da più istanze Amazon EC2. Il file system è accessibile anche da tutte le zone di disponibilità in Regione AWS cui è stato creato.

È possibile montare un file system Amazon EFS sulle istanze EC2 nel proprio cloud privato virtuale (VPC) basato su Amazon VPC utilizzando il protocollo Network File System versioni 4.0 e 4.1 (NFSv4). Per ulteriori informazioni, consulta Amazon EFS: come funziona.

Ad esempio, supponiamo che si disponga di una o più istanze EC2 avviate nel VPC. Ora si desidera creare e utilizzare un file system su queste istanze. Di seguito sono riportate le fasi tipiche che è necessario eseguire per utilizzare i file system Amazon EFS nella VPC:

- Crea un file system Amazon EFS: quando crei un file system, ti consigliamo di utilizzare il tag Name. Il valore del tag Name viene visualizzato nella console e semplifica l'identificazione del file system. È anche possibile aggiungere al file system altri tag facoltativi.
- Crea target di montaggio per il file system - Per accedere al file system nella VPC e montare il file system sull'istanza Amazon EC2, è necessario creare target di montaggio nelle sottoreti della VPC.
- Crea i gruppi di sicurezza - Sia l'istanza Amazon EC2 che un target di montaggio devono essere associati a dei gruppi di sicurezza. Questi gruppi di sicurezza fungono da firewall virtuale che controlla il traffico tra di essi. È possibile utilizzare il gruppo di sicurezza associato al target di montaggio per controllare il traffico in entrata verso il file system. A tale scopo, aggiungi una regola in entrata al gruppo di sicurezza del target di montaggio che consente l'accesso da una specifica istanza EC2. Quindi, è possibile montare il file system solo su tale istanza di EC2.

Se non conosci Amazon EFS, ti consigliamo di provare i seguenti esercizi che forniscono un' end-to-end esperienza diretta dell'uso di un file system Amazon EFS:

- Nozioni di base: l'esercizio introduttivo illustra come creare un file system con le impostazioni consigliate dal servizio. In questo esercizio, creerai un file system utilizzando la procedura guidata Amazon EFS Quick Create, lo monterai su un'istanza EC2 e testerai la configurazione. La console si occupa di molte cose al posto tuo e ti aiuta a configurare rapidamente l' end-to-end esperienza.
- Procedura dettagliata: Creazione di un file system Amazon EFS e montarlo su un'istanza Amazon EC2 utilizzandoAWS CLI— La procedura dettagliata è simile all'esercizio Getting Started, ma

utilizza il AWS Command Line Interface (AWS CLI) per eseguire la maggior parte delle attività. Poiché i AWS CLI comandi sono strettamente correlati all'API Amazon EFS, la procedura dettagliata può aiutarti a familiarizzare con le operazioni dell'API Amazon EFS.

Per ulteriori informazioni sulla creazione di risorse EFS e sull'accesso a un file system, consulta i seguenti argomenti.

Argomenti



# ID risorsa

Amazon EFS assegna identificatori di risorse (ID) univoci a tutte le risorse EFS al momento della creazione. Tutti gli ID di risorsa EFS sono costituiti da un identificatore di risorsa e da una combinazione di cifre da 0 a 9 e lettere minuscole dalla a alla f.

Prima di ottobre 2021, gli ID assegnati alle risorse di target di montaggio e file system appena create utilizzavano 8 caratteri dopo il trattino (ad esempio, `fs-12345678`). Da maggio 2021 a ottobre 2021, sono stati modificati gli ID di questi tipi di risorse per utilizzare 17 caratteri dopo il trattino (ad esempio, `fs-1234567890abcdef0`). A seconda di quando è stato creato l'account, è possibile che le risorse del file system e del target di montaggio abbiano ID brevi, ma tutte le nuove risorse di questo tipo ricevono ID più lunghi. Gli ID delle risorse EFS esistenti non cambiano mai.

# Creazione di file system Amazon EFS

Di seguito, puoi imparare a creare un file system Amazon EFS utilizzando AWS Management Console e il AWS CLI.

Se non conosci Amazon EFS, ti consigliamo di seguire l'esercizio introduttivo. Questo esercizio fornisce end-to-end istruzioni basate su console per creare e accedere a un file system nel cloud privato virtuale (VPC). Per ulteriori informazioni, consulta Nozioni di base.

Argomenti



## Requisiti

Questa sezione descrive i requisiti e i prerequisiti per la creazione di file system Amazon EFS.

### Token di creazione e idempotenza

L'idempotenza assicura che una richiesta API venga completata solo una volta. Quando si utilizzano richieste idempotenti, se la richiesta originale viene completata correttamente, le richieste successive non hanno alcun effetto aggiuntivo. Ciò è utile per evitare che vengano creati lavori duplicati quando interagisci con l'API Amazon EFS.

L'API Amazon EFS supporta l'idempotenza con i token di richiesta del client. Un token di richiesta client è una stringa univoca che specifichi quando effettui una richiesta di creazione del processo.

Un token di richiesta client può essere qualsiasi stringa che include fino a 64 caratteri ASCII. Se riutilizzi un token di richiesta del cliente entro un minuto dall'esito positivo della richiesta, l'API restituisce i dettagli del lavoro della richiesta originale.

Se si utilizza la console, questa genera il token per conto dell'utente. Se utilizzi il flusso di Creazione personalizzata nella console, il token di creazione generato per te ha il seguente formato:

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

Se si utilizza Quick Create per creare un file system con le impostazioni consigliate dal servizio, il token di creazione ha il seguente formato:

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

### Autorizzazioni richieste

Per creare risorse EFS, come un file system e punti di accesso, è necessario disporre delle autorizzazioni AWS Identity and Access Management (IAM) per l'operazione e la risorsa API corrispondenti.

Crea utenti IAM e concedi loro le autorizzazioni per le azioni di Amazon EFS con le policy degli utenti. È inoltre possibile utilizzare i ruoli per concedere le autorizzazioni a più account. Amazon Elastic File System utilizza anche un ruolo collegato al servizio IAM che include le autorizzazioni necessarie per chiamare altri utenti per tuo Servizi AWS conto. Per ulteriori informazioni sulla gestione delle autorizzazioni per le operazioni API, consulta Gestione dell'identità e degli accessi per Amazon Elastic File System.

## Opzioni di configurazione durante la creazione di un file system

È possibile creare un file system utilizzando la console Amazon EFS o utilizzando AWS Command Line Interface (AWS CLI). Puoi anche creare file system a livello di codice utilizzando AWS SDK o direttamente l'API Amazon EFS. Se utilizzi l'API Amazon EFS o un AWS SDK, puoi utilizzare l'azione API `CreateFileSystem` EFS per creare policy di file system.

Quando crei un file system Amazon EFS utilizzando il flusso di creazione personalizzato nella console o in AWS CLI, puoi scegliere le impostazioni per le seguenti funzionalità e opzioni di configurazione del file system.

### Tipo di file system

Il tipo di file system determina la disponibilità e la durabilità con cui il file system Amazon EFS archivia i dati all'interno di Regione AWS. Sono disponibili le seguenti opzioni per il tuo tipo di file system:

- Scegli Regionale per creare un file system che archivia dati e metadati in modo ridondante in tutte le zone di disponibilità all'interno di Regione AWS. È possibile creare inoltre target di montaggio per ogni zona di disponibilità in Regione AWS. Regionale offre i massimi livelli di disponibilità e durabilità.
- Scegli Zona singola per creare un file system che archivia dati e metadati in modo ridondante in tutte le zone di disponibilità all'interno di una singola zona di disponibilità. I file system che utilizzano classi di storage possono avere un solo target di montaggio. Questo target di montaggio deve trovarsi nella zona di disponibilità in cui viene creato il file system.

## Backup automatici

I backup automatici sono sempre abilitati per impostazione predefinita quando crei un file system utilizzando la console. Quando si utilizza la CLI o l'API per creare un file system, i backup automatici sono abilitati per impostazione predefinita solo quando si creano file system che utilizzano i file system della zona di disponibilità. Per ulteriori informazioni, consulta Backup automatici.

## Policy del ciclo di vita

la gestione del ciclo di vita utilizza le politiche del ciclo di vita per spostare automaticamente i file da e verso la classe di storage Infrequent Access (IA) a basso costo in base ai modelli di accesso. Quando si crea un file system utilizzando AWS Management Console, la politica del ciclo di vita del file system viene configurata con le seguenti impostazioni predefinite:

- Transizione a IA impostata su 30 giorni dall'ultimo accesso.
- TransitionToArchiveimpostato su 90 giorni dall'ultimo accesso.
- Transizione a standard impostato su Nessuno.

Quando crei un file system utilizzando l' AWS CLI API Amazon EFS o gli AWS SDK, non puoi impostare contemporaneamente una policy del ciclo di vita. È necessario attendere la creazione del file system e quindi utilizzare l'operazione PutLifecycleConfiguration API per aggiornare la policy del ciclo di vita. Per ulteriori informazioni, consulta Gestione dello storage del file system.

## Crittografia

Alla creazione di un file system, è possibile abilitare la crittografia dei dati memorizzati su disco. Se sul proprio file system si abilita la crittografia dei dati memorizzati su disco, tutti i dati e i metadati in esso memorizzati saranno crittografati. Successivamente, al montaggio del file system, è possibile abilitare la crittografia dei dati in transito. Per ulteriori informazioni sulla crittografia in Amazon EFS consulta Crittografia dei dati in Amazon EFS.

Per creare i target di montaggio dei file system nella VPC, è necessario specificare le sottoreti della VPC. La console precompila l'elenco delle VPC nel proprio account che appartengono alla Regione AWS selezionata. In primo luogo, si seleziona la VPC e quindi la console elenca le zone di disponibilità nella VPC. Per ogni zona di disponibilità, è possibile selezionare una sottorete dall'elenco o utilizzare la sottorete predefinita, se esistente. Dopo aver selezionato una sottorete, è possibile specificare un indirizzo IP disponibile nella sottorete o lasciare che Amazon EFS scelga un indirizzo.

## Modalità di velocità di trasmissione effettiva

È possibile scegliere tra tre modalità di throughput:

- Elastic (consigliata): offre una velocità di trasmissione effettiva scalabile automaticamente verso l'alto e verso il basso in tempo reale, per soddisfare le esigenze prestazionali del carico di lavoro.

> **Note**
>
> Il throughput elastico è disponibile solo per i file system con la modalità di prestazioni General Purpose.

- Con provisioning: fornisce il livello di throughput specificato, indipendentemente dalle dimensioni del file system.
- Bursting: fornisce un throughput scalabile in base alla quantità di dati nello storage Standard.

Per ulteriori informazioni, consulta Modalità di velocità di trasmissione effettiva.

> **Note**
>
> Alla modalità di Throughput Elastic e con provisioning sono associati dei costi aggiuntivi. Per ulteriori informazioni, consulta Prezzi di Amazon EFS.

## Modalità prestazionali

Quando si crea un file system, è anche possibile scegliere una modalità prestazionale. È possibile scegliere tra due modalità: General Purpose e Max I/O.

- La Modalità a scopi generali ha la latenza per operazione più bassa ed è la modalità consigliata per i file system.
- Max I/O è un tipo di prestazioni della generazione precedente progettato per carichi di lavoro altamente parallelizzati in grado di tollerare latenze più elevate rispetto alla modalità General Purpose. La modalità I/O max non è supportata per i file system a zona singola o per i file system che utilizzano la velocità di trasmissione effettiva Elastic.

> **Important**
>
> A causa delle più elevate latenze per operazione con I/O max, consigliamo di utilizzare la modalità prestazionale a scopi generali per tutti i file system.

Per ulteriori informazioni, consulta Modalità prestazionali.

## Creazione di un file system con impostazioni personalizzate utilizzando la console Amazon EFS

Questa sezione descrive il processo di utilizzo della console Amazon EFS per creare un file system EFS con impostazioni personalizzate anziché utilizzare le impostazioni consigliate dal servizio. Per ulteriori informazioni sulla creazione di un file system con le impostazioni consigliate dal servizio, consulta Fase 1: Creazione di un file system Amazon EFS.

La creazione di un file system Amazon EFS con impostazioni personalizzate utilizzando la console è un processo che si articola in quattro fasi:

- Fase 1 - Configurazione delle impostazioni generali del file system, tra cui la classe di storage e la modalità di throughput.
- Fase 2 - Configurazione delle impostazioni di rete del file system, tra cui il cloud privato virtuale (VPC) e i target di montaggio. Per ogni target di montaggio, imposta la zona di disponibilità, la sottorete, l'indirizzo IP e i gruppi di sicurezza.
- Fase 3 — (Facoltativo) Creare una policy del file system per controllare l'accesso del client NFS al file system.
- Fase 4 — Rivedere le impostazioni del file system, apportare eventuali modifiche e quindi creare il file system.

Fase 1: Configurazione delle impostazioni del file system

1. Accedi AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Scegli Crea file system per aprire la finestra di dialogo Crea file system.
3. Scegli Personalizza per creare un file system personalizzato anziché creare un file system utilizzando le impostazioni consigliate dal servizio. Viene visualizzata la pagina delle Impostazioni del file system.

4. Per le impostazioni Generali, effettua quanto segue.

   a. (Facoltativo) In Nome, immetti un nome per il file system.

   b. Per Tipo di file system, scegli un'opzione di disponibilità:

      - Scegli Regionale per creare un file system che archivia dati e metadati in modo ridondante in tutte le zone di disponibilità all'interno di Regione AWS. Regionale offre i massimi livelli di disponibilità e durabilità.
      - Scegli Zona singola per creare un file system che archivia dati e metadati in modo ridondante in tutte le zone di disponibilità all'interno di una singola zona di disponibilità. Se scegli Zona singola, seleziona la Zona di disponibilità in cui desideri creare il file system o mantieni il valore predefinito. Per ulteriori informazioni, consulta Classi di storage EFS.

   c. Per impostazione predefinita, i backup automatici sono attivati. È possibile disattivare i backup automatici deselezionando la casella di controllo. Per ulteriori informazioni, consulta Backup dei file system di Amazon EFS.

   d. Per la gestione del ciclo di vita, modifica le politiche relative al ciclo di vita, se necessario.

      - Transizione a IA: seleziona quando trasferire i file nella classe di storage Infrequent Access (IA), in base all'ora trascorsa dall'ultimo accesso ai file nello storage Standard.
      - Transizione all’archivio: seleziona quando trasferire i file nella classe di storage di archivio, in base all'ora trascorsa dall'ultimo accesso ai file nello storage Standard.
      - Transizione a Standard: seleziona se trasferire il file system alla classe di storage.

        Per ulteriori informazioni sulle policy del ciclo di vita consulta Gestione dello storage del file system.

   e. Per la Crittografia, la crittografia dei dati a riposo è abilitata per impostazione predefinita. Amazon EFS utilizza la tua AWS Key Management Service chiave di servizio EFS (`aws/elasticfilesystem`) per impostazione predefinita.AWS KMS Per scegliere una chiave KMS diversa da utilizzare per la crittografia, espandi Personalizza le impostazioni di crittografia e scegli una chiave dall'elenco. In alternativa, inserisci un ID chiave KMS o nome della risorsa Amazon (ARN) per la chiave KMS che desideri utilizzare.

      Se devi creare una nuova chiave, scegli Crea un AWS KMS key per avviare la AWS KMS console e creare una nuova chiave.

      È possibile disattivare la crittografia dei dati a riposo deselezionando la casella di controllo.

5. Nella impostazioni Prestazioni, esegui la seguente operazione:

a. Per la modalità Throughput, la modalità Elastic è selezionata per impostazione predefinita.

   - Per usare la velocità di trasmissione effettiva con provisioning, scegli Con provisioning, quindi, in Throughput con provisioning (MiB/s), inserisci la quantità di throughput da fornire per le richieste del file system. La quantità di Velocità di trasmissione effettiva massima in lettura appare come tre volte la quantità di velocità di trasmissione effettiva inserita.
   - Per utilizzare il bursting throughput, scegli Bursting.

   I file system Amazon EFS misurano le richieste di lettura a una velocità di un terzo rispetto alle altre richieste. Dopo aver inserito il throughput, viene mostrata una stima del costo mensile per il file system. È possibile modificare la modalità di trasmissione dopo che il file system diventa disponibile.

   Per ulteriori informazioni sulla scelta della modalità di throughput corretta per le tue esigenze di prestazioni, consulta Modalità di velocità di trasmissione effettiva.

b. In Modalità prestazioni, l'opzione predefinita è Scopi generici. Per modificare la modalità di prestazioni, espandi Impostazioni aggiuntive, quindi scegli Max I/O.

   Non è possibile modificare la modalità di prestazioni dopo che il file system è diventato disponibile. Per ulteriori informazioni, consulta Modalità prestazionali.

   > **Important**
   >
   > A causa delle più elevate latenze per operazione con I/O max, consigliamo di utilizzare la modalità prestazionale a scopi generali per tutti i file system.

6. (Facoltativo) Aggiungi coppie chiave-valore del tag al tuo file system.
7. Scegli Avanti per configurare l'accesso alla rete per il file system.

Fase 2: configurazione dell’accesso di rete

Nel passaggio 2, si configurano le impostazioni di rete del file system, inclusi il VPC e i target di montaggio.

1. Scegli il Virtual Private Cloud (VPC) a cui desideri che le istanze EC2 si connettano al tuo file system. Per ulteriori informazioni, consulta Gestione dell'accessibilità del file system dalla rete.

2. Per i target di montaggio, crei una o più target di montaggio per il tuo file system. Per ciascun target di montaggio, imposta le seguenti proprietà:

   - Zona di disponibilità: per impostazione predefinita, un target di montaggio è configurato in ogni zona di disponibilità in Regione AWS. Se non desideri un target di montaggio in una particolare zona di disponibilità, scegli Rimuovi per eliminare il target di montaggio per quella zona. Crea un target di montaggio in ogni zona di disponibilità da cui si prevede di accedere al file system: questa operazione non comporta costi.
   - ID di sottorete: scegli tra le sottoreti disponibili in una zona di disponibilità. La sottorete predefinita è preselezionata.
   - Indirizzo IP: per impostazione predefinita, Amazon EFS sceglie automaticamente l'indirizzo IP tra gli indirizzi disponibili nella sottorete. In alternativa, puoi inserire un indirizzo IP specifico che si trova nella sottorete. Sebbene i target di montaggio abbiano un unico indirizzo IP, sono risorse di rete ridondanti e ad alta disponibilità.
   - Gruppi di sicurezza: è possibile specificare uno o più gruppi di sicurezza per il target di montaggio. Per ulteriori informazioni, consulta Utilizzo di gruppi di sicurezza VPC per istanze Amazon EC2 e destinazioni di montaggio.

     Per aggiungere un altro gruppo di sicurezza o modificare il gruppo di sicurezza, scegli Scegli i gruppi di sicurezza e aggiungi un altro gruppo di sicurezza dall'elenco. Se non vuoi utilizzare il gruppo di sicurezza predefinito, puoi eliminarlo. Per ulteriori informazioni, consulta Creazione dei gruppi di sicurezza.
3. Scegli Aggiungi target di montaggio per creare un target di montaggio per una zona di disponibilità che non ne ha una. Se è configurato un target di montaggio per ogni zona di disponibilità, questa scelta non è disponibile.
4. Scegli Avanti per salvare la policy del file system.

### Fase 3: creazione di una policy del file system (opzionale)

Facoltativamente, è possibile creare una policy per il file system. Una policy di file system EFS è una policy di risorse IAM utilizzata per controllare l'accesso client NFS a un file system. Per ulteriori informazioni, consulta Utilizzo di IAM per controllare l'accesso ai dati del file system.

1. In Opzioni policy, puoi scegliere qualsiasi combinazione delle policy preconfigurate disponibili:

   - Impedisci l'accesso root per impostazione predefinita
   - Applica l'accesso in sola lettura per impostazione predefinita

- Applica la crittografia in transito per tutti i client

2. Utilizza l'editor delle policy per personalizzare una policy preconfigurata o per creare una policy personalizzata. Quando scegli una delle policy preconfigurate, la definizione della policy JSON viene visualizzata nell'editor delle policy. Puoi modificare il codice JSON per creare una policy a tua scelta. Per annullare le modifiche, scegli Annulla.

   Le policy preconfigurate sono nuovamente disponibili nelle Opzioni policy.
3. Scegli Avanti per rivedere e creare il file system.

Fase 4: Revisione e creazione

1. Esamina ciascuno dei gruppi di configurazione del file system. È possibile apportare modifiche a ciascun gruppo in questo momento scegliendo Modifica.
2. Scegli Crea per creare il tuo file system e tornare alla pagina File system.

   Un banner nella parte superiore mostra che il nuovo file system è in fase di creazione. Quando il file system diventa disponibile, nel banner viene visualizzato un collegamento per accedere alla pagina dei dettagli del file system.

## Creazione di un file system mediante AWS CLI

Quando si utilizza il AWS CLI, si creano queste risorse in ordine. Prima di tutto si crea il file system. Quindi, potete creare obiettivi di montaggio ed eventuali tag opzionali aggiuntivi per il file system utilizzando AWS CLI i comandi corrispondenti.

I seguenti esempi utilizzano `adminuser` come valore del parametro `--profile`. È necessario utilizzare un profilo utente appropriato per fornire le proprie credenziali. Per informazioni su AWS CLI, vedere Installazione di AWS CLI nella Guida per l'AWS Command Line Interface utente.

- Per creare un file system crittografato che utilizza le classi di storage EFS Archive, con i backup automatici abilitati, utilizza il comando `create-file-system` CLI di Amazon EFS (l'operazione corrispondente è CreateFileSystem), come illustrato di seguito.

```
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
```

Ad esempio, il seguente comando `create-file-system` crea un file system in `us-west-2` Regione AWS. Il comando specifica `MyFirstFS` come token di creazione. Per un elenco di applicazioni Regione AWS in cui è possibile creare un file system Amazon EFS, consulta il Riferimenti generali di 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
```

Dopo aver creato il file system, Amazon EFS restituisce la descrizione del file system in formato JSON, come mostrato nel seguente esempio.

```
{
    "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"
      }
   ]
}
```

- L'esempio seguente crea un file system che utilizza la classe di archiviazione Standard nella zona `us-west-2a` di disponibilità utilizzando la proprietà `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
```

Dopo aver creato il file system, Amazon EFS restituisce la descrizione del file system in formato JSON, come mostrato nel seguente esempio.

```
{
    "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 fornisce anche il comando CLI `describe-file-systems` (l'operazione API corrispondente è DescribeFileSystems) che è possibile utilizzare per recuperare l'elenco dei file system presenti nel proprio account, come illustrato di seguito.

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

Amazon EFS restituisce un elenco dei file system presenti nell'area Account AWS creata nella regione specificata.

## Cancellazione di un file system Amazon EFS

La cancellazione di un file system è un'azione distruttiva che non è possibile annullare. Comporta la perdita del file system e di tutti i dati in esso contenuti. Qualsiasi dato eliminato da un file system è perso e non è possibile ripristinarlo. Quando gli utenti eliminano i dati da un file system, tali dati sono immediatamente resi inutilizzabili. EFS sovrascrive forzatamente i dati in modo definitivo.

> **Note**
>
> Non è possibile eliminare un file system che fa parte di una configurazione di replica. La configurazione di replica deve prima essere eliminata. Per ulteriori informazioni, consulta Eliminazione di configurazioni di replica.

> **Important**
>
> È sempre consigliabile smontare un file system prima di eliminarlo.

## Utilizzo della console

Per eliminare un file system

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Scegli il file system che desideri eliminare dalla pagina File system.
3. Scegli Elimina.
4. Nella finestra di dialogo Elimina file system, immetti l'ID del file system visualizzato e scegli Conferma per confermare l'eliminazione.

   La console semplifica l'eliminazione del file system da parte dell'utente. Prima elimina i target di montaggio, quindi elimina il file system.

## Utilizzo della CLI

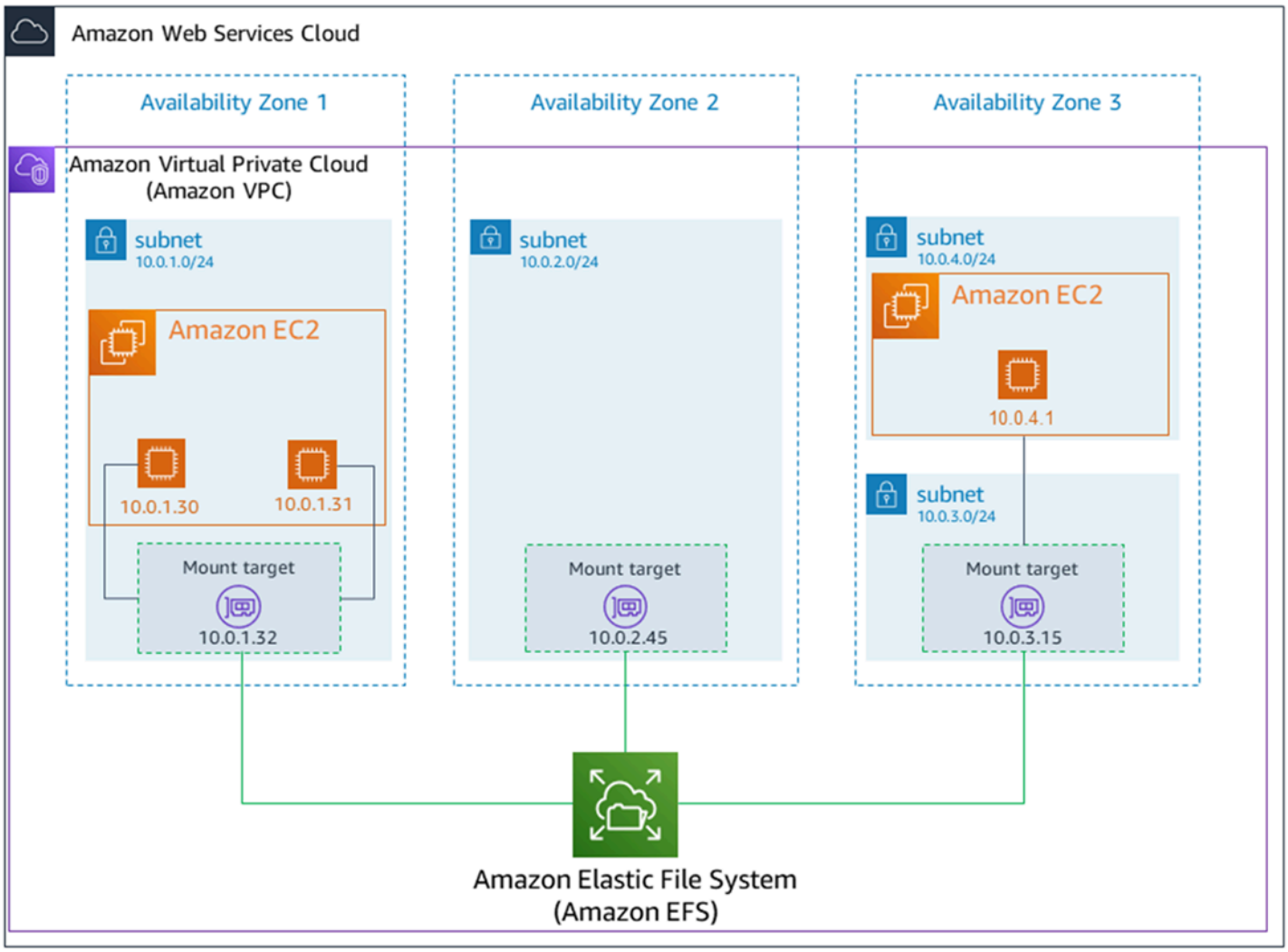
Prima di poter utilizzare il AWS CLI comando per eliminare un file system, è necessario eliminare tutte le destinazioni di montaggio e i punti di accesso creati per il file system.

Ad esempio, AWS CLI i comandi, vedereFase 4: Elimina.

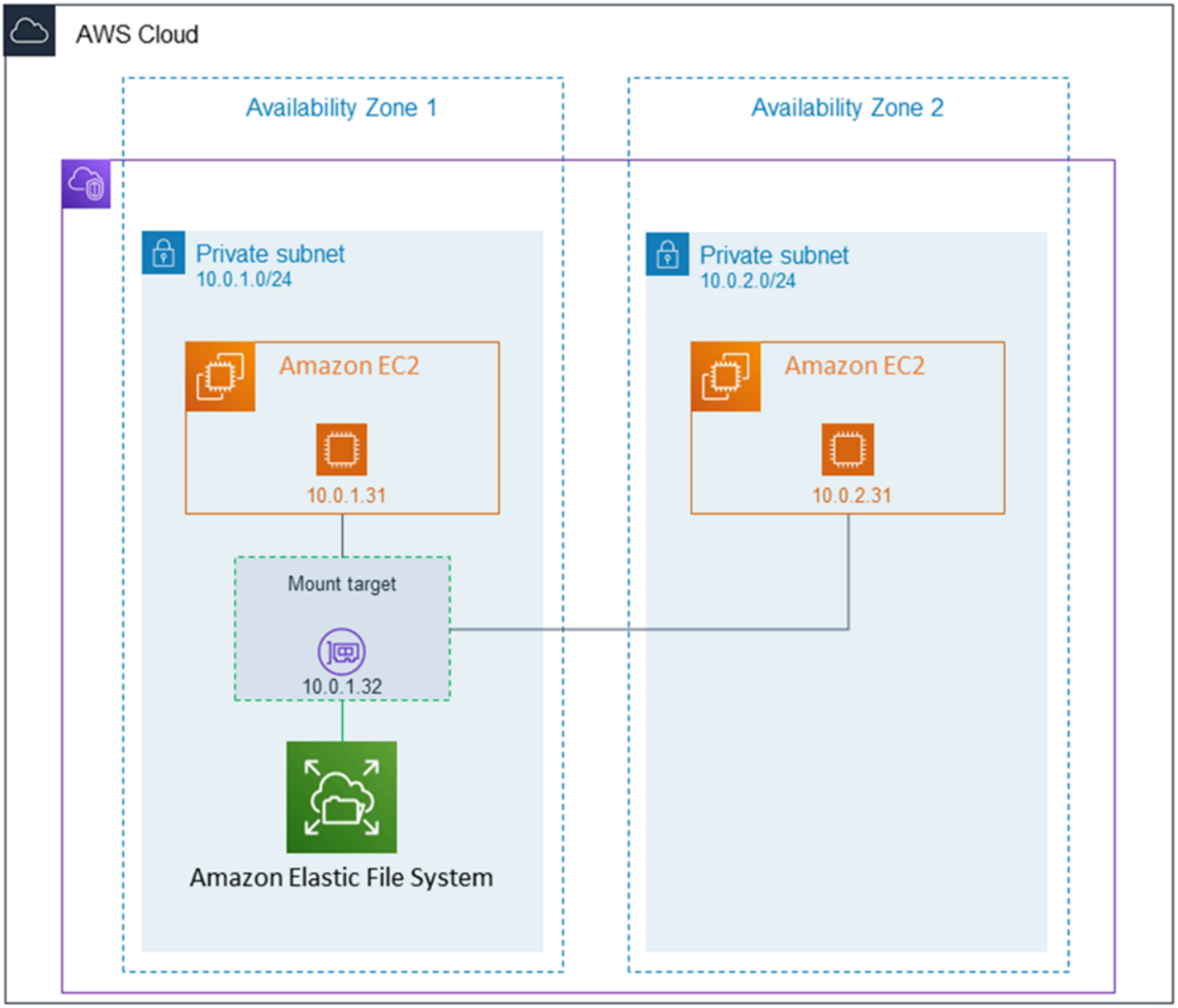
# Creazione e gestione di target di montaggio e gruppi di sicurezza

Dopo aver creato un file system Amazon EFS, puoi creare target di montaggio. Per i file system Amazon EFS che usano classi di storage regionali, puoi creare un target di montaggio in ogni zona di disponibilità di Regione AWS. Per i file system a zona singola, è possibile creare un solo target di montaggio nella stessa zona di disponibilità del file system. Quindi puoi montare il file system su istanze di calcolo, tra cui Amazon EC2, Amazon ECS AWS Lambda e nel tuo cloud privato virtuale (VPC).

Il diagramma seguente mostra un file system Amazon EFS che utilizza classi di storage Standard, con target di montaggio creati in tutte le zone di disponibilità del VPC.




Il diagramma seguente mostra un file system a zona singola, con un singolo target di montaggio creato nella stessa zona di disponibilità del file system. L'accesso al file system utilizzando l'istanza EC2 nella zona `us-west2c` di disponibilità comporta costi di accesso ai dati perché l'istanza si trova in una zona di disponibilità diversa rispetto al target di montaggio.




Il gruppo di sicurezza del target di montaggio agisce come un firewall virtuale che controlla il traffico. Ad esempio, determina quali client possono accedere al file system. Questa sezione descrive quanto segue:

- Gestione dei gruppi di sicurezza del target di montaggio e abilitazione del traffico.
- Montaggio del file system sui tuoi client.
- Considerazioni sulle autorizzazioni a livello di NFS.

  Inizialmente, solo l'utente root sull'istanza Amazon EC2 dispone read-write-execute delle autorizzazioni sul file system. Questa sezione illustra le autorizzazioni a livello di NFS e

fornisce esempi che illustrano come concedere le autorizzazioni in scenari comuni. Per ulteriori informazioni, consulta Utilizzo di utenti, gruppi e autorizzazioni a livello di Network File System (NFS).

Puoi creare destinazioni di montaggio per un file system utilizzando o a livello di codice utilizzando gli SDK. AWS Management Console AWS CLI AWS Quando si utilizza la console, è possibile creare target di montaggio quando si crea un file system o dopo la sua creazione.

Per istruzioni su come creare target di montaggio utilizzando la console Amazon EFS durante la creazione di un nuovo file system, consulta Fase 2: configurazione dell'accesso di rete.

## Gestione dei target di montaggio utilizzando la console di Amazon EFS

Utilizza la procedura seguente per aggiungere o modificare target di montaggio per un file system Amazon EFS esistente.

Gestione di target di montaggio su un file system Amazon EFS (console)

1. Accedi AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Nel pannello di navigazione a sinistra, scegli File system. La pagina File system mostra i file system EFS presenti nel tuo account.
3. Scegli il file system per cui desiderate gestire i target di montaggio selezionandone Nome o ID del file system per visualizzare la pagina dei dettagli del file system.
4. Scegli Rete per visualizzare l'elenco dei target di montaggio esistenti.
5. Scegli Gestisci per visualizzare la pagina della Zona di disponibilità e apportare le modifiche.

   In questa pagina, per i target di montaggio esistenti, è possibile aggiungere e rimuovere gruppi di sicurezza o eliminare il target di montaggio. È inoltre possibile creare nuovi target di montaggio.

   > **Note**
   >
   > Per i file system a zona singola, è possibile creare un singolo target di montaggio che si trovi nella stessa zona di disponibilità del file system.

   - Per rimuovere un gruppo di sicurezza da un target di montaggio, Scegli X accanto all'ID del gruppo di sicurezza.

- Per aggiungere un gruppo di sicurezza a un target di montaggio, scegli Seleziona gruppi di sicurezza per visualizzare un elenco di gruppi di sicurezza disponibili. In alternativa, inserisci un ID del gruppo di sicurezza nel campo di ricerca nella parte superiore dell'elenco.
- Per mettere in coda un target di montaggio per l'eliminazione, scegli Rimuovi.

> **Note**
>
> Prima di eliminare un target di montaggio, smonta il file system.

- Per aggiungere un target di montaggio, scegli Aggiungi target di montaggio. Questa opzione è disponibile solo per i file system che utilizzano classi di storage regionali EFS e se i target di montaggio non esistono già in ogni zona di disponibilità per Regione AWS.

6. Scegliere Salva per salvare le modifiche.

### Come modificare il VPC per un file system Amazon EFS (console)

Per modificare il VPC per la configurazione di rete di un file system, è necessario eliminare tutti i target di montaggio esistenti del file system.

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Nel pannello di navigazione a sinistra, scegli File system. La pagina File system mostra i file system EFS presenti nel tuo account.
3. Per il file system per cui desideri modificare VPC, scegli Nome o ID del file system. Viene visualizzata la pagina dei dettagli per il file system.
4. Scegli Rete per visualizzare l'elenco dei target di montaggio esistenti.
5. Scegli Gestisci. Viene visualizzata la pagina della zona di disponibilità.
6. Rimuovi tutti i target di montaggio visualizzati nella pagina.
7. Scegli Salva per salvare le modifiche ed eliminare i target di montaggio. La scheda Rete mostra lo stato di eliminazione dei target di montaggio.
8. Quando tutti gli stati dei target di montaggio vengono visualizzati come eliminati, scegli Gestisci. Viene visualizzata la pagina della zona di disponibilità.
9. Scegli il nuovo VPC dall'elenco Virtual Private Cloud (VPC).
10. Scegli Aggiungi target di montaggio per aggiungere un nuovo target di montaggio. Per ciascun target di montaggio aggiunto, immetti quanto segue:

- Una zone di disponibilità
- Un ID di sottorete
- Un indirizzo IP (in alternativa, mantienilo impostato su Automatico)
- Uno o più gruppi di sicurezza

11. Scegli Salva per implementare le modifiche al VPC e al target di montaggio.

## Gestione dei target di montaggio utilizzando AWS CLI

> **Note**
>
> Per i file system a zona singola, è possibile creare un singolo target di montaggio che si trovi nella stessa zona di disponibilità del file system.

Per creare un target di montaggio (CLI)

- Per creare un target di montaggio, utilizza il comando CLI `create-mount-target` (l'operazione corrispondente è CreateMountTarget), come mostrato qui di seguito.

```
$ 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
```

Il seguente esempio mostra il comando con i dati campione.

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

Dopo aver creato correttamente il target di montaggio, Amazon EFS restituisce la descrizione del target di montaggio in formato JSON, come mostrato nel seguente esempio.

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

Per recuperare un elenco di target di montaggio per un file system (CLI)

- È anche possibile ottenere un elenco dei target di montaggio creati per un file system utilizzando il comando CLI describe-mount-targets (l'operazione corrispondente è DescribeMountTargets), come mostrato qui di seguito.

```
$ 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"
        }
    ]
}
```

Per eliminare un target di montaggio esistente (CLI)

- Per eliminare un target di montaggio esistente, usa il `delete-mount-target` AWS CLI comando (l'operazione corrispondente èDeleteMountTarget), come illustrato di seguito.

> **Note**
>
> Prima di eliminare un target di montaggio di un file system, smontare il file system.

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

Di seguito vengono riportati dati campione per questo esempio.

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

Per modificare il gruppo di sicurezza di un target di montaggio esistente

- Per modificare i gruppi di sicurezza attivi per un target di montaggio, utilizzate il `modify-mount-target-security-group` AWS CLI comando (l'operazione corrispondente èModifyMountTargetSecurityGroups) per sostituire qualsiasi gruppo di sicurezza esistente, come illustrato di seguito.

```
$ 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
```

  Di seguito vengono riportati dati campione per questo esempio.

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

Per ulteriori informazioni, consulta Procedura dettagliata: Creazione di un file system Amazon EFS e montarlo su un'istanza Amazon EC2 utilizzandoAWS CLI.

## Creazione dei gruppi di sicurezza

> **Note**
>
> La sezione seguente è specifica per Amazon EC2 e illustra come creare gruppi di sicurezza in modo che sia possibile utilizzare Secure Shell (SSH) per connettersi a tutte le istanze che hanno montato un file system Amazon EFS. Se non si utilizza SSH per connettersi all'istanza Amazon EC2, è possibile ignorare questa sezione.

Sia l'istanza Amazon EC2 che un target di montaggio sono associati a dei gruppi di sicurezza. Questi gruppi di sicurezza fungono da firewall virtuale che controlla il traffico tra di essi. Se non si indica un gruppo di sicurezza durante la creazione di un target di montaggio, Amazon EFS associa ad essa il gruppo di sicurezza predefinito della VPC.

Indipendentemente da ciò, per abilitare il traffico tra un'istanza EC2 e un target di montaggio (e quindi verso il file system), è necessario configurare le seguenti regole in questi gruppi di sicurezza:

- I gruppi di sicurezza associati a un target di montaggio devono consentire l'accesso in entrata tramite protocollo TCP sulla porta NFS da tutte le istanze EC2 su cui si desidera montare il file system.
- Ogni istanza EC2 che monta il file system deve disporre di un gruppo di sicurezza che consente l'accesso in uscita verso il target di montaggio sulla porta NFS.

Per modificare i gruppi di sicurezza associati ai target di montaggio dei file system EFS, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

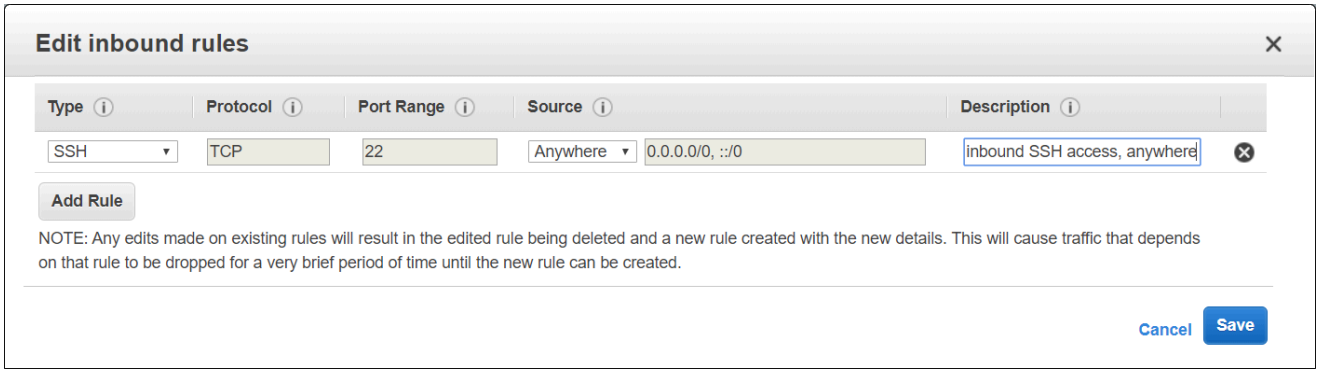
Per ulteriori informazioni sui gruppi di sicurezza, consulta Gruppi di sicurezza Amazon EC2 nella Guida per l'utente di Amazon EC2 per istanze Linux.

## Creazione di gruppi di sicurezza tramite AWS Management Console

Puoi usare il AWS Management Console per creare gruppi di sicurezza nel tuo VPC. Per collegare il file system Amazon EFS all'istanza Amazon EC2, è necessario creare due gruppi di sicurezza: uno per l'istanza Amazon EC2 e un altro per il target di montaggio di Amazon EFS.

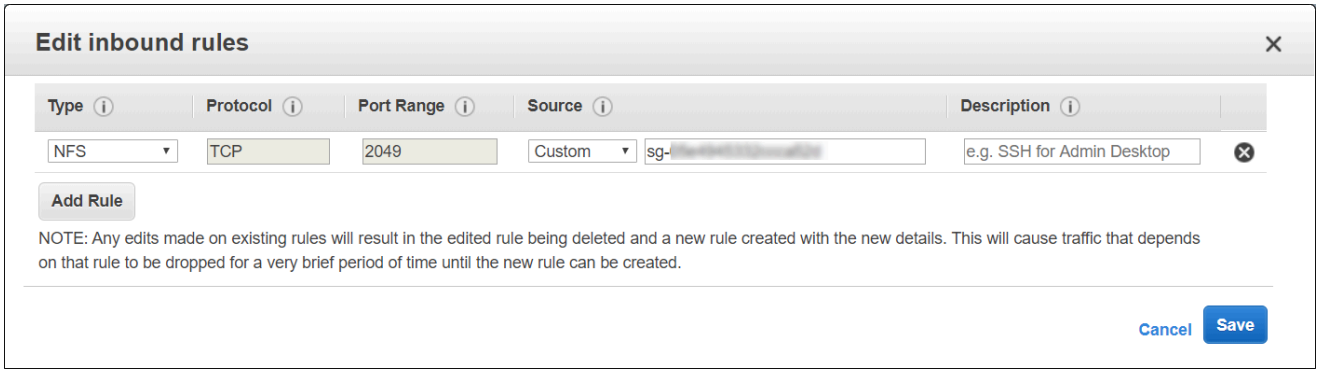
1. Creare due gruppi di sicurezza nella VPC. Per le istruzioni, consulta Creazione di un gruppo di sicurezza nella Guida per l'utente di Amazon VPC.
2. Nella console VPC, verificare le regole di default per questi gruppi di sicurezza. Entrambi i gruppi di sicurezza dovrebbero avere solo una regola in uscita che consente l'uscita del traffico.
3. È necessario autorizzare un accesso aggiuntivo per i gruppi di sicurezza come segue:

    a. Aggiungere una regola al gruppo di sicurezza di EC2 per consentire l'accesso SSH all'istanza sulla porta 22, come illustrato di seguito. Questo è utile se si prevede di utilizzare un client SSH come PuTTY per connettersi e amministrare l'istanza EC2 tramite l'interfaccia del terminale. Facoltativamente, è possibile limitare l'indirizzo Origine.




Per istruzioni, consulta Aggiunta, eliminazione e aggiornamento delle regole nella Guida per l'utente di Amazon VPC.

b. Aggiungi una regola per il gruppo di sicurezza del target di montaggio per consentire l'accesso in entrata dal gruppo di sicurezza di EC2 sulla porta TCP 2049. Il gruppo di sicurezza nella colonna Origine è il gruppo di sicurezza associato all'istanza EC2.




Per visualizzare i gruppi di sicurezza associati ai target di montaggio dei file system, nella console EFS, scegli la scheda Rete nella pagina dei dettagli del file system. Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

> **Note**
>
> Non è necessario aggiungere una regola in uscita, perché la regola di default consente l'uscita di tutto il traffico. (Se si rimuove la regola in uscita predefinita, è necessario aggiungere una regola in uscita per aprire una connessione TCP sulla porta NFS e identificare il gruppo di sicurezza del target di montaggio come destinazione).

4. Verificare che entrambi i gruppi di sicurezza autorizzino l'accesso in ingresso e in uscita come descritto in questa sezione.

## Creazione di gruppi di sicurezza tramite AWS CLI

Per un esempio che mostra come creare gruppi di sicurezza utilizzando il AWS CLI, vediFase 1: Creazione delle risorse Amazon EC2.

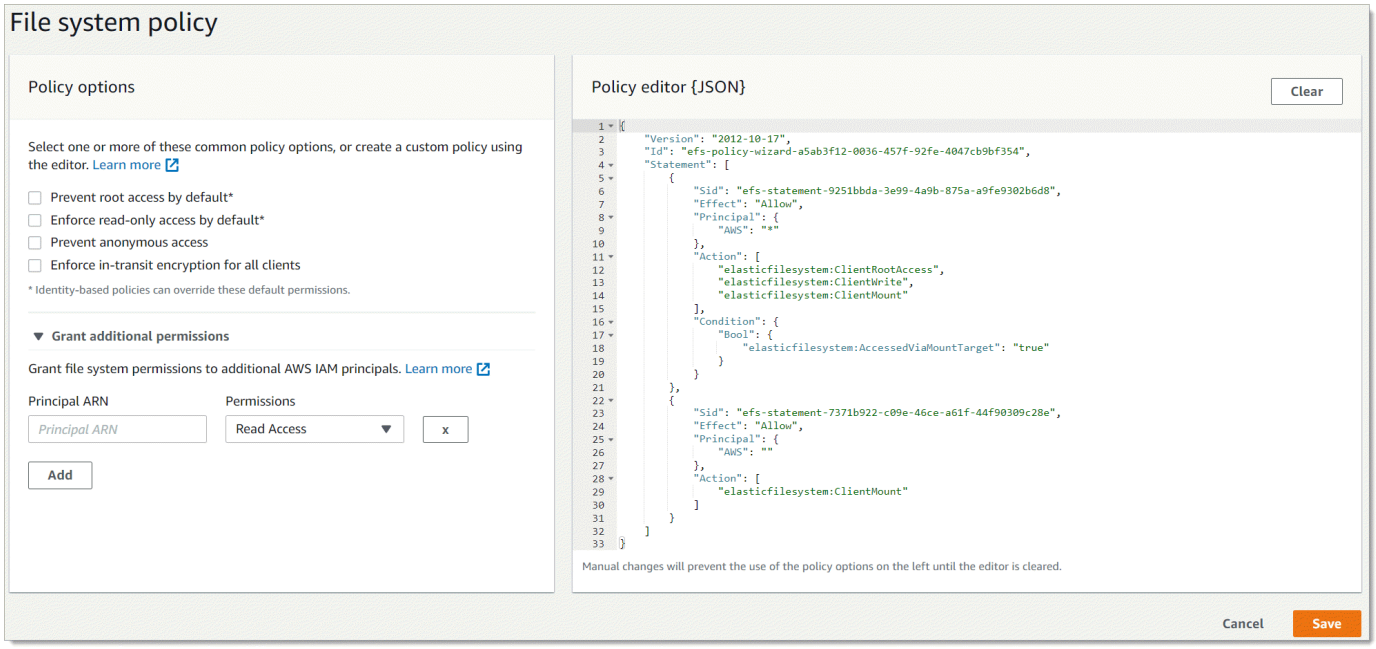
# Creazione di policy del file system

È possibile creare un file system utilizzando la console Amazon EFS o utilizzando AWS CLI. Puoi anche creare una policy del file system a livello di codice utilizzando gli AWS SDK o direttamente l'API Amazon EFS. Le policy del file system EFS hanno un limite di 20.000 caratteri. Per ulteriori informazioni sull'utilizzo di una policy del file system EFS ed esempi, consulta Utilizzo di IAM per controllare l'accesso ai dati del file system.

> **Note**
>
> Le modifiche alle policy del file system di Amazon EFS possono richiedere diversi minuti per diventare effettive.

### Creazione di una policy del file system (Console)

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Selezionare File Systems (File system).
3. Nella pagina File systems (File system), scegli il file system per cui vuoi creare una policy di file system. Viene visualizzata la pagina dei dettagli per il file system scelto.
4. Scegli Policy del file system, quindi scegli Modifica. Viene visualizzata la pagina Policy del file system.




5. Nelle Opzioni policy, puoi scegliere qualsiasi combinazione delle policy preconfigurate del file system:

   - Impedisci l'accesso root per impostazione predefinita: questa opzione rimuove `ClientRootAccess` dal set di azioni EFS consentite.
   - Applica l'accesso root per impostazione predefinita: questa opzione rimuove `ClientWriteAccess` dal set di azioni EFS consentite.
   - Impedisci l'accesso anonimo: questa opzione rimuove `ClientMount` dal set di azioni EFS consentite.
   - Applica la crittografia in transito per tutti i client: questa opzione nega l'accesso ai client non crittografati.

   Quando si sceglie una policy preconfigurata, l'oggetto JSON della policy viene visualizzato nel riquadro dell'editor delle policy.

6. Usa Grant additional permissions per concedere autorizzazioni di file system a principali IAM aggiuntivi, inclusi altri. Account AWS Scegli Aggiungi e inserisci l'ARN principale dell'entità a cui stai concedendo le autorizzazioni. Scegli le Autorizzazioni che desideri concedere. Le autorizzazioni aggiuntive sono mostrate nell'editor delle policy.
7. È possibile utilizzare l'editor delle policy per personalizzare una policy preconfigurata o per creare una policy del file system personalizzata. Quando si utilizza l'editor, le opzioni di policy

preconfigurate non sono più disponibili. Per cancellare la policy corrente del file system e iniziare a creare una nuova policy, scegli Annulla.

Quando si rimuovo i dati dall'editor, le policy preconfigurate diventano nuovamente disponibili.

8. Dopo aver completato la modifica della policy, scegli Salva.

## Creazione di una policy del file system (CLI)

Nell'esempio seguente, il comando put-file-system-policyCLI crea una policy del file system che consente l'accesso in Account AWS sola lettura specificato al file system EFS. Il comando API equivalente è 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"
            }
        ]
    }
}
```

# Creazione ed eliminazione dei punti di accesso

Puoi creare punti di accesso Amazon EFS utilizzando AWS Management Console o il AWS CLI. Puoi anche creare punti di accesso in modo programmatico utilizzando direttamente gli AWS SDK o l'API Amazon EFS. Non è possibile modificare un punto di accesso dopo la sua creazione. Un file system può avere un massimo di 1.000 punti di accesso. Per ulteriori informazioni sui punti di accesso EFS, consulta Utilizzo dei punti di accesso Amazon EFS.

Le procedure seguenti descrivono come creare un punto di accesso utilizzando la console e AWS CLI.

## Creazione di un punto di accesso (Console)

Puoi creare ed eliminare punti di accesso Amazon EFS utilizzando AWS Management Console, the AWS Command Line Interface (AWS CLI) e l'API e gli SDK di Amazon EFS. Non è possibile modificare un punto di accesso dopo la sua creazione. Un file system può avere un massimo di 1.000 punti di accesso.

> **Note**
>
> Se più richieste di creazione di punti di accesso sullo stesso file system vengono inviate in rapida successione e il file system è vicino al limite di 1.000 punti di accesso, è possibile che si verifichi una risposta limitata per queste richieste. Ciò serve a garantire che il file system non superi il limite di punti di accesso dichiarato.

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Scegli Punti di accesso per aprire la finestra Punti di accesso.
3. Scegli Crea punti di accesso per visualizzare la pagina Crea punto di accesso.

Puoi anche aprire la pagina Crea punto di accesso scegliendo File system. Scegli un nome o un ID del file system, quindi scegli Punti di accesso e Crea punto di accesso per creare un punto di accesso per quel file system.

# Create access point

An access point is an application-specific entry point into an EFS file system that makes it easier to manage application access to shared datasets. Learn more

## Details

File system
Choose the file system to which your access point is associated.

Enter a file system name or ID

Name - *optional*

EFS access point name

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . _ : /

Root directory path - *optional*
Connections use the specified path as the file system's virtual root directory **Learn more**

Defaults to /

Example: "/foo/bar"

## POSIX user - *optional*

The full POSIX identity on the access point that is used for all file operations by NFS clients. **Learn more**

User ID
POSIX user ID used for all file system operations using this access point.

POSIX UID

Accepts values from 0 to 4294967295

Group ID
POSIX group ID used for all file system operations using this access point.

POSIX GID

Accepts values from 0 to 4294967295

Secondary group IDs
Secondary POSIX group IDs used for all file system operations using this access point.

Example: "123,456,789"

A comma-separated list of valid POSIX group IDs

## Root directory creation permissions - *optional*

EFS will automatically create the specified root directory with these permissions if the directory does not already exist. **Learn more**

Owner user ID
Owner user ID for the access point's root directory, if the directory does not already exist.

POSIX user ID to apply to path

Accepts values from 0 to 4294967295

Owner group ID
Owner group ID for the access point's root directory, if the directory does not already exist.

a. Nel pannello Dettagli immetti le seguenti informazioni:

   - File system: inserisci un nome o un ID del file system e scegli il file system corrispondente. Puoi anche scegliere il file system dall'elenco che appare quando scegli il campo di input.
   - (Facoltativo) Per Nome, immetti un nome per il punto di accesso.
   - (Facoltativo) Percorso della directory principale: è possibile specificare una directory principale per il punto di accesso; la radice del punto di accesso predefinita è /. Per inserire il percorso della directory principale, utilizza il formato`/foo/bar`. Per ulteriori informazioni, consulta Applicazione di una directory principale con un punto di accesso.

b. (Facoltativo) Nel pannello Utente POSIX, è possibile specificare l'identità POSIX completa da utilizzare per applicare le informazioni su utenti e gruppi per tutte le operazioni sui file da parte dei client NFS che utilizzano il punto di accesso. Per ulteriori informazioni, consulta Far rispettare l'identità di un utente utilizzando un punto di accesso.

   - ID utente - Immetti l'ID utente POSIX numerico dell'utente.
   - ID gruppo - Immetti l'ID numerico del gruppo POSIX dell'utente.
   - ID gruppi secondari - Immetti un elenco di ID gruppi secondari facoltativi separati da virgole.

c. (Facoltativo) Per Autorizzazioni di creazione della directory principale, puoi specificare le autorizzazioni da utilizzare quando Amazon EFS crea il percorso della directory principale, se specificato e la directory principale non esiste già. Per ulteriori informazioni, consulta Applicazione di una directory principale con un punto di accesso.

   > **Note**
   >
   > Se non si specifica alcuna proprietà e autorizzazione della directory principale e la directory principale non esiste già, EFS non creerà la directory principale. Qualsiasi tentativo di montare il file system utilizzando il punto di accesso avrà esito negativo.

   - ID utente proprietario: immetti l'ID utente POSIX numerico da utilizzare come proprietario della directory radice.
   - ID gruppo proprietario: immetti l'ID gruppo POSIX numerico da utilizzare come gruppo proprietario della directory radice.

- Permessi: immetti la modalità Unix della directory. Una configurazione comune è 755. Assicurati che il bit di esecuzione sia impostato per l'utente del punto di accesso in modo che sia in grado di eseguire il montaggio.

4. Scegli Crea punto di accesso per creare il punto di accesso utilizzando questa configurazione.

## Creazione di un punto di accesso (CLI)

Nell'esempio seguente, il comando CLI `create-access-point` crea un punto di accesso per il file system EFS. Il comando API equivalente è CreateAccessPoint.

```
aws efs create-access-point --file-system-id fs-abcdef0123456789a --client-token
 010102020-3 \
--root-directory “Path=/efs/mobileapp/
east,CreationInfo={OwnerUid=0,OwnerGid=11,Permissions=775}” \
--posix-user “Uid=22,Gid=4” \
--tags Key=Name,Value=east-users
```

Se la richiesta ha esito positivo, la CLI risponde con la descrizione del punto di accesso.

```
{
    "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**
>
> Se più richieste di creazione di punti di accesso sullo stesso file system vengono inviate in rapida successione e il file system è vicino al limite di 1.000 punti di accesso, è possibile che si verifichi una risposta limitata per queste richieste. Ciò serve a garantire che il file system non superi il limite di punti di accesso dichiarato.

## Eliminazione di un punto di accesso

Quando elimini un punto di accesso, tutti i client che lo utilizzano perdono l'accesso al file system Amazon EFS per cui è configurato.

Eliminazione di un punto di accesso (Console)

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso per aprire la pagina Punti di accesso.
3. Seleziona il punto di accesso da eliminare.
4. Scegli Elimina.
5. Scegli Conferma per confermare l'azione ed eliminare il punto di accesso.

Eliminazione di un punto di accesso (CLI)

Nell'esempio seguente, il comando `delete-access-point` CLI elimina il punto di accesso specificato. Il comando API equivalente è DeleteAccessPoint. Se il comando riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

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

# Aggiunta di tag alle risorse Amazon ECS

Per semplificare la gestione delle risorse Amazon EFS, è possibile assegnare metadati personalizzati a ciascuna risorsa sotto forma di tag. Con i tag, puoi classificare AWS le tue risorse in diversi modi,

ad esempio per scopo, proprietario o ambiente. Questa classificazione è molto utile quando hai tante risorse dello stesso tipo in quanto puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Questo argomento descrive i tag e mostra come crearli.

## Nozioni di base sui tag

Un tag è un'etichetta che si assegna a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag consentono di classificare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ad esempio, puoi definire un set di tag per i file system Amazon ECR del tuo account che consentono di monitorare ogni proprietario del repository.

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Con un set di chiavi di tag coerente, la gestione delle risorse risulta semplificata. Puoi cercare e filtrare le risorse in base ai tag aggiunti.

I tag non hanno alcun significato semantico per Amazon ECS e vengono interpretati rigorosamente come una stringa di caratteri. Inoltre, i tag non vengono assegnati automaticamente alle risorse. Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

## Assegnazione di tag alle risorse

Puoi assegnare tag alle risorse del file system e dei punti di accesso di Amazon EFS già esistenti nel tuo account.

Puoi utilizzare la console Amazon EFS per applicare tag alle risorse esistenti utilizzando la scheda Tag nella schermata dei dettagli delle risorse. Nella console Amazon EFS, puoi specificare i tag per una risorsa quando la crei. Ad esempio, puoi aggiungere un tag con una chiave `Name` e un valore specificato dall'utente. Nella maggior parte dei casi, la console applica i tag subito dopo la creazione della risorsa, anziché durante il processo di creazione. La console può organizzare le risorse in base al relativo tag `Name` ma questo tag non ha un significato semantico per il servizio Amazon EFS.

Se utilizzi l'API Amazon EFS o un AWS SDK AWS CLI, puoi utilizzare l'azione API `TagResource` EFS per applicare tag alle risorse esistenti. Inoltre, alcune operazioni per la creazione di risorse ti consentono di specificare tag per una risorsa durante la sua creazione.

I AWS CLI comandi per la gestione dei tag e le azioni API Amazon EFS equivalenti sono elencati nella tabella seguente.

| Comando CLI | Descrizione | Operazione API equivalente |
| --- | --- | --- |
| tag-resource | Aggiungere nuovi tag o aggiornare i tag esistenti | TagResource |
| list-tags-for-resource | Recuperare i tag esistenti | ListTagsForResource |
| untag-resource | Eliminare i tag esistenti | UntagResource |

## Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- Lunghezza massima della chiave: 128 caratteri Unicode in formato UTF-8
- Lunghezza massima del valore: 256 caratteri Unicode in formato UTF-8
- Sebbene Amazon EFS consenta l'uso di qualsiasi carattere nei tag, altri servizi presentano limitazioni più restrittive. I caratteri consentiti nei servizi sono: lettere, numeri e spazi rappresentabili in formato UTF-8 e i seguenti caratteri speciali + – = . _ : / @.
- Per chiavi e valori di tag viene fatta la distinzione tra maiuscole e minuscole.
- Il `aws:` prefisso è riservato all' AWS uso. Se il tag ha una chiave di tag con questo prefisso, non puoi modificare o eliminare la chiave o il valore de tag. I tag con il prefisso `aws:` non vengono conteggiati per il limite del numero di tag per risorsa.

Non puoi aggiornare o eliminare una risorsa solo sulla base dei relativi tag. Devi specificare il relativo identificatore. Ad esempio, per eliminare i file system con tag associati a una chiave di tag denominata `DeleteMe`, devi utilizzare l'operazione `DeleteFileSystem` con gli identificatori di risorsa del file system, ad esempio `fs-1234567890abcdef0`.

Quando si aggiungono tag a risorse pubbliche o condivise, i tag assegnati sono disponibili solo per Account AWS. Nessun altro Account AWS avrà accesso a quei tag. Per il controllo dell'accesso

basato su tag alle risorse condivise, ognuno Account AWS deve assegnare il proprio set di tag per controllare l'accesso alla risorsa.

È possibile etichettare il file system Amazon EFS e le risorse dei punti di accesso.

## Utilizzo di tag per il controllo degli accessi

È possibile utilizzare i tag per controllare l'accesso alle risorse Amazon EFS e per implementare il controllo degli accessi basato su attributi (ABAC).

> **Note**
>
> la replica non supporta l'utilizzo di tag per il controllo degli accessi basato sugli attributi (ABAC).

# Backup dei file system di Amazon EFS

Amazon Elastic File System offre un'interfaccia standard ai file system che supporta la semantica di accesso completa. Utilizzando il Network File System (NFS) versione 4.1 (NFSv4.1), è possibile montare il file system Amazon EFS su qualsiasi istanza Amazon Elastic Compute Cloud (Amazon EC2) basata su Linux. Dopo aver montato il sistema, è possibile lavorare con i file e le directory secondo le stesse modalità applicate per i file system locali. Per ulteriori informazioni sul montaggio, consultare Montaggio dei file system EFS.

Una volta creato un file system e dopo averlo montato su un istanza EC2, per utilizzare in modo efficace il file system devi conoscere come gestire le autorizzazioni a livello di NFS per utenti, gruppi e risorse correlate. Quando si crea il file system, è disponibile solo una directory principale all'indirizzo `/`. Per impostazione predefinita, solo l'utente root (UID 0) dispone delle read-write-execute autorizzazioni. Affinché gli altri utenti possano modificare il file system, l'utente root deve esplicitamente concedere loro l'accesso. Utilizzare i punti di accesso EFS per effettuare il provisioning di directory scrivibili da un'applicazione specifica. Per ulteriori informazioni, consultare Utilizzo di utenti, gruppi e autorizzazioni a livello di Network File System (NFS) e Utilizzo dei punti di accesso Amazon EFS.

## Argomenti correlati

Amazon EFS: come funziona

Nozioni di base

Procedure guidate

# Utilizzo degli amazon-efs-utils strumenti

Il pacchetto `amazon-efs-utils` è una raccolta open source di strumenti Amazon EFS, nota anche come client Amazon EFS. Di seguito, puoi trovare una descrizione del client Amazon EFS. Il client Amazon EFS include l'helper di montaggio Amazon EFS, che semplifica il montaggio dei file system EFS. L'uso del client EFS consente di utilizzare Amazon CloudWatch per monitorare lo stato di montaggio di un file system EFS. È necessario installare il client Amazon EFS su un'istanza Amazon EC2 prima di montare un file system EFS.

Argomenti



## Panoramica

Il client Amazon EFS (`amazon-efs-utils`) è una raccolta open source di strumenti Amazon EFS. Non sono previsti costi aggiuntivi per l'utilizzo del client Amazon EFS, che puoi scaricare da GitHub qui: https://github.com/aws/efs-utils. Il pacchetto `amazon-efs-utils` è disponibile nel repository dei pacchetti Amazon Linux, ed è possibile compilare e installare il pacchetto su altre distribuzioni Linux. Puoi anche utilizzare AWS Systems Manager per installare o aggiornare automaticamente il pacchetto. Per ulteriori informazioni, consulta Utilizzo di AWS Systems Manager per installare o aggiornare automaticamente i client Amazon EFS.

> **Note**
>
> Il pacchetto `amazon-efs-utils` viene preinstallato su Amazon Linux e Amazon Linux 2 Amazon Machine Image (AMI).

Il client Amazon EFS include un supporto di montaggio e strumenti che semplificano l'esecuzione della crittografia dei dati in transito per i file system Amazon EFS. Un helper di montaggio è un

programma che si utilizza quando si installa uno specifico tipo di file system. Si consiglia di utilizzare l'helper di montaggio incluso nel client Amazon EFS per montare i file system Amazon EFS. L'uso del client Amazon EFS semplifica il montaggio dei file system EFS e può fornire migliori prestazioni del file system. Per ulteriori informazioni sull'uso del client EFS e dell'helper di montaggio, consulta Montaggio dei file system EFS.

Quando si installa il pacchetto `amazon-efs-utils`, vengono installate le seguenti dipendenze esistenti per `amazon-efs-utils`:

- Client NFS
  - `nfs-utils` per distribuzioni RHEL, CentOS, Amazon Linux e Fedora
  - `nfs-common` per distribuzioni Debian e Ubuntu
- Relay di rete (pacchetto stunnel, versione 4.56 o successiva)
- Python (versione 3.4 o successiva)
- OpenSSL versione 1.0.2 o successiva

> **Note**
>
> Per impostazione predefinita, quando utilizzi l'helper di montaggio di con Transport Layer Security (TLS), viene eseguita la verifica del certificato associato al nome dell'host. L'helper di montaggio di Amazon EFS utilizza il programma `stunnel` per la sua funzionalità TLS. Alcune versioni di Linux non includono una versione di `stunnel` che supporta queste funzionalità di TLS per impostazione predefinita. Quando si utilizza una di tali versioni di Linux, il montaggio di un file system Amazon EFS con l'utilizzo di TLS ha esito negativo. Dopo l'installazione del pacchetto `amazon-efs-utils`, per effettuare l'upgrade della versione di stunnel del sistema, consulta Aggiornamento di `stunnel`.
> Puoi utilizzarlo AWS Systems Manager per gestire i client Amazon EFS e automatizzare le attività richieste per installare o aggiornare il amazon-efs-utils pacchetto sulle tue istanze EC2. Per ulteriori informazioni, consulta Utilizzo di AWS Systems Manager per installare o aggiornare automaticamente i client Amazon EFS.
> Per problemi relativi alla crittografia, consultare Risoluzione dei problemi di crittografia.

## Distribuzioni supportate

Il client Amazon EFS è stato verificato rispetto alle seguenti distribuzioni Linux e Mac:

| Distribuzione | Tipo di pacchetto | Sistema **`init`** |
|---|---|---|
| Amazon Linux 2023 (AL2023) | rpm | `systemd` |
| Amazon Linux 2017.09 | rpm | `upstart` |
| Amazon Linux 2 | rpm | `systemd` |
| CentOS 7, 8 | rpm | `systemd` |
| Debian 9, 10 | deb | `systemd` |
| Fedora 28 - 32 | rpm | `systemd` |
| macOS Big Sur | | `launchd` |
| macOS Monterey | | `launchd` |
| macOS Ventura | | `launchd` |
| OpenSUSE Leap, Tumbleweed | rpm | `systemd` |
| Oracle8 | 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` |

Per un elenco completo delle distribuzioni supportate rispetto alle quali il pacchetto è stato verificato, consulta `amazon-efs-utils` README su Github.

Nelle sezioni seguenti sono descritte le procedure di installazione del client Amazon EFS sulle istanze EC2 Linux e Mac.

# Utilizzo di AWS Systems Manager per installare o aggiornare automaticamente i client Amazon EFS

Puoi utilizzare AWS Systems Manager per semplificare la gestione del client Amazon EFS (`amazon-efs-utils`). AWS Systems Manager è un servizio AWS che puoi utilizzare per visualizzare e controllare la tua infrastruttura su AWS. Con AWS Systems Manager puoi automatizzare le attività richieste per installare o aggiornare il pacchetto `amazon-efs-utils` sulle tue istanze EC2. Le funzionalità di Systems Manager come Distributor e State Manager consentono di automatizzare i seguenti processi:

- Mantenimento del controllo della versione sul client Amazon EFS.
- Archiviazione centralizzata e distribuzione sistematica del client Amazon EFS nelle istanze Amazon EC2.
- Automatizza il processo per mantenere le istanze Amazon EC2 gestite in un determinato stato.

Per ulteriori informazioni, consulta la Guida per l'utente di AWS Systems Manager.

## Comportamento del client Amazon EFS durante l'installazione

Utilizzi il client Amazon EFS per automatizzare il monitoraggio dei CloudWatch log di Amazon per lo stato di montaggio del file system e l'aggiornamento `stunnel` alla versione più recente per distribuzioni Linux selezionate. Quando installi il client Amazon EFS sulle istanze Amazon EC2 mediante Systems Manager, vengono eseguite le seguenti operazioni:

- Viene installato il pacchetto `botocore` utilizzando gli stessi passaggi descritti in Installazione di `botocore`. Il client Amazon EFS utilizza `botocore` per monitorare lo stato di montaggio del file system EFS.
- Consente il monitoraggio dello stato di montaggio del file system CloudWatch EFS nei log mediante l'aggiornamento`efs-utils.conf`. Per ulteriori informazioni, consulta Monitoraggio dello stato di successo o di fallimento del tentativo di montaggio.
- Per le istanze EC2 che eseguono `RHEL7` o `CentOS7`, il client Amazon EFS aggiorna automaticamente `stunnel` come descritto in Aggiornamento di `stunnel`. L'aggiornamento di `stunnel` è necessario per montare correttamente un file system EFS utilizzando TLS e la versione `stunnel` fornita con `RHEL7` e `CentOS7` non supporta il cliente Amazon EFS (`amazon-efs-utils`).

## Sistemi operativi supportati per Systems Manager Distributor

Le tue istanze EC2 devono eseguire uno dei seguenti sistemi operativi per poter essere utilizzate con AWS Systems Manager per aggiornare o installare automaticamente il client Amazon EFS.

| Piattaforma | Versione della piattaforma | Architettura |
|---|---|---|
| Amazon Linux | 2017,09, 2018,03 | x86_64 |
| Amazon Linux 2 | 2.0 | x86_64, arm64 (Amazon Linux 2, tipi di istanza A1) |
| CentOS | 7, 8 | x86_64 |
| Red Hat Enterprise Linux (RHEL) | 7, 8 | x86_64, arm64 (RHEL 7.6 e versioni successive, tipi di istanza A1) |
| SUSE Linux Enterprise Server (SLES) | 12, 15 | x86_64 |
| Ubuntu Server | 16,04, 18,04, 20,04 | x86_64, arm64 (Ubuntu 16 e versioni successive, tipi di istanza A1) |

## Come usare per installare AWS Systems Manager o aggiornare automaticamente amazon-efs-utils

Sono necessarie due configurazioni monouso per configurare Systems Manager per installare o aggiornare automaticamente il amazon-efs-utils pacchetto.

1. Configura un profilo di istanza AWS Identity and Access Management (IAM) con le autorizzazioni richieste.
2. Configura un'associazione (inclusa la pianificazione) utilizzata per l'installazione o gli aggiornamenti da parte dello State Manager

### Fase 1: Configurazione di un profilo di istanza IAM con le autorizzazioni richieste

Per impostazione predefinita, AWS Systems Manager non dispone dell'autorizzazione per gestire i client Amazon EFS e installare o aggiornare il amazon-efs-utils pacchetto. Devi concedere l'accesso a Systems Manager utilizzando un profilo dell'istanza AWS Identity and Access Management (IAM). Un profilo dell'istanza è un container che trasferisce le informazioni sul ruolo IAM a un'istanza EC2 all'avvio.

Utilizza la policy di autorizzazione `AmazonElasticFileSystemsUtils` AWS gestita per assegnare le autorizzazioni appropriate ai ruoli. Puoi creare un nuovo ruolo per il profilo dell'istanza o aggiungere la policy `AmazonElasticFileSystemsUtils` di autorizzazione a un ruolo esistente. È quindi necessario utilizzare questo profilo dell'istanza per avviare le istanze Amazon EC2. Per ulteriori informazioni, consulta Fase 4: Creazione di un profilo dell'istanza IAM per Systems Manager.

### Fase 2: Configurazione di un'associazione utilizzata da State Manager per l'installazione o l'aggiornamento del client Amazon EFS

Il pacchetto `amazon-efs-utils` è incluso nel Distributor ed è pronto per l'implementazione su istanze EC2 gestite. Per visualizzare l'ultima versione di `amazon-efs-utils` disponibile per l'installazione, è possibile utilizzare la console AWS Systems Manager o lo strumento a riga di comando AWS preferito. Per accedere a Distributor, apri https://console.aws.amazon.com/systems-manager/ e scegli Distributor nel riquadro di navigazione a sinistra. Individua AmazonEFSUtils nella sezione Proprietà di Amazon. Scegli AmazonEFSUTils per vedere i dettagli del pacchetto. Per ulteriori informazioni, consulta Visualizzazione di pacchetti.

Utilizzando State Manager, puoi installare o aggiornare il pacchetto `amazon-efs-utils` sulle istanze EC2 gestite immediatamente o secondo una pianificazione. Inoltre, puoi assicurarti che `amazon-efs-utils` venga installato automaticamente sulle nuove istanze EC2. Per ulteriori informazioni sull'installazione o l'aggiornamento dei pacchetti utilizzando Distributor e State Manager, consulta Operazioni con Distributor.

Per installare o aggiornare automaticamente il amazon-efs-utils pacchetto sulle istanze che utilizzano la console Systems Manager, vedere Pianificazione dell'installazione o dell'aggiornamento di un pacchetto (console). Ciò richiederà di creare un'associazione per State Manager, che definisce lo stato da applicare a un set di istanze. Utilizza i seguenti input quando create l'associazione:

- Per Parametri scegli Azione > Installa e Tipo di installazione > Aggiornamento in loco.
- Per Target, l'impostazione consigliata è Scegli tutte le istanze per registrare tutte le istanze EC2 nuove ed esistenti come destinazioni per installare o aggiornare automaticamente

AmazonEFSUtils. In alternativa, puoi specificare i tag delle istanze, selezionare le istanze manualmente o scegliere un gruppo di risorse per applicare l'associazione a un sottoinsieme di istanze. Se specifichi i tag delle istanze, devi avviare le istanze EC2 con i tag per consentire a AWS Systems Manager di installare o aggiornare automaticamente il client Amazon EFS.

- Per Specifica pianificazione, l'impostazione consigliata per AmazonEFSUTils è ogni 30 giorni. Puoi utilizzare i controlli per creare una pianificazione cron o rate per l'associazione.

Per usare AWS Systems Manager per montare più file system Amazon EFS su più istanze EC2, consulta Montaggio di EFS su più istanze EC2 utilizzando AWS Systems Manager.

# Installazione manuale del client Amazon EFS

Puoi installare manualmente il client Amazon EFS sulle tue istanze Amazon EC2 Linux che eseguono Amazon Linux e Amazon Linux 2 e altre distribuzioni Linux supportate e su istanze Mac EC2 che eseguono macOS Big Sur, macOS Monterey e macOS Ventura. Le procedure di installazione `amazon-efs-utils` per questi sistemi operativi sono descritte nelle sezioni seguenti.

Argomenti

- Installazione del client Amazon EFS su Amazon Linux e Amazon Linux 2
- Installazione del client Amazon EFS su altre distribuzioni Linux
- Installazione del client Amazon EFS su istanze Mac EC2 che eseguono macOS Big Sur, macOS Monterey o macOS Ventura

## Installazione del client Amazon EFS su Amazon Linux e Amazon Linux 2

Il pacchetto `amazon-efs-utils` per l'installazione su Amazon Linux e Amazon Linux 2 è disponibile nelle seguenti posizioni:

- I repository di pacchetti Amazon Linux e Amazon Linux 2 Amazon Machine Image (AMI).
- Il repository AWS efs-utils GitHub .

La procedura seguente descrive come eseguire l'installazione di `amazon-efs-utils` dagli archivi di pacchetti AMI Amazon Linux e Amazon Linux 2.

È inoltre possibile eseguire l'installazione o l'aggiornamento `amazon-efs-utils` dal repository efs-utils. AWS GitHub Per istruzioni che descrivono come installare e aggiornare il client Amazon EFS

utilizzando GitHub, consulta Compilare e installare `amazon-efs-utils` come pacchetto RPM per Amazon Linux, Amazon Linux 2.

Per installare il client Amazon EFS su altre distribuzioni Linux, consulta Installazione del client Amazon EFS su altre distribuzioni Linux.

> **Note**
>
> Se si utilizza AWS Direct Connect, è possibile trovare le istruzioni di installazione in Procedura dettagliata: creare e montare un file system in locale con una VPN AWS Direct Connect.

Per installare il pacchetto **`amazon-efs-utils`** su Amazon Linux 2 e Amazon Linux

1. assicurati di aver creato un'istanza EC2 Amazon Linux o Amazon Linux 2. Per ulteriori informazioni, consulta Fase 1: Avvio di un'istanza nella Guida per l'utente di Amazon EC2 per istanze Linux.
2. Accedi al terminale dell'istanza utilizzando SSH (Secure Shell) e accedi con il nome utente opportuno. Per ulteriori informazioni sulla procedura, consulta Connessione all'istanza Linux tramite SSH nella Guida per l'utente di Amazon EC2 per le istanze Linux.
3. Per installare il pacchetto `amazon-efs-utils`, esegui il comando seguente.

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

## Passaggi successivi

Dopo l'installazione di `amazon-efs-utils` sulla tua istanza EC2, procedi con i passaggi successivi per il montaggio del file system:

- Installa `botocore` in modo da poter utilizzare Amazon CloudWatch per monitorare lo stato di montaggio del tuo file system.
- Esegui l'upgrade alla versione più recente di `stunnel` per abilitare la crittografia dei dati in transito.
- Installazione del file system utilizzando EFS Mount Helper.

# Installazione del client Amazon EFS su altre distribuzioni Linux

Se non desideri scaricare il `amazon-efs-utils` pacchetto dagli archivi di pacchetti AMI Amazon Linux o Amazon Linux 2, è disponibile anche su GitHub.

Dopo aver clonato il pacchetto, è possibile compilare e installare `amazon-efs-utils` utilizzando uno dei seguenti metodi, a seconda del tipo di pacchetti supportati dalla distribuzione Linux:

- RPM - Questo tipo di pacchetto è supportato da Amazon Linux, Amazon Linux 2 Red Hat Linux, CentOS e simili.
- DEB - Questo tipo di pacchetto è supportato da Ubuntu, Debian e simili.

Compila e installa **`amazon-efs-utils`** come pacchetto RPM per Amazon Linux, Amazon Linux 2 e distribuzioni Linux diverse da OpenSUSE o SLES

Da clonare da **`amazon-efs-utils`** GitHub

1. Esegui la connessione all'istanza EC2 mediante l'SSH (Secure Shell) e accedi con il nome utente appropriato. Per ulteriori informazioni, consulta Connessione all'istanza Linux tramite SSH nella Guida per l'utente di Amazon EC2 per le istanze Linux.
2. Installa `git` utilizzando il seguente comando:

   ```
   sudo yum -y install git
   ```
3. Clona `amazon-efs-utils` GitHub usando il seguente comando.

   ```
   git clone https://github.com/aws/efs-utils
   ```

Compilazione e installazione del pacchetto RPM **`amazon-efs-utils`**

1. Apri un terminale sul client e accedi alla directory che contiene il pacchetto `amazon-efs-utils`.

   ```
   cd /path/efs-utils
   ```
2. Installa il comando `make` bash se non è già presente nel tuo sistema operativo come segue.

   ```
   sudo yum -y install make
   ```

3. Installa il pacchetto `rpm-build` se non è già installato usando il seguente comando:

```
sudo yum -y install rpm-build
```

4. Compila il pacchetto `amazon-efs-utils` utilizzando il seguente comando:

```
sudo make rpm
```

5. Installare il pacchetto `amazon-efs-utils` con il seguente comando.

```
sudo yum -y install ./build/amazon-efs-utils*rpm
```

Passaggi successivi

Dopo l'installazione di `amazon-efs-utils` sulla tua istanza EC2, procedi con i passaggi successivi per il montaggio del file system:

- Installa `botocore` in modo da poter utilizzare Amazon CloudWatch per monitorare lo stato di montaggio del tuo file system.
- Esegui l'upgrade alla versione più recente di `stunnel` per abilitare la crittografia dei dati in transito.
- Installazione del file system utilizzando EFS Mount Helper.

Compilare e installare **`amazon-efs-utils`** come pacchetto RPM per openSUSE e SLES

Da clonare da **`amazon-efs-utils`** GitHub

1. Esegui la connessione all'istanza EC2 mediante l'SSH (Secure Shell) e accedi con il nome utente appropriato. Per ulteriori informazioni, consulta Connessione all'istanza Linux tramite SSH nella Guida per l'utente di Amazon EC2 per le istanze Linux.
2. Installa `zypper` utilizzando il seguente comando:

```
sudo zypper refresh
```

3. Installa il pacchetto `rpm-build` e il bash make se non sono già installati usando il seguente comando:

```
sudo zypper install -y git rpm-build make
```

a. Per OpenSUSE, se si verifica un errore simile al seguente:

```
File './suse/noarch/bash-completion-2.11-2.1.noarch.rpm' not found on medium
 'http://download.opensuse.org/tumbleweed/repo/oss/'
```

Esegui il seguente comando per aggiungere nuovamente i repository OSS e NON-OSS.

```
sudo zypper ar -f -n OSS http://download.opensuse.org/tumbleweed/repo/oss/ OSS
sudo zypper ar -f -n NON-OSS http://download.opensuse.org/tumbleweed/repo/non-
oss/ NON-OSS
sudo zypper refresh
```

b. Esegui nuovamente lo script di installazione git:

```
sudo zypper install -y git rpm-build make
```

4. Clona `amazon-efs-utils` GitHub usando il seguente comando.

```
git clone https://github.com/aws/efs-utils
```

Compilazione e installazione del pacchetto RPM **`amazon-efs-utils`**

1. Apri un terminale sul client e accedi alla directory che contiene il pacchetto `amazon-efs-utils`.

```
cd /path/efs-utils
```

2. Compila il pacchetto `amazon-efs-utils` utilizzando il seguente comando:

```
make rpm
```

3. Installare il pacchetto `amazon-efs-utils` con il seguente comando.

```
sudo zypper --no-gpg-checks install -y build/amazon-efs-utils*rpm
```

### Passaggi successivi

Dopo l'installazione di `amazon-efs-utils` sulla tua istanza EC2, procedi con i passaggi successivi per il montaggio del file system:

- Installa `botocore` in modo da poter utilizzare Amazon CloudWatch per monitorare lo stato di montaggio del tuo file system.
- Esegui l'upgrade alla versione più recente di `stunnel` per abilitare la crittografia dei dati in transito.
- Installazione del file system utilizzando EFS Mount Helper.

### Da compilare e installare amazon-efs-utils come pacchetto Debian per Ubuntu e Debian

#### Per clonare da **`amazon-efs-utils`** GitHub

1. Esegui la connessione all'istanza EC2 mediante l'SSH (Secure Shell) e accedi con il nome utente appropriato. Per ulteriori informazioni, consulta Connessione all'istanza Linux tramite SSH nella Guida per l'utente di Amazon EC2 per le istanze Linux.
2. (Facoltativo) Applica gli aggiornamenti prima di installare il pacchetto con il comando seguente:

   ```
   sudo apt-get update
   ```

   Installa gli aggiornamenti secondo necessità.
3. Installa `git` e `binutils` e utilizza il seguente comando. `binutils` è necessario per creare pacchetti DEB.

   ```
   sudo apt-get -y install git binutils
   ```
4. Clona `amazon-efs-utils` GitHub usando il seguente comando.

   ```
   git clone https://github.com/aws/efs-utils
   ```

#### Compilazione e installazione del pacchetto DEB **`amazon-efs-utils`**

1. Passa alla directory che contiene il pacchetto `amazon-efs-utils`.

   ```
   cd /path/efs-utils
   ```

2. Compila `amazon-efs-utils` utilizzando il seguente comando:

```
./build-deb.sh
```

3. Installa il pacchetto con il seguente comando.

```
sudo apt-get -y install ./build/amazon-efs-utils*deb
```

Passaggi successivi

Dopo l'installazione di `amazon-efs-utils` sulla tua istanza EC2, procedi con i passaggi successivi per il montaggio del file system:

- Installa `botocore` in modo da poter utilizzare Amazon CloudWatch per monitorare lo stato di montaggio del tuo file system.
- Esegui l'upgrade alla versione più recente di `stunnel` per abilitare la crittografia dei dati in transito.
- Installazione del file system utilizzando EFS Mount Helper.

## Installazione del client Amazon EFS su istanze Mac EC2 che eseguono macOS Big Sur, macOS Monterey o macOS Ventura

Il pacchetto `amazon-efs-utils` è disponibile per l'installazione su istanze Mac EC2 che eseguono macOS Big Sur, macOS Monterey o macOS Ventura.

Installazione del pacchetto **`amazon-efs-utils`**

1. Assicurati di aver creato un'istanza EC2 per Mac che esegue uno dei sistemi operativi Mac supportati:

   - macOS Big Sur
   - macOS Monterey
   - macOS Ventura

   Per informazioni su come eseguire questa operazione, consulta Fase 1: Avvio di un'istanza nella Guida per l'utente di Amazon EC2 per istanze Mac.

2. Accedi al terminale dell'istanza utilizzando SSH (Secure Shell) e accedi con il nome utente opportuno. Per ulteriori informazioni sulla procedura, consulta Connessione all'istanza tramite SSH nella Guida per l'utente di Amazon EC2 per le istanze Mac.
3. Esegui il comando seguente per installare `amazon-efs-utils`.

```
brew install amazon-efs-utils
```

> **Note**
>
> Il sistema risponde con le istruzioni per configurare l'helper di montaggio e abilitare il processo watchdog, incluse nei due passaggi successivi. Per visualizzare le istruzioni in un secondo momento, esegui il comando riportato.
>
> ```
> brew info amazon-efs-utils
> ```

4. Assicurati che l'helper di montaggio EFS in `amazon-efs-utils` sia accessibile tramite il comando di montaggio. Il comando da eseguire dipende dall'istanza EC2 Mac su cui stai installando il pacchetto.

   - Se stai installando il pacchetto su EC2 x86 Mac (mac1.metal), esegui il seguente comando:

   ```
   sudo mkdir -p /Library/Filesystems/efs.fs/Contents/Resources
   sudo ln -s /usr/local/bin/mount.efs /Library/Filesystems/efs.fs/Contents/
   Resources/mount_efs
   ```

   - Se stai installando il pacchetto su EC2 M1 Mac (mac2.metal), esegui il seguente comando:

   ```
   sudo mkdir -p /Library/Filesystems/efs.fs/Contents/Resources
   sudo ln -s /opt/homebrew/bin/mount.efs /Library/Filesystems/efs.fs/Contents/
   Resources/mount_efs
   ```

5. Abilita il processo watchdog (`amazon-efs-mount-watchdog`) che monitora lo stato dei montaggi TLS sul tuo file system EFS. Il comando da eseguire dipende dall'istanza EC2 Mac su cui stai installando il pacchetto.

   - Se stai installando il pacchetto su EC2 x86 Mac (mac1.metal), esegui il seguente comando:

   ```
   sudo cp /usr/local/Cellar/amazon-efs-utils/<version>/libexec/amazon-efs-mount-
   watchdog.plist /Library/LaunchAgents
   ```

```
sudo launchctl load /Library/LaunchAgents/amazon-efs-mount-watchdog.plist
```

- Se stai installando il pacchetto su EC2 M1 Mac (mac2.metal), esegui il seguente comando:

```
sudo cp /opt/homebrew/Cellar/amazon-efs-utils/<version>/libexec/amazon-efs-mount-watchdog.plist /Library/LaunchAgents
sudo launchctl load /Library/LaunchAgents/amazon-efs-mount-watchdog.plist
```

### Passaggi successivi

Dopo l'installazione di `amazon-efs-utils` sulla tua istanza EC2, procedi con i passaggi successivi per il montaggio del file system:

- Installa `botocore` in modo da poter utilizzare Amazon CloudWatch per monitorare lo stato di montaggio del tuo file system.
- Esegui l'upgrade alla versione più recente di `stunnel` per abilitare la crittografia dei dati in transito.
- Installazione del file system utilizzando EFS Mount Helper.

## Installazione di **`botocore`**

Il client Amazon EFS utilizza `botocore` per interagire con altri servizi AWS. È necessario se desideri monitorare il successo o il fallimento dei tentativi di montaggio per i tuoi file system Amazon EFS in CloudWatch Logs. Per ulteriori informazioni, consulta Monitoraggio dello stato di successo o di fallimento del tentativo di montaggio. Questa sezione descrive come eseguire l'installazione e l'upgrade di `botocore` su un'istanza Amazon EC2.

### Installazione di **`botocore`** come pacchetto RPM

1. Esegui il comando seguente per installare `wget`.

```
sudo yum -y install wget
```

2. Utilizza lo script seguente per installare la versione appropriata del gestore di pacchetti `pip`.

```
if [[ "$(python3 -V 2>&1)" =~ ^(Python 3.6.*) ]]; then
    sudo wget https://bootstrap.pypa.io/pip/3.6/get-pip.py -O /tmp/get-pip.py
elif [[ "$(python3 -V 2>&1)" =~ ^(Python 3.5.*) ]]; then
    sudo wget https://bootstrap.pypa.io/pip/3.5/get-pip.py -O /tmp/get-pip.py
```

```
elif [[ "$(python3 -V 2>&1)" =~ ^(Python 3.4.*) ]]; then
    sudo wget https://bootstrap.pypa.io/pip/3.4/get-pip.py -O /tmp/get-pip.py
else
    sudo wget https://bootstrap.pypa.io/get-pip.py -O /tmp/get-pip.py
fi
```

3. Esegui i comandi seguenti per installare `botocore`.

```
sudo python3 /tmp/get-pip.py
sudo pip3 install botocore
```

Or

```
sudo /usr/local/bin/pip3 install botocore
```

## Installazione di botocore come pacchetto DEB

1. Esegui i comandi seguenti per installare `wget`.

```
sudo apt-get update
sudo apt-get -y install wget
```

2. Utilizza lo script seguente per installare la versione appropriata del gestore di pacchetti `pip`.

```
if echo $(python3 -V 2>&1) | grep -e "Python 3.6"; then
    sudo wget https://bootstrap.pypa.io/pip/3.6/get-pip.py -O /tmp/get-pip.py
elif echo $(python3 -V 2>&1) | grep -e "Python 3.5"; then
    sudo wget https://bootstrap.pypa.io/pip/3.5/get-pip.py -O /tmp/get-pip.py
elif echo $(python3 -V 2>&1) | grep -e "Python 3.4"; then
    sudo wget https://bootstrap.pypa.io/pip/3.4/get-pip.py -O /tmp/get-pip.py
else
    sudo apt-get -y install python3-distutils
    sudo wget https://bootstrap.pypa.io/get-pip.py -O /tmp/get-pip.py
fi
```

3. Esegui i comandi seguenti per installare `botocore`.

```
sudo python3 /tmp/get-pip.py
sudo pip3 install botocore
```

Or

```
sudo /usr/local/bin/pip3 install botocore
```

Se stai installando `botocore` su Debian10 o Ubuntu20, usa i seguenti comandi per l'installazione di `botocore` nella cartella di destinazione specificata.

- Per Debian10:

```
sudo python3 /tmp/get-pip.py
sudo pip3 install --target /usr/lib/python3/dist-packages botocore
```

- Per Ubuntu20:

```
sudo /usr/local/bin/pip3 install --target /usr/lib/python3/dist-packages botocore
```

### Installazione di **`botocore`** su un'istanza Mac

- Esegui il seguente comando per installare `botocore` sull'istanza Mac.

```
sudo pip3 install botocore
```

## Aggiornamento di **`botocore`**

Per eseguire l'aggiornamento all'ultima versione compatibile di botocore, utilizza l'opzione `--upgrade`. Per esempio:

```
sudo pip3 install botocore --upgrade
```

# Aggiornamento di **`stunnel`**

La crittografia dei dati in transito con l'helper di montaggio Amazon EFS richiede la versione 1.0.2 0penSSL o più recente e una versione `stunnel` che supporti sia l'Online Certificate Status Protocol (OCSP) che il controllo del nome host del certificato. L'helper di montaggio di Amazon EFS utilizza il programma `stunnel` per la sua funzionalità TLS. Si noti che alcune versioni di Linux non includono una versione di `stunnel` che supporta queste funzionalità di TLS per impostazione predefinita.

Quando si utilizza una di tali distribuzioni di Linux, il montaggio di un file system Amazon EFS con l'utilizzo di TLS ha esito negativo.

Dopo aver installato l'helper di montaggio di Amazon EFS, è possibile effettuare l'upgrade della versione di stunnel del sistema con le seguenti istruzioni.

Per eseguire l'aggiornamento di **`stunnel`** su Amazon Linux, Amazon Linux 2 e altre distribuzioni Linux supportate (ad eccezione di SLES 12)

1. In un browser Web, vai alla pagina dei download `stunnel` https://stunnel.org/downloads.html.
2. Individua l'ultima versione di `stunnel` disponibile in formato `tar.gz`. Prendere nota del nome del file poiché sarà necessario per le fasi successive.
3. Aprire un terminale sul client Linux ed eseguire questi comandi nell'ordine indicato.

   a. Per RPM:

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

   Per DEB:

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

   b. Sostituiscilo *`latest-stunnel-version`*con il nome del file annotato in precedenza nel passaggio 2.

   ```
   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. Il pacchetto `stunnel` corrente è installato in `bin/stunnel`. Affinché la nuova versione possa essere installata, rimuovere tale cartella con il comando seguente.

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

h. Per installare la versione più recente:

```
sudo make install
```

i. Crea un symlink:

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

Per aggiornare stunnel su macOS

- Apri un terminale sulla tua istanza EC2 per Mac ed esegui il seguente comando per eseguire l'aggiornamento alla versione più recente di stunnel.

```
brew upgrade stunnel
```

Aggiornamento di stunnel per SLES 12

- Esegui i seguenti comandi e segui le istruzioni del gestore di pacchetti zypper per aggiornare stunnel sulla tua istanza di calcolo che esegue 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
```

Dopo aver installato una versione di stunnel con le funzionalità necessarie, è possibile montare il file system usando TLS con le impostazioni consigliate di Amazon EFS.

## Disabilitazione della verifica del certificato associato al nome dell'host

Se non riesci a installare le dipendenze necessarie, è possibile disabilitare facoltativamente la verifica del certificato associato al nome dell'host all'interno della configurazione dell'helper di montaggio di Amazon EFS. Non è consigliabile disabilitare questa funzione in ambienti di produzione. Per disabilitare la verifica del certificato associato al nome dell'host, procedere nel seguente modo:

1. Utilizzando un editor di testo a scelta, aprire il file `/etc/amazon/efs/efs-utils.conf`.
2. Impostare il parametro `stunnel_check_cert_hostname` su falso.
3. Salvare le modifiche e chiudere il file.

Per maggiori informazione sull'utilizzo della crittografia dei dati in transito, vedere Montaggio dei file system EFS.

## Abilitazione di OCSP (Online Certificate Status Protocol)

Per massimizzare la disponibilità del file system nel caso in cui la CA non sia raggiungibile dal VPC, l'Online Certificate Status Protocol (OCSP) non è abilitato per impostazione predefinita quando si sceglie di crittografare i dati in transito. Amazon EFS utilizza un'autorità di certificazione (CA) Amazon per emettere e firmare i propri certificati TLS e la CA ordina al client di utilizzare OCSP per verificare la presenza di certificati revocati. L'endpoint OCSP deve essere accessibile su Internet tramite il Virtual Private Cloud (VPC) per poter verificare lo stato di un certificato. All'interno del servizio, EFS monitora continuamente lo stato del certificato ed emette nuovi certificati con cui sostituire i certificati revocati rilevati.

Per offrire la massima sicurezza possibile, puoi abilitare OCSP in modo tale che i client Linux possano verificare la presenza di certificati revocati. OCSP protegge dall'uso dannoso dei certificati revocati, il che è improbabile che si verifichi nel VPC. Nel caso in cui un certificato TLS di EFS venga revocato, Amazon pubblicherà un bollettino sulla sicurezza e rilascerà una nuova versione dell'helper di montaggio di EFS che rifiuta il certificato revocato.

Per abilitare OCSP sul tuo client Linux per tutte le connessioni TLS future a EFS

1. Aprire un terminale sul client Linux.
2. Utilizzando un editor di testo a scelta, aprire il file `/etc/amazon/efs/efs-utils.conf`.
3. Impostare il valore `stunnel_check_cert_validity` su true.
4. Salvare le modifiche e chiudere il file.

Per abilitare OCSP come parte del comando **`mount`**

- Utilizzare il seguente comando mount per abilitare OCSP durante il montaggio del file system.

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

# Montaggio dei file system EFS

Nella sezione seguente, è possibile imparare come montare un file system Amazon EFS su un'istanza Linux utilizzando l'helper di montaggio EFS. Inoltre, è possibile scoprire come utilizzare il file `fstab` per rimontare automaticamente il file system dopo un riavvio del sistema. Utilizzando l'helper di montaggio EFS, hai le seguenti opzioni per montare il tuo file system Amazon EFS:

- Montaggio su istanze EC2 supportate
- Montaggio con autorizzazione IAM
- Montaggio con punti di accesso Amazon EFS
- Montaggio con un client Linux locale
- Montaggio automatico dei file system EFS al riavvio di un'istanza EC2
- Montaggio di un file system durante la creazione di una nuova istanza EC2

> **Note**
>
> Amazon EFS non supporta il montaggio da istanze Windows di Amazon EC2.

L'helper di montaggio EFS fa parte del pacchetto `amazon-efs-utils`. Il pacchetto `amazon-efs-utils` è una collezione di strumenti open source per Amazon EFS. Per ulteriori informazioni, consulta Installazione manuale del client Amazon EFS.

Prima della disponibilità dell'helper di montaggio di Amazon EFS, consigliavamo di montare i file system Amazon EFS utilizzando il client NFS standard di Linux. Per ulteriori informazioni, consulta Montaggio dei file system senza l'assistente per il montaggio di EFS.

Argomenti

- Monta il file system utilizzando l'helper di montaggio di EFS
- Ulteriori considerazioni sul montaggio
- Risoluzione dei problemi con versioni di AMI e kernel

# Monta il file system utilizzando l'helper di montaggio di EFS

L'helper di montaggio EFS ti aiuta a montare i tuoi file system EFS sulle istanze EC2 Linux e Mac che eseguono le distribuzioni supportate elencate in Panoramica.

L'helper di montaggio di Amazon EFS semplifica il montaggio dei file system. Include per default le opzioni di montaggio di Amazon EFS raccomandate. Inoltre, l'helper di montaggio include il mantenimento dei log per la risoluzione dei problemi. Se riscontri un problema con il tuo file system Amazon EFS, puoi condividere questi log con AWS Support. Per ulteriori informazioni sul montaggio di un file system, consulta Montaggio dei file system EFS.

> **Note**
>
> Amazon EFS non supporta il montaggio da istanze Windows di Amazon EC2.

Argomenti



## Come funziona

L'helper di montaggio definisce un nuovo tipo di file system di rete, denominato `efs`, che è completamente compatibile con il comando standard Linux `mount`. L'helper di montaggio supporta

anche il montaggio automatico di un file system Amazon EFS all'avvio dell'istanza utilizzando elementi del file di configurazione `/etc/fstab` su istanze EC2 Linux.

> **Warning**
>
> In caso di montaggio automatico del file system, utilizzare l'opzione `_netdev`, usata per identificare i file system di rete. Se `_netdev` è mancante, l'istanza EC2 potrebbe smettere di rispondere. Questo risultato è dovuto al fatto che i file system di rete devono essere inizializzati dopo che l'istanza di calcolo ha avviato la sua interfaccia di rete. Per ulteriori informazioni, consulta Il montaggio automatico non funziona e l'istanza non risponde.

Puoi montare un file system specificando una delle seguenti proprietà:

- Nome DNS del file system: se si utilizza il nome DNS del file system e l'helper di montaggio non è in grado di risolverlo, ad esempio quando si monta un file system in un altro VPC, si tornerà a utilizzare l'indirizzo IP del target di montaggio. Per ulteriori informazioni, consulta Montaggio di file system EFS da un altro Account AWS o da un VPC.
- ID del file system: se si utilizza l'ID del file system, l'helper di montaggio lo risolve nell'indirizzo IP locale della Elastic Network Interface (ENI) del target di montaggio senza richiamare risorse esterne.
- Indirizzo IP di target di montaggio: è possibile utilizzare l'indirizzo IP di uno dei target di montaggio del file system.

Puoi trovare il valore per tutte queste proprietà nella console Amazon EFS. Il nome DNS del file system si trova nella schermata Allega.

Quando tra le opzioni di montaggio del file system Amazon EFS è inclusa la crittografia dei dati in transito, l'helper di montaggio inizializza un processo client `stunnel` e un processo supervisore denominato `amazon-efs-mount-watchdog`. Il processo `amazon-efs-mount-watchdog` monitora lo stato dei montaggi TLS e viene avviato automaticamente la prima volta che un file system EFS viene montato su TLS. Se il client è in esecuzione su Linux, questo processo è gestito da `upstart` o dall'altra distribuzione`systemd` Linux. Per i client che eseguono su un macOS supportato, è gestito da `launchd`.

`Stunnel` è un relay di rete multifunzione open source. Il processo client `stunnel` rimane in ascolto su una porta locale in attesa del traffico in entrata e l'helper di montaggio reindirizza il traffico del client NFS verso questa porta locale.

L'helper di montaggio utilizza TLS versione 1.2 per comunicare con il file system. L'utilizzo di TLS richiede dei certificati e questi certificati sono firmati da un'autorità di certificazione di Amazon. Per ulteriori informazioni sul funzionamento della crittografia, consultare Crittografia dei dati in Amazon EFS.

## Opzioni di montaggio utilizzate dal client Amazon EFS

Il client di supporto per il montaggio di Amazon EFS utilizza le seguenti opzioni di montaggio ottimizzate per Amazon EFS:

- `nfsvers=4.1`: utilizzato durante il montaggio su istanze EC2 Linux

  `nfsvers=4.0`: utilizzato per il montaggio su istanze Mac EC2 supportate che eseguono macOS Big Sur, Monterey e Ventura
- `rsize=1048576`: imposta il numero massimo di byte di dati che il client NFS è in grado di ricevere per ogni richiesta READ della rete su 1048576, il massimo disponibile, per evitare una riduzione delle prestazioni.
- `wsize=1048576`: imposta il numero massimo di byte di dati che il client NFS è in grado di inviare per ogni richiesta WRITE della rete su `1048576`, il massimo disponibile, per evitare una riduzione delle prestazioni.
- `hard`: imposta il comportamento di ripristino del client NFS dopo il timeout di una richiesta NFS, in modo che la richiesta NFS venga ritentata a tempo indeterminato fino alla risposta del server.
- `timeo=600`: imposta il valore di timeout utilizzato dal client NFS in attesa di una risposta prima di ripetere la richiesta NFS su 600 decisecondi (60 secondi) per evitare un calo delle prestazioni.
- `retrans=2`: imposta su 2 il numero di volte che il client NFS ritenta una richiesta prima di eseguire un'altra operazione di ripristino.
- `noresvport`: indica al client NFS di usare una nuova porta TCP (Transmission Control Protocol) di origine quando la connessione di rete viene ripristinata. Utilizza l'opzione `noresvport` per garantire che il file system EFS abbia una disponibilità ininterrotta dopo una riconnessione o un evento di ripristino della rete.
- `mountport=2049`: utilizzato solo per il montaggio su istanze Mac EC2 che eseguono macOS Big Sur, Monterey e Ventura.

## Ottenimento dei log per il supporto

L'helper di montaggio include il mantenimento dei log del file system Amazon EFS. È possibile condividere questi registri con AWS Support per la risoluzione dei problemi. È possibile trovare i log archiviati nei client `/var/log/amazon/efs` utilizzando l'helper di montaggio EFS. Questi log riguardano l'helper di montaggio EFS, lo stesso processo stunnel (disattivato per impostazione predefinita) e il processo `amazon-efs-mount-watchdog` che monitora il processo stunnel.

> **Note**
>
> Il processo `amazon-efs-mount-watchdog` garantisce che ogni processo stunnel associato al montaggio sia in esecuzione, e arresta stunnel quando il file system Amazon EFS viene smontato. Se per qualsiasi motivo un processo stunnel si arresta in modo inatteso, il processo watchdog lo riavvia.

È possibile modificare la configurazione dei log in `/etc/amazon/efs/efs-utils.conf`. Affinché le modifiche al registro abbiano effetto, è necessario smontare e rimontare il file system utilizzando l'helper di montaggio EFS. Il volume dei log conservati per l'helper di montaggio e il processo watchdog è limitato a 20 MiB. Per impostazione predefinita, i log per il processo di stunnel sono disattivati.

> **Important**
>
> È possibile abilitare la registrazione dei log per il processo stunnel. Tuttavia, l'abilitazione dei log di stunnel potrebbe portare ad un consumo di spazio di memorizzazione sul file system non indifferente.

## Prerequisiti per l'utilizzo dell'helper di montaggio EFS

È possibile montare un file system Amazon EFS su un'istanza Amazon EC2 utilizzando l'helper di montaggio di Amazon EFS. Per utilizzare l'helper di montaggio è necessario disporre di:

- ID del file system di montaggio: l'helper di montaggio risolve l'ID del file system nell'indirizzo IP locale della Elastic Network Interface (ENI) del target di montaggio senza richiamare risorse esterne.

- Target di montaggio Amazon EFS: i target di montaggio possono essere create nel cloud privato virtuale (VPC, Virtual Private Cloud). Se si crea il file system nella console utilizzando le impostazioni consigliate dal servizio, viene creata una destinazione di montaggio in ogni zona di disponibilità in Regione AWS cui si trova il file system. Per istruzioni sulla creazione di target di montaggio consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

  > **Note**
  >
  > Si consiglia di attendere 60 secondi dopo la disponibilità dello stato del ciclo di vita del target di montaggio appena creato prima di montare il file system tramite DNS. Questa attesa consente ai record DNS di propagarsi completamente nel luogo in Regione AWS cui risiede il file system.

  Se utilizzi un target di montaggio in una zona di disponibilità diversa da quella dell'istanza EC2 incorri nei costi EC2 standard per i dati inviati nelle zone di disponibilità. Potresti anche osservare un aumento delle latenze per le operazioni del file system.
- Per montare i file system a zona singola da una zona di disponibilità diversa:
  - Nome della zona di disponibilità del file system: se si sta montando un file system EFS a zona singola che si trova in una zona di disponibilità diversa rispetto all'istanza EC2.
  - Nome DNS del target di montaggio: in alternativa, puoi specificare il nome DNS del target di montaggio anziché la zona di disponibilità.
- Un'istanza Amazon EC2 che esegue una distribuzione supportata di Linux o macOS - Le distribuzioni Linux supportate per montare il file system con l'helper di montaggio sono le seguenti:
  - Amazon Linux 2
  - Amazon Linux 2017.09 e versioni successive
  - macOS Big Sur
  - Red Hat Enterprise Linux (e derivati come CentOS) versione 7 e successive
  - Ubuntu 16.04 LTS e versioni più recenti

  > **Note**
  >
  > Le istanze Amazon EC2 Mac che eseguono macOS Big Sur supportano solo NFS v4.0.

- L'helper di montaggio di Amazon EFS è installato sull'istanza EC2: il mount helper è uno strumento `amazon-efs-utils` incluso nel pacchetto di utilità. Per ulteriori informazioni sull'installazione di `amazon-efs-utils`, consulta Utilizzo di AWS Systems Manager per installare `amazon-efs-utils` e Installazione manuale di `amazon-efs-utils`.
- Istanza EC2 in VPC - L'istanza EC2 di connessione deve trovarsi in un cloud privato virtuale (VPC, Virtual Private Cloud) basato sul servizio Amazon VPC. Inoltre, deve essere configurato per utilizzare il server DNS fornito da. AWS Per ulteriori informazioni sul server DNS di Amazon, consulta Impostazioni delle opzioni DHCP nella Guida per l'utente di Amazon VPC.
- VPC con hostname DNS attivati – La VPC dell'istanza EC2 che si connette deve avere gli hostname DNS abilitati. Per ulteriori informazioni, consulta Visualizzazione degli hostname DNS dell'istanza EC2 nella Guida per l'utente di Amazon VPC.
- Per istanze EC2 e file system diversi Regioni AWS: se l'istanza EC2 e il file system che stai montando si trovano in luoghi diversi Regioni AWS, dovrai modificare la `region` proprietà nel file. `efs-utils.conf` Per ulteriori informazioni, consulta Montaggio di file system Amazon EFS da un altro Regione AWS.

## Montaggio su istanze Amazon EC2 Linux utilizzando l'helper di montaggio EFS

Questo processo richiede i seguenti elementi:

- È necessario installare il pacchetto `amazon-efs-utils` nell'istanza EC2. Per ulteriori informazioni, consulta Installazione manuale del client Amazon EFS.
- Il file system dispone di target di montaggio creati. Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

Montaggio del file system Amazon EFS su istanze Linux utilizzando l'helper di montaggio su istanze EC2 Linux

1. Apri la finestra del terminale dell'istanza EC2 utilizzando SSH (Secure Shell) e accedete con il nome utente opportuno. Per ulteriori informazioni, consulta Connessione all'istanza Linux tramite SSH per le istanze Linux.
2. Crea una directory `efs` che utilizzerai come punto di montaggio del file system usando il seguente comando:

```
sudo mkdir efs
```

3. Esegui uno dei seguenti comandi per montare il file system.

> **Note**
>
> Se l'istanza EC2 e il file system che stai montando si trovano in differenti Regione AWS, consulta Montaggio di file system Amazon EFS da un altro Regione AWS per modificare la proprietà `region` nel file `efs-utils.conf` .

- Per eseguire il montaggio utilizzando l'id del file system:

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

Usa l'ID del file system che stai montando al posto *`file-system-id`* e al posto `efs` di. *`efs-mount-point`*

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

In alternativa, se si desidera utilizzare la crittografia dei dati in transito, è possibile montare il file system con il comando seguente.

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

- Montaggio di un file system utilizzando il nome DNS del file system:

```
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/
```

- Per eseguire il montaggio utilizzando l'indirizzo IP di destinazione del mount:

```
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/
```

È possibile visualizzare e copiare i comandi esatti per montare il file system nella finestra di dialogo Allega.

a. Nella console Amazon EFS, scegli il file system che desideri montare per visualizzare la relativa pagina dei dettagli.

b. Per visualizzare i comandi di montaggio da utilizzare per questo file system, scegli Allega in alto a destra.

   La schermata Allega mostra i comandi esatti da usare per il montaggio del file system nei seguenti modi:

   - (Montaggio tramite DNS) Utilizzo del nome DNS del file system con l'helper di montaggio EFS o un client NFS.
   - (Montaggio tramite IP) Utilizzo dell'indirizzo IP di target di montaggio nella zona di disponibilità selezionata con un client NFS.

## Montaggio su istanze Mac Amazon EC2 utilizzando l'helper di montaggio EFS

Questo processo richiede i seguenti elementi:

- È necessario aver installato il pacchetto `amazon-efs-utils` nell'istanza Mac EC2. Per ulteriori informazioni, consulta Installazione del client Amazon EFS su istanze Mac EC2 che eseguono macOS Big Sur, macOS Monterey o macOS Ventura.
- Il file system creato dispone di target di montaggio. È possibile creare target di montaggio al momento della creazione del file system e aggiungerli ai file system esistenti. Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.
- Stai montando il file system su un'istanza EC2 Mac che esegue macOS Big Sur, Monterey o Ventura. Non sono supportate altre versioni macOS.

> **Note**
>
> Sono supportate solo le istanze EC2 Mac con macOS Big Sur, Monterey e Ventura. Altre versioni di macOS non sono supportate per l'uso con Amazon EFS.

Per montare il file system Amazon EFS utilizzando l'helper di montaggio EFS su istanze EC2 Mac con macOS Big Sur, Monterey o Ventura

1. Apri la finestra del terminale dell'istanza Mac EC2 utilizzando SSH (Secure Shell) e accedi con il nome utente opportuno. Per ulteriori informazioni, consulta Connetti l'istanza Linux tramite SSH per istanze Mac nella Guida per l'utente di Amazon EC2 per le istanze Linux.
2. Crea una directory che utilizzerai come punto di montaggio del file system usando il seguente comando:

```
sudo mkdir efs
```

3. Eseguire il seguente comando per montare il file system.

> **Note**
>
> Per impostazione predefinita, l'helper di montaggio EFS utilizza la crittografia in transito durante il montaggio su istanze Mac EC2, indipendentemente dal fatto che si utilizzi o meno l'opzione `tls` nel comando di montaggio.

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

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

Inoltre puoi utilizzare l'opzione `tls` durante il montaggio.

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

Per montare un file system su un'istanza EC2 Mac senza utilizzare la crittografia in transito, usa l'opzione `notls` come mostrato nel comando seguente.

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

È possibile visualizzare e copiare i comandi esatti per montare il file system nella finestra di dialogo Allega della console di gestione, descritta di seguito.

a. Nella console Amazon EFS, scegli il file system che desideri montare per visualizzare la relativa pagina dei dettagli.

b. Per visualizzare i comandi di montaggio da utilizzare per questo file system, scegli Allega in alto a destra.

   La schermata Allega mostra i comandi esatti da usare per il montaggio del file system nei seguenti modi:

   - (Montaggio tramite DNS) Utilizzo del nome DNS del file system con l'helper di montaggio EFS o un client NFS.
   - (Montaggio tramite IP) Utilizzo dell'indirizzo IP del target di montaggio nella zona di disponibilità selezionata con un client NFS.

## Montaggio di file system Amazon EFS da un altro Regione AWS

Se stai montando il tuo file system EFS da un'istanza Amazon EC2 che si trova in un file system Regione AWS diverso dal file, dovrai modificare il valore della `region` proprietà nel `efs-utils.conf` file.

Per modificare la proprietà della regione in **`efs-utils.conf`**

1. Accedi al terminale dell'istanza EC2 utilizzando SSH (Secure Shell) e accedi con il nome utente opportuno. Per ulteriori informazioni sulla procedura, consulta Connessione all'istanza Linux tramite SSH nella Guida per l'utente di Amazon EC2 per le istanze Linux.
2. Individua il file `efs-utils.conf` e aprilo tramite l'editor di testo preferito.
3. Individua la riga seguente:

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

   a. Rimuovi i commenti dalla riga.

   b. Se il file system non si trova nella regione `us-east-1` sostituisci `us-east-1` con l'ID della regione in cui si trova il file system.

   c. Salvare le modifiche.
4. Aggiungi una voce host per il montaggio su più regioni. Per ulteriori informazioni su come effettuare tale operazione, consulta Passaggio 3: Aggiungere una voce host per la destinazione di montaggio.

5. Monta il file system utilizzando l'helper di montaggio EFS per istanze Linux o Mac.

## Montaggio dei file system a zona singola

I file system Amazon EFS a zona singola supportano solo un target di montaggio che si trova nella stessa zona di disponibilità del file system. Non è possibile aggiungere ulteriori target di montaggio. Questa sezione descrive gli aspetti da considerare durante il montaggio dei file system a zona singola.

Puoi evitare i costi di trasferimento dei dati tra zone di disponibilità e ottenere prestazioni migliori accedendo a un file system EFS utilizzando un'istanza di calcolo Amazon EC2 che si trova nella stessa zona di disponibilità di quella del target di montaggio del file system.

Questa sezione contiene le procedure seguenti:

- È necessario installare `amazon-efs-utils package` nell'istanza EC2. Per ulteriori informazioni, consulta Installazione manuale del client Amazon EFS.
- Il target di montaggio del file system è stato creato. Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

### Montaggio dei file system a zona singola su EC2 in una zona di disponibilità diversa

Se stai montando un file system a zona singola su un'istanza EC2 che si trova in una zona di disponibilità diversa, devi specificare il nome della zona di disponibilità del file system o il nome DNS del target di montaggio del file system nell'apposito comando dell'helper di montaggio.

Crea una directory chiamata `efs` che utilizzerai come punto di montaggio del file system usando il seguente comando:

```
sudo mkdir efs
```

Utilizzare il comando seguente per montare il file system utilizzando un helper di montaggio EFS. Il comando specifica il nome della zona di disponibilità del file system.

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

Questo è il comando con valori di esempio:

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

Il comando seguente monta il file system, specificando il nome DNS del target di montaggio del file system.

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

Questo è il comando con un esempio di nome DNS del target di montaggio.

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

Montaggio automatico dei file system a zona singola in una zona di disponibilità diversa con helper di montaggio EFS

Se si utilizza `/etc/fstab` per montare un file system EFS a zona singola su un'istanza EC2 che si trova in una zona di disponibilità diversa, è necessario specificare il nome della zona di disponibilità del file system o il nome DNS del target di montaggio del file system nella voce `/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
```

Montaggio automatico dei file system a zona singola con NFS

Se si utilizza `/etc/fstab` per montare un file system EFS utilizzando lo storage One Zone su un'istanza EC2 che si trova in una zona di disponibilità diversa, è necessario specificare il nome della zona di disponibilità del file system con il nome DNS del file system nella `/etc/fstab` voce.

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

Per ulteriori informazioni su come modificare il file `/etc/fstab` e i valori utilizzati in questo comando, consulta Utilizzo di NFS per montare automaticamente i file system EFS.

## Montaggio dei file system con il file system One Zone su altre AWS istanze di calcolo

Quando utilizzi un file system One Zone con Amazon Elastic Container Service, Amazon Elastic Kubernetes Service AWS Lambda oppure, devi configurare il servizio per utilizzare la stessa zona di disponibilità in cui si trova il file system EFS, illustrata di seguito e descritta nelle sezioni seguenti.


### Connessione da Amazon Elastic Container Service

Puoi utilizzare i file system Amazon EFS con Amazon ECS per condividere i dati del file system all'interno del tuo parco istanze di container in modo che le tue operazioni abbiano accesso allo stesso storage persistente, indipendentemente dall'istanza su cui si basano. Per utilizzare i file system Amazon EFS a zona singola con Amazon ECS, è necessario scegliere solo sottoreti che si trovano nella stessa zona di disponibilità del file system all'avvio dell'attività. Per ulteriori informazioni, consulta Volumi Amazon EFS nella Guida per gli sviluppatori di Amazon Elastic Container Service.

### Connessione da Amazon Elastic Kubernetes Service

Quando monti un file system a zona singola da Amazon EFS, puoi utilizzare il driver Amazon EFS Container Storage Interface (CSI), che supporta i punti di accesso Amazon EFS, per condividere un

file system tra più pod in un cluster Amazon EFS o Kubernetes autogestito. Il driver CSI Amazon EFS è installato nello stack Fargate. Quando utilizzi il driver CSI Amazon EFS con i file system Amazon EFS a zona singola, puoi utilizzare l'opzione `nodeSelector` all'avvio del pod per assicurarti che venga pianificato all'interno della stessa zona di disponibilità del file system.

Connessione da AWS Lambda

Puoi usare Amazon EFS AWS Lambda per condividere dati tra chiamate di funzioni, leggere file di dati di riferimento di grandi dimensioni e scrivere l'output delle funzioni in un archivio persistente e condiviso. Lambda collega in modo sicuro le istanze della funzione ai target di montaggio di Amazon EFS che si trovano nella stessa zona di disponibilità e sottorete. Quando usi Lambda con i file system a zona singola, configura la funzione per lanciare chiamate solo nelle sottoreti che si trovano nella stessa zona di disponibilità del file system.

## Montaggio con autorizzazione IAM

Per montare il tuo file system Amazon EFS su istanze Linux utilizzando l'autorizzazione AWS Identity and Access Management (IAM), usi l'helper di montaggio EFS. Per ulteriori informazioni sull'autorizzazione IAM per i client NFS, vedere Utilizzo di IAM per controllare l'accesso ai dati del file system.

Crea una directory che utilizzerai come punto di montaggio del file system nelle seguenti sezioni. Puoi utilizzare il comando sottostante per creare una directory del punto di montaggio `efs`:

```
sudo mkdir efs
```

È quindi possibile sostituire le istanze di *`efs-mount-point`* con `efs`.

### Montaggio con IAM utilizzando un profilo dell'istanza EC2

Se si sta montando con autorizzazione IAM in un'istanza Amazon EC2 con un profilo dell'istanza, utilizza le opzioni di montaggio `tls` e `iam`, mostrate di seguito.

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

Per eseguire automaticamente il montaggio con autorizzazione IAM in un'istanza Amazon EC2 che dispone di un profilo dell'istanza, aggiungi la riga seguente al file `/etc/fstab` nell'istanza EC2.

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

### Montaggio con IAM utilizzando un profilo denominato

Puoi eseguire il montaggio con l'autorizzazione IAM utilizzando le credenziali IAM presenti nel file delle AWS CLI credenziali o nel file di `~/.aws/credentials` configurazione. AWS CLI `~/.aws/config` Se `"awsprofile"` non viene specificato, viene utilizzato il profilo «predefinito».

Per eseguire il montaggio con autorizzazione `tls` in un'istanza Linux utilizzando un file delle credenziali, utilizzare le opzioni di montaggio , `awsprofile` e `iam` mostrate di seguito.

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

Per eseguire automaticamente il montaggio con autorizzazione IAM in un'istanza Linux utilizzando un file delle credenziali, aggiungi la seguente riga al file `/etc/fstab` nell'istanza EC2.

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

## Montaggio con punti di accesso EFS

È possibile montare un file system EFS utilizzando un punto di accesso EFS solo utilizzando l'helper di montaggio EFS.

> **Note**
>
> È necessario configurare uno o più target di montaggio per il file system quando si monta un file system utilizzando punti di accesso EFS.

Quando si monta un file system utilizzando un punto di accesso, il comando mount include l'opzione `access-point-id` e l'opzione mount `tls` oltre alle normali opzioni di montaggio. Di seguito viene mostrato un esempio.

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

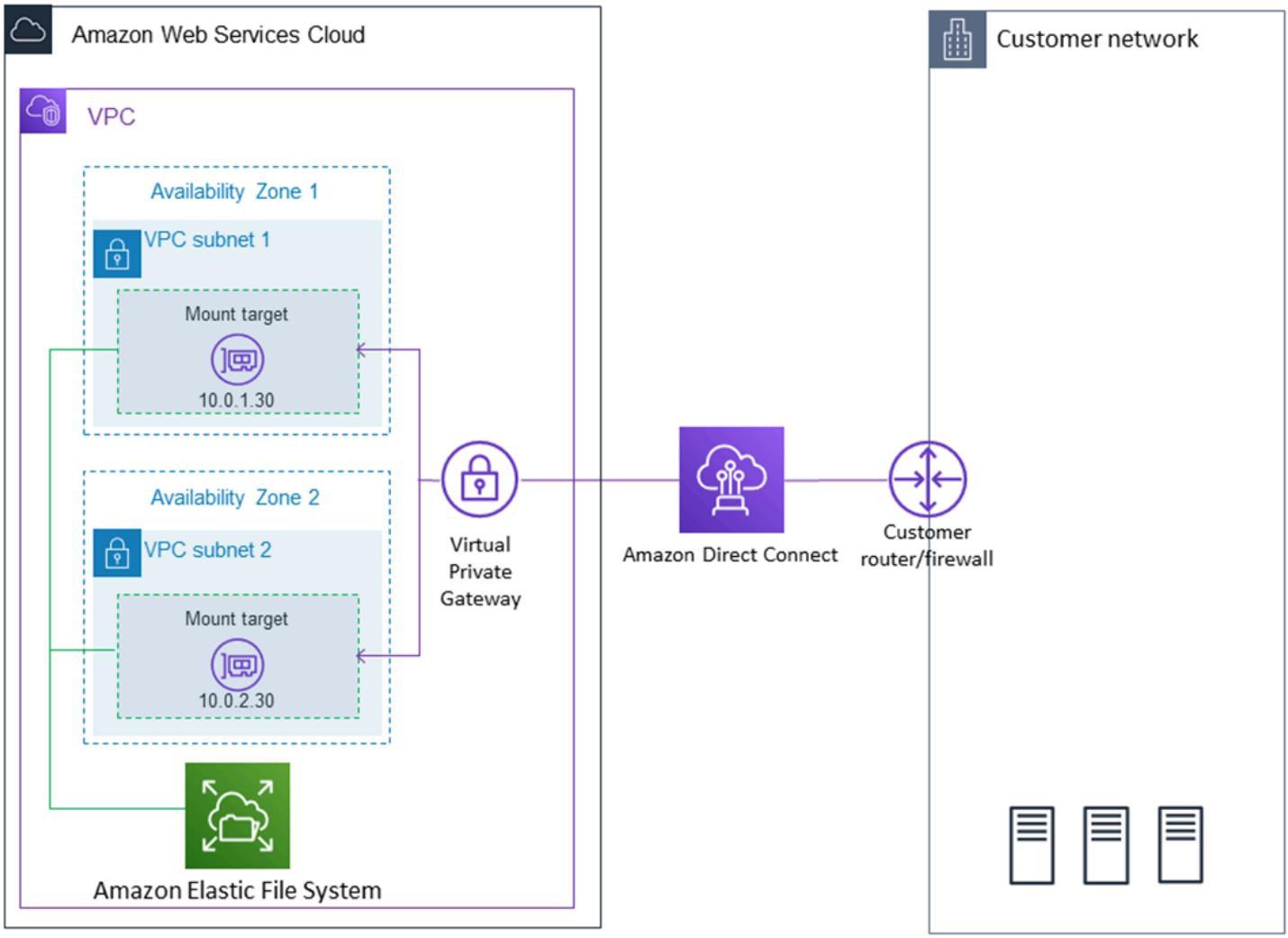
Per eseguire automaticamente il montaggio di un file system utilizzando un punto di accesso, aggiungere la riga seguente al file `/etc/fstab` nell'istanza EC2.

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

Per ulteriori informazioni sui punti di accesso EFS, consulta Utilizzo dei punti di accesso Amazon EFS.

## Montaggio con client Linux locali utilizzando EFS, AWS Direct Connect mount helper e VPN

Puoi montare i tuoi file system Amazon EFS sui server dei data center locali quando sei connesso ad Amazon VPC AWS Direct Connect con o VPN. L'immagine seguente mostra un diagramma schematico di alto livello dei Servizi AWS requisiti necessari per il montaggio dei file system Amazon EFS da locale.




Per ulteriori informazioni su come utilizzare `amazon-efs-utils` con AWS Direct Connect una VPN per montare i file system Amazon EFS su client Linux locali, consultaProcedura dettagliata: creare e montare un file system in locale con una VPN AWS Direct Connect.

# Montaggio automatico del file system Amazon EFS

Puoi configurare un'istanza Amazon EC2 per montare automaticamente un file system EFS al riavvio utilizzando l'helper di montaggio EFS o NFS.

- Uso dell'helper di montaggio di EFS:
  - Collega un file system EFS quando si crea una nuova istanza EC2 Linux utilizzando la procedura guidata di avvio dell'istanza EC2.
  - Aggiornando il file EC2 `/etc/fstab` con una voce per il file system EFS.
- Utilizzo di NFS senza l'helper di montaggio EFS per aggiornare il file `/etc/fstab` EC2, per supportare le istanze EC2 Linux e Mac.

> **Note**
>
> L'helper di montaggio EFS non supporta il montaggio automatico sulle istanze Amazon EC2 Mac con macOS Big Sur o Monterey. Invece, puoi utilizzare NFS per configurare il file /etc/fstab su un'istanza Mac EC2 per montare automaticamente un file system EFS.

Argomenti



## Utilizzo dell’helper di montaggio EFS per rimontare automaticamente i file system EFS

Utilizza l'assistente di montaggio EFS per configurare `/etc/fstab` su istanze Linux EC2 in modo da rimontare automaticamente i file system EFS al riavvio dell'istanza.

Argomenti

### Collega un file system EFS durante la creazione di un'istanza EC2 per abilitare il montaggio automatico al riavvio

Questo metodo utilizza l'helper di montaggio EFS per montare il file system e aggiornare il file /etc/fstab sull'istanza EC2. Il supporto di montaggio fa parte del set di strumenti `amazon-efs-utils`.

Quando si crea una nuova istanza Amazon EC2 Linux utilizzando la procedura guidata di avvio dell'istanza EC2, è possibile configurarla per montare automaticamente il file system Amazon EFS. L'istanza EC2 monta il file system automaticamente sull'istanza avviata per la prima volta e anche ogni volta che si riavvia.

> **Note**
>
> I file system Amazon EFS non supportano il montaggio su istanze Amazon EC2 Mac con macOS Big Sur o Monterey all'avvio dell'istanza.

Prima di eseguire questa procedura, accertati di avere creato il file system Amazon EFS. Per ulteriori informazioni, consulta Fase 1: Creazione di un file system Amazon EFS nell'esercitazione sulle nozioni di base di Amazon EFS.

> **Note**
>
> Amazon EFS non può essere utilizzato con istanze Amazon EC2 basate su Microsoft Windows.

Prima di poter avviare e connettersi a un'istanza Amazon EC2, è necessario creare una coppia di chiavi, a meno che non sia già disponibile. Segui i passaggi in Configurazione con Amazon EC2 nella Guida per l'utente di Amazon EC2 per le istanze Linux per creare una coppia di chiavi. Se disponi già di una coppia di chiavi, puoi utilizzarla per questo esercizio.

Per configurare l'istanza EC2 affinché monti automaticamente il file system EFS all'avvio

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. In Step 1: Choose an Amazon Machine Image (AMI) (Fase 1: Scegli una Amazon Machine Image (AMI)), trovare un'AMI Amazon Linux all'inizio dell'elenco e scegliere Select (Seleziona).

4. In Fase 2: Scelta di un tipo di istanza scegli Passaggio successivo: Configura i dettagli dell'istanza.
5. In Fase 3: Configurazione dei dettagli dell'istanza, fornisci le seguenti informazioni:
   - Per Network (Rete), scegliere la voce per lo stesso VPC in cui si trova il file system EFS che si sta montando.
   - Per Sottorete, scegli una sottorete predefinita in qualsiasi zona di disponibilità.
   - Per File systems (File system), scegliere il file system EFS da montare. Il percorso mostrato accanto all'ID del file system è il punto di montaggio che verrà utilizzato dall'istanza EC2, che è possibile modificare.
   - In Dettagli avanzati, i dati utente vengono generati automaticamente e includono i comandi necessari per montare i file system EFS specificati in File system.
6. Scegli Passaggio successivo: aggiunta dello storage.
7. Scegliere Passaggio successivo: aggiunta di tag.
8. Denomina l'istanza e scegli Passaggio successivo: configurazione del gruppo di sicurezza.
9. In Fase 6: Configurazione del gruppo di sicurezza, imposta Assegna un gruppo di sicurezza su Seleziona un gruppo di sicurezza esistente. Scegli il gruppo di sicurezza predefinito per assicurarti che possa accedere al file system EFS.

   Non è possibile accedere all'istanza EC2 tramite Secure Shell (SSH) utilizzando questo gruppo di sicurezza. Per l'accesso tramite SSH, successivamente è possibile modificare la sicurezza predefinita e aggiungere una regola per consentire SSH o un nuovo gruppo di sicurezza che consenta SSH. Puoi utilizzare le seguenti impostazioni:

   - Tipo: SSH
   - Protocollo: TCP
   - Intervallo porte: 22
   - Origine: Qualsiasi 0.0.0.0/0
10. Scegli Analizza e avvia.
11. Scegli Avvia.
12. Seleziona la casella di controllo relativa alla coppia di chiavi creata e scegli Avvia istanze.

L'istanza EC2 è ora configurata per montare il file system EFS all'avvio e ogni volta che viene riavviata.

### Utilizzo di **/etc/fstab** con EFS mount helper per rimontare automaticamente i file system EFS

Il file `/etc/fstab` contiene informazioni sui file system. Il comando `mount -a`, che viene eseguito durante l'avvio dell'istanza, monta i file system elencati in `/etc/fstab`. In questa procedura, aggiornerai manualmente `/etc/fstab` su un'istanza EC2 Linux in modo che l'istanza utilizzi l'helper di montaggio EFS per rimontare automaticamente un file system EFS al riavvio dell'istanza.

> **Note**
>
> I file system Amazon EFS non supportano il montaggio automatico utilizzando l'helper `/etc/fstab` di montaggio EFS su istanze Mac Amazon EC2 che eseguono macOS Big Sur o Monterey. Puoi invece utilizzare NFS con `/etc/fstab` per montare automaticamente il tuo file system su istanze Mac EC2 che eseguono macOS Big Sur e Monterey.

Questo metodo utilizza l'helper di montaggio EFS per montare il file system. Il supporto di montaggio fa parte del set di strumenti `amazon-efs-utils`.

Gli strumenti `amazon-efs-utils` sono disponibili per l'installazione su Amazon Linux e Amazon Linux 2 Amazon Machine Image (AMI). Per ulteriori informazioni su `amazon-efs-utils`, consulta Utilizzo degli amazon-efs-utils strumenti. Se si utilizza un'altra distribuzione Linux, ad esempio Red Hat Enterprise Linux (RHEL), compilare e installare manualmente `amazon-efs-utils`. Per ulteriori informazioni, consulta Installazione del client Amazon EFS su altre distribuzioni Linux.

Prerequisiti

Prima di poter implementare con successo questa procedura, è necessario soddisfare i seguenti requisiti:

- Hai già creato il file system Amazon EFS che desideri venga rimontato automaticamente. Per ulteriori informazioni, consulta Fase 1: Creazione di un file system Amazon EFS.
- Hai già creato l'istanza EC2 Linux che desideri configurare per rimontare automaticamente un file system EFS.
- L'helper di montaggio EFS è installato sull'istanza EC2 Linux. Per ulteriori informazioni, consulta Utilizzo degli amazon-efs-utils strumenti.

Per aggiornare il file /etc/fstab nell'istanza EC2

1. Connettiti all'istanza EC2:

- Per connettersi all'istanza da un computer che esegue macOS o Linux, specificare il file .pem per il comando SSH. Per fare ciò, utilizzare l'opzione `-i` e il percorso della chiave privata.
- Per connetterti alla tua istanza da un computer che esegue Windows, puoi usare uno dei due MindTerm o PuTTY. Per utilizzare PuTTY, installarlo e convertire il file .pem in un file .ppk.

Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per l'utente Amazon EC2 per le istanze Linux:

- Connessione all'istanza Linux da Windows tramite PuTTY
- Connessione all'istanza Linux tramite SSH

2. Aprire il file `/etc/fstab` in un editor.
3. Per il montaggio automatico utilizzando l'autorizzazione IAM o un punto di accesso EFS:

   - Per eseguire automaticamente il montaggio con autorizzazione IAM in un'istanza Amazon EC2 che dispone di un profilo dell'istanza, aggiungi la riga seguente al file `/etc/fstab`.

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

   - Per eseguire automaticamente il montaggio con autorizzazione IAM in un'istanza Linux utilizzando un file delle credenziali, aggiungere la seguente riga al file `/etc/fstab`.

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

   - Per eseguire automaticamente il montaggio di un file system utilizzando un punto di accesso, aggiungere la riga seguente al file `/etc/fstab`.

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

   > **Warning**
   >
   > In caso di montaggio automatico del file system, utilizzare l'opzione `_netdev`, usata per identificare i file system di rete. Se `_netdev` è mancante, l'istanza EC2 potrebbe smettere di rispondere. Questo risultato è dovuto al fatto che i file system di rete devono essere inizializzati dopo che l'istanza di calcolo ha avviato la sua interfaccia di rete. Per

ulteriori informazioni, consulta Il montaggio automatico non funziona e l'istanza non risponde.

Per ulteriori informazioni, consultare Montaggio con autorizzazione IAM e Montaggio con punti di accesso EFS.

4. Salvare le modifiche apportate al file.
5. Verificare la voce `fstab` utilizzando il comando `mount` con l'opzione `'fake'` insieme alle opzioni `'all'` e `'verbose'`.

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

L'istanza EC2 è ora configurata per montare il file system EFS ogni volta che si riavvia.

> **Note**
>
> In alcuni casi, potrebbe essere necessario avviare l'istanza Amazon EC2 indipendentemente dallo stato del file system Amazon EFS montato. In questi casi, aggiungere l'opzione `nofail` alla voce del file system nel file `/etc/fstab`.

La riga di codice aggiunta al file `/etc/fstab` imposta quanto segue.

| Campo | Descrizione |
| --- | --- |
| *file-system-id* :/ | L'ID del file system Amazon EFS. Puoi ottenere questo ID dalla console o a livello di codice dalla CLI o da un SDK. AWS |
| *efs-mount-point* | Il punto di montaggio del file system EFS sull'istanza EC2. |
| `efs` | Il tipo di file system. Quando si utilizza l'helper di montaggio, questo tipo è sempre `efs`. |
| `mount options` | Le opzioni di montaggio per il file system. Questo è un elenco separato da virgole delle seguenti opzioni: |

| Campo | Descrizione |
| --- | --- |
| | • `_netdev` - Questa opzione indica al sistema operativo che il file system risiede su un dispositivo che richiede l'accesso di rete. Questa opzione impedisce all'istanza da montare il file system fino a quando la rete non è stata abilitata sul client.<br>• `noresvport` : indica al client NFS di usare una nuova porta TCP (Transmission Control Protocol) di origine quando la connessione di rete viene ripristinata. Ciò contribuisce a garantire che il file system EFS abbia la disponibilità continua dopo un evento di ripristino di rete.<br>• `tls`: abilita la crittografia dei dati in transito.<br>• `iam`: utilizza questa opzione per eseguire il montaggio con l'autorizzazione IAM su un Amazon EC2 con un profilo di istanza. L'utilizzo dell'opzione di montaggio `iam` richiede anche l'utilizzo dell'opzione `tls`. Per ulteriori informazioni, consulta Utilizzo di IAM per controllare l'accesso ai dati del file system.<br>• `awsprofile=` *`namedprofile`* : utilizza questa opzione con le opzioni `iam` e `tls` per eseguire il montaggio con autorizzazione IAM in un'istanza Linux utilizzando un file delle credenziali. Per ulteriori informazioni sui punti di accesso EFS, consulta Utilizzo di IAM per controllare l'accesso ai dati del file system.<br>• `accesspoint=` *`access-point-id`* : utilizza questa opzione con l'opzione`tls` per montare utilizzando un punto di accesso EFS. Per ulteriori informazioni sui punti di accesso EFS, consulta Utilizzo dei punti di accesso Amazon EFS. |
| `0` | Un valore diverso da zero indica che il file system dovrebbe essere soggetto a backup tramite `dump`. Per EFS, questo valore dovrebbe essere impostato a `0`. |
| `0` | L'ordine in base al quale `fsck` verifica i file system all'avvio. Per i file system EFS, questo valore dovrebbe essere `0` a indicare che `fsck` non dovrebbe essere eseguito all'avvio. |

## Utilizzo di NFS per montare automaticamente i file system EFS

Per aggiornare il file **`/etc/fstab`** nell'istanza EC2

1. Connettiti all'istanza EC2:

   - Per connettersi all'istanza da un computer che esegue macOS o Linux, specificare il file .pem per il comando SSH. Per fare ciò, utilizzare l'opzione `-i` e il percorso della chiave privata.
   - Per connetterti alla tua istanza da un computer che esegue Windows, puoi usare uno dei due MindTerm o PuTTY. Per utilizzare PuTTY, installarlo e convertire il file .pem in un file .ppk.

   Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per l'utente Amazon EC2 per le istanze Linux:

   - Connessione all'istanza Linux da Windows tramite PuTTY
   - Connessione all'istanza Linux tramite SSH
2. Aprire il file `/etc/fstab` in un editor.
3. Per montare automaticamente un file system usando NFS invece dell'helper di montaggio EFS, aggiungi la seguente riga al file `/etc/fstab`.

   - Sostituisci *`file_system_id`* con l'ID del file system che stai montando.
   - Sostituisci *`aws-region`* con quello in cui Regione AWS è installato il file system, ad esempio. `us-east-1`
   - Sostituisci *`mount_point`* con il punto di montaggio del file system.

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

La riga di codice aggiunta al file `/etc/fstab` imposta quanto segue.

| Campo | Descrizione |
| --- | --- |
| *`file-system-id`* `:/` | L'ID del file system Amazon EFS. Puoi ottenere questo ID dalla console o a livello di codice dalla CLI o da un SDK. AWS |

| Campo | Descrizione |
| --- | --- |
| *efs-mount-point* | Il punto di montaggio del file system EFS sull'istanza EC2. |
| nfs4 | Specifica il tipo di file system. |

| Campo | Descrizione |
| --- | --- |
| `mount options` | L'elenco separato da virgole delle opzioni di montaggio per il file system:<br>• `nfsvers=4.1` : specifica l'utilizzo di NFS v4.1.<br>• `rsize=1048576` : per migliorare le prestazioni, imposta il numero massimo di byte di dati che il client NFS può ricevere per ogni richiesta READ di rete durante la lettura di dati da un file su un file system EFS. `1048576` è la massima dimensione possibile.<br>• `wsize=1048576` : per migliorare le prestazioni, imposta il numero massimo di byte di dati che il client NFS può inviare per ogni richiesta di rete WRITE quando si scrivono dati su un file in un file system EFS. `1048576` è la massima dimensione possibile.<br>• `hard`: imposta il comportamento di ripristino del client NFS dopo il timeout di una richiesta NFS, in modo che la richiesta NFS venga ritentata a tempo indeterminato fino alla risposta del server. È consigliabile utilizzare l'opzione di montaggio hard (`hard`) per garantire l'integrità dei dati. Se utilizzi un mofintaggio `soft`, imposta il parametro `timeo` su almeno `150` decisecondi (15 secondi). In questo modo consenti di ridurre al minimo il rischio di danneggia mento dei dati che è insito nei montaggi soft.<br>• `timeo=600` : imposta il valore di timeout utilizzato dal client NFS in attesa di una risposta prima di ripetere la richiesta NFS su 600 decisecondi (60 secondi). Se è necessario modificare il parametro timeout (`timeo`), si consiglia di utilizzare un valore di almeno `150`, che è pari a 15 secondi. In questo modo è possibile evitare una riduzione delle prestazioni.<br>• `retrans=2` : imposta su 2 il numero di volte che il client NFS ritenta una richiesta prima di eseguire un'altra operazione di ripristin o.<br>• `noresvport` : indica al client NFS di usare una nuova porta TCP (Transmission Control Protocol) di origine quando la connessione di rete viene ripristinata. Ciò contribuisce a garantire che il file system |

| Campo | Descrizione |
| --- | --- |
| | EFS abbia la disponibilità continua dopo un evento di ripristino di rete.<br>• `_netdev`: impedisce al client di tentare di montare il file system EFS fino a quando la rete non è stata abilitata. |
| `0` | Specifica il valore `dump`; `0` indica all'utility `dump` di evitare di eseguire il backup del file system. |
| `0` | Indica di evitare di eseguire l'utility `fsck` all'avvio. |

## Montaggio di EFS su più istanze EC2 utilizzando AWS Systems Manager

Puoi montare i file system EFS su più istanze Amazon EC2 in remoto e in modo sicuro senza dover accedere alle istanze utilizzando il comando. AWS Systems Manager Run Per ulteriori informazioni su AWS Systems Manager Run Command, consulta AWS Systems Manager run command nella Guida per l'utente.AWS Systems Manager  Prima di montare i file system EFS con questo metodo, sono necessari i seguenti prerequisiti:

1. Le istanze EC2 vengono avviate con un profilo di istanza che include la policy `AmazonElasticFileSystemsUtils` delle autorizzazioni. Per ulteriori informazioni, consulta Fase 1: Configurazione di un profilo di istanza IAM con le autorizzazioni richieste.
2. La versione 1.28.1 o successiva del client Amazon EFS (amazon-efs-utils pacchetto) è installata sulle istanze EC2. È possibile utilizzare AWS Systems Manager per installare automaticamente il pacchetto sulle istanze. Per ulteriori informazioni, consulta Fase 2: Configurazione di un'associazione utilizzata da State Manager per l'installazione o l'aggiornamento del client Amazon EFS.

Montaggio di più file system EFS su più istanze EC2 utilizzando la console

1. Aprire la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione seleziona Esegui comando.
3. Scegli Esegui comando.
4. Inserisci **`AWS-RunShellScript`** nel campo di ricerca Comandi.

5. Seleziona AWS- RunShellScript.
6. In Parametri di comando immetti il comando di montaggio da utilizzare per ogni file system EFS che desideri montare. Per esempio:

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

   Per ulteriori informazioni sui comandi di montaggio EFS utilizzando il client Amazon EFS, consulta Montaggio su istanze Amazon EC2 Linux utilizzando l'helper di montaggio EFS o Montaggio su istanze Mac Amazon EC2 utilizzando l'helper di montaggio EFS.
7. Seleziona le istanze EC2 AWS Systems Manager gestite di destinazione su cui desideri eseguire il comando.
8. Effettua tutte le altre impostazioni aggiuntive secondo necessità. Quindi, scegli Esegui per eseguire il comando e montare i file system EFS specificati nel comando.

   Una volta eseguito il comando, è possibile visualizzare il relativo stato nella cronologia dei comandi.

## Montaggio di file system EFS da un altro Account AWS o da un VPC

È possibile montare il file system Amazon EFS utilizzando l'autorizzazione IAM per i client NFS e i punti di accesso EFS usando l'helper di montaggio EFS. Per impostazione predefinita, l'helper di montaggio EFS utilizza il servizio DNS (Domain Name Service) per risolvere l'indirizzo IP del target di montaggio EFS. Se si sta montando il file system da un altro account o da un cloud privato virtuale (VPC), è necessario risolvere manualmente il target di montaggio EFS.

Di seguito, è possibile trovare le istruzioni per determinare l'indirizzo IP di target di montaggio EFS corretto da utilizzare per il client NFS. È inoltre possibile trovare istruzioni per configurare il client e montare il file system EFS utilizzando tale indirizzo IP.

### Montaggio utilizzando IAM o i punti di accesso da un altro VPC

Quando si utilizza una connessione peering VPC o Transit Gateway per connettere i VPC, le istanze Amazon EC2 in un VPC possono accedere ai file system EFS in un altro VPC, anche se i VPC appartengono a account diversi.

### Prerequisiti

Prima di utilizzare la procedura seguente, attieniti ai passaggi seguenti:

- Installa il client Amazon EFS, parte del set `amazon-efs-utils` di utility sull'istanza di calcolo su cui stai montando il file system EFS. Si utilizza l'helper di montaggio EFS, incluso in `amazon-efs-utils`, per montare il file system. Per istruzioni sull'installazione di `amazon-efs-utils`, vedere Utilizzo degli amazon-efs-utils strumenti.
- Consenti l'azione `ec2:DescribeAvailabilityZones` nella policy IAM per il ruolo IAM che hai associato all'istanza. Ti consigliamo di allegare la policy AWS gestita `AmazonElasticFileSystemsUtils` a un'entità IAM per fornire le autorizzazioni necessarie all'entità.
- Durante il montaggio da un altro Account AWS, aggiorna la politica delle risorse del file system per consentire l'`elasticfilesystem:DescribeMountTarget`azione per l'ARN principale di un altro. Account AWS Per esempio:

```
{
    "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"
        }
    ]
}
```

  Per ulteriori informazioni sulle policy delle risorse del file system EFS, consulta Policy basate su risorse all'interno di Amazon EFS.
- Installa botocore. Il client EFS utilizza botocore per recuperare l'indirizzo IP del target di montaggio quando il nome DNS del file system non può essere risolto durante il montaggio di un file system in un altro VPC. Per ulteriori informazioni, consulta Installazione di botocore nel file README `amazon-efs-utils`.
- Configurare una connessione di peering VPC o un gateway di transito VPC.

Connettere il VPC del client e il VPC del file system EFS utilizzando una connessione di peering VPC o un gateway di transito VPC. Quando si utilizza una connessione peering VPC o Transit Gateway per connettere i VPC, le istanze Amazon EC2 in un VPC possono accedere ai file system EFS in un altro VPC, anche se i VPC appartengono a account diversi.

Un Transit Gateway è un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti locali. Per ulteriori informazioni sull'utilizzo di VPC Transit Gateway, consulta l'argomento relativo alle nozioni di base su Transit Gateway nella Guida di Amazon VPC Transit Gateway.

Una connessione di peering VPC è una connessione di rete tra due VPC. Questo tipo di connessione consente di instradare il traffico tra di essi utilizzando indirizzi IPv4 (Internet Protocol version 4) o IPv6 (Internet Protocol version 6) privati. Puoi utilizzare il peering VPC per connettere VPC all'interno dello stesso Regione AWS o tra di s. Regione AWS Per ulteriori informazioni, consulta Che cos'è il peering di VPC? nella Guida al peering di Amazon VPC.

Per garantire la disponibilità elevata del file system, si consiglia di utilizzare sempre un indirizzo IP di destinazione del montaggio EFS che si trova nella stessa zona di disponibilità (AZ) del client NFS. Se si sta montando un file system EFS in un altro account, assicurati che il client NFS e il target di montaggio EFS siano nello stesso ID della zona di disponibilità. Questo requisito si applica perché i nomi AZ possono differire da un account all'altro.

Per montare un file system EFS in un altro VPC utilizzando IAM o un punto di accesso

1. Connettiti all'istanza EC2:

   - Per connettersi all'istanza da un computer che esegue macOS o Linux, specificare il file .pem per il comando SSH. Per fare ciò, utilizzare l'opzione `-i` e il percorso della chiave privata.
   - Per connetterti alla tua istanza da un computer che esegue Windows, puoi usare uno dei due MindTerm o PuTTY. Per utilizzare PuTTY, installarlo e convertire il file .pem in un file .ppk.

   Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per l'utente Amazon EC2 per le istanze Linux:

   - Connessione all'istanza Linux da Windows tramite PuTTY
   - Connessione all'istanza Linux tramite SSH
2. Creare una directory per il montaggio del file system utilizzando il seguente comando.

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

3. Per montare il file system utilizzando l'autorizzazione IAM, utilizzare il seguente comando:

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

   Per ulteriori informazioni sull'utilizzo dell'autorizzazione IAM con EFS, vedere Utilizzo di IAM per controllare l'accesso ai dati del file system.

   Per montare il file system utilizzando un punto di accesso EFS, utilizzare il comando seguente:

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

   Per ulteriori informazioni sui punti di accesso EFS, consulta Utilizzo dei punti di accesso Amazon EFS.

Montaggio dei file system Amazon EFS da un altro Regione AWS

Se stai montando il file system EFS da un altro VPC che si trova in un file system Regione AWS diverso dal file, dovrai modificare il `efs-utils.conf` file. In `/dist/efs-utils.conf` individua le righe seguenti:

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

Rimuovi i commenti dalla riga e sostituisci il valore dell'ID della regione in cui si trova il file system, se non è presente in `us-east-1`.

## Montaggio da un altro Account AWS nello stesso VPC

Utilizzando VPC condivisi, puoi montare un file system Amazon EFS di proprietà di una delle Account AWS istanze Amazon EC2 di proprietà di un'altra istanza. Account AWS Per ulteriori informazioni sulla configurazione di un VPC condiviso, consulta la sezione Utilizzo dei VPC condivisi nella Guida al peering di Amazon VPC.

Dopo aver configurato la condivisione VPC, le istanze EC2 possono montare il file system EFS utilizzando la risoluzione dei nomi Domain Name System (DNS) o l'helper EFS. Si consiglia di montare il file system EFS utilizzando l'helper di montaggio EFS.

# Ulteriori considerazioni sul montaggio

Consigliamo i seguenti valori predefiniti per le opzioni di montaggio su Linux:

- `rsize=1048576`: imposta il numero massimo di byte di dati che il client NFS è in grado di ricevere per ogni richiesta READ della rete. Questo valore si applica per la lettura dei dati da un file in un file system EFS. È consigliabile utilizzare la dimensione massima possibile (fino a `1048576`) per evitare una riduzione delle prestazioni.
- `wsize=1048576`: imposta il numero massimo di byte di dati che il client NFS è in grado di inviare per ogni richiesta WRITE della rete. Questo valore si applica per la scrittura dei dati in un file in un file system EFS. È consigliabile utilizzare la dimensione massima possibile (fino a `1048576`) per evitare una riduzione delle prestazioni.
- `hard`: imposta il comportamento di ripristino del client NFS dopo il timeout di una richiesta NFS, in modo che la richiesta NFS venga ritentata a tempo indeterminato fino alla risposta del server. È consigliabile utilizzare l'opzione di montaggio hard (`hard`) per garantire l'integrità dei dati. Se utilizzi un mofintaggio `soft`, imposta il parametro `timeo` su almeno `150` decisecondi (15 secondi). In questo modo consenti di ridurre al minimo il rischio di danneggiamento dei dati che è insito nei montaggi soft.
- `timeo=600`: imposta il valore di timeout utilizzato dal client NFS in attesa di una risposta prima di ripetere la richiesta NFS su 600 decisecondi (60 secondi). Se è necessario modificare il parametro timeout (`timeo`), si consiglia di utilizzare un valore di almeno `150`, che è pari a 15 secondi. In questo modo è possibile evitare una riduzione delle prestazioni.
- `retrans=2`: imposta su 2 il numero di volte che il client NFS ritenta una richiesta prima di eseguire un'altra operazione di ripristino.
- `noresvport`: indica al client NFS di usare una nuova porta TCP (Transmission Control Protocol) di origine quando la connessione di rete viene ripristinata. Ciò contribuisce a garantire che il file system EFS abbia la disponibilità continua dopo un evento di ripristino di rete.
- `_netdev`: se presente in `/etc/fstab` impedisce al client di tentare di montare il file system EFS fino a quando la rete non è stata abilitata.

In generale, evita di impostare opzioni di montaggio diverse dai valori predefiniti in quanto possono causare una riduzione delle prestazioni e altri problemi. Se non usi i valori predefiniti precedenti, tieni presente quanto segue:

- La modifica della dimensione dei buffer di lettura o scrittura o la disabilitazione del caching degli attributi possono ridurre le prestazioni.
- Amazon EFS ignora le porte di origine. La modifica delle porte di origine di Amazon EFS non ha alcun effetto.
- Amazon EFS non supporta nessuna delle varianti di sicurezza di Kerberos. Ad esempio, il seguente comando di montaggio non ha esito positivo.

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

- È consigliabile montare il file system utilizzando il nome DNS. Amazon EFS risolve questo nome con l'indirizzo IP del target di montaggio Amazon EFS nella stessa zona di disponibilità dell'istanza Amazon EC2 senza chiamare risorse esterne. Se utilizzi un target di montaggio in una zona di disponibilità diversa da quella dell'istanza Amazon EC2 incorri nei costi EC2 standard per i dati inviati nelle zone di disponibilità. Potresti anche osservare un aumento delle latenze per le operazioni del file system.
- Per ulteriori opzioni di montaggio e una spiegazione dettagliata delle impostazioni predefinite, consulta le pagine `man fstab` e `man nfs` della documentazione di Linux.

> **Note**
>
> Se l'istanza EC2 deve avviarsi indipendentemente dallo stato del montaggio del file system EFS, aggiungere l'opzione `nofail` alla voce del file system nel file `/etc/fstab`.

## Smontaggio dei file system

Prima di eliminare un file system, consigliamo di smontarlo da ogni istanza Amazon EC2 che si è connessa ad esso. È possibile smontare un file system sull'istanza Amazon EC2 eseguendo il comando `umount` sull'istanza stessa. Non puoi smontare un file system Amazon EFS tramite AWS CLI AWS Management Console, il o tramite uno qualsiasi degli AWS SDK. Per smontare un file system Amazon EFS connesso a un'istanza Amazon EC2 su cui è in esecuzione Linux, utilizza il comando `umount` come segue:

```
umount /mnt/efs
```

È consigliabile non specificare nessun'altra opzione di `umount`. Evitare di impostare qualsiasi altra opzione di `umount` differente da quelle di default.

È possibile verificare che il file system Amazon EFS sia stato smontato eseguendo il comando `df`. Questo comando visualizza le statistiche sull'utilizzo del disco per i file system attualmente montati nell'istanza Amazon EC2 basata su Linux. Se il file system Amazon EFS che si desidera smontare non è presente nell'output del comando `df`, ciò significa che il file system è smontato.

Example Identificazione dello stato di montaggio di un file system Amazon EFS per smontarlo

```
$ 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% /
```

## Risoluzione dei problemi con versioni di AMI e kernel

Per risolvere i problemi correlati a specifiche versioni di Amazon Machine Image (AMI) o kernel durante l'utilizzo di Amazon EFS da un'istanza Amazon EC2, consulta Risoluzione dei problemi di AMI e kernel.

> **Note**
>
> Amazon EFS non supporta il montaggio da istanze Windows di Amazon EC2.

# Trasferimento di dati da e verso Amazon EFS

Puoi usare AWS Transfer Family e AWS DataSync trasferire dati da e verso i tuoi file system Amazon EFS. AWS DataSyncè un servizio di trasferimento dati online in grado di copiare dati tra file server Network File System (NFS), Server Message Block (SMB), storage di oggetti autogestito e anche tra servizi. AWS Per ulteriori informazioni sull'utilizzo DataSync con Amazon EFS, consultaUtilizzo AWS DataSync per trasferire dati in Amazon EFS.

AWS Transfer Familyè un AWS servizio completamente gestito che puoi utilizzare per trasferire file da e verso i file system Amazon EFS tramite i protocolli Secure File Transfer Protocol (SFTP), File Transfer Protocol (FTP) e FTP over Secure Sockets Layer (FTPS). Utilizzando Transfer Family, puoi fornire ai tuoi partner commerciali l'accesso ai file archiviati nei tuoi file system Amazon EFS per casi d'uso come distribuzione dei dati, catena di fornitura, gestione dei contenuti e applicazioni di web serving. Per ulteriori informazioni sull'utilizzo di Transfer Family con Amazon EFS, consultaUtilizzo di AWS Transfer Family per accedere ai file nel file system Amazon EFS.

Argomenti



## Utilizzo AWS DataSync per trasferire dati in Amazon EFS

AWS DataSyncè un servizio di trasferimento dati online che semplifica, automatizza e accelera lo spostamento e la replica dei dati tra sistemi di storage locali e anche tra servizi di storage. AWS DataSyncpuò copiare dati tra file server Network File System (NFS), Server Message Block (SMB), storage di oggetti autogestitoAWS Snowcone, bucket Amazon S3, file system Amazon EFS e file system FSx per Windows File Server.

È inoltre possibile utilizzarlo DataSync per trasferire file tra due file system Regione AWS EFS, inclusi file system in sistemi diversi e file system di proprietà di sistemi diversiAccount AWS. Utilizzando DataSync per copiare i dati tra i file system EFS, è possibile eseguire migrazioni dei dati in un'unica fase, l'acquisizione di dati periodici per i carichi di lavoro distribuiti e la replica automatica per la protezione e il ripristino dei dati.

Per ulteriori informazioni, consulta Guida introduttiva ad Amazon Elastic File System e la Guida per l'utente di AWS DataSync.

# Utilizzo di AWS Transfer Family per accedere ai file nel file system Amazon EFS

AWS Transfer Family è un servizio AWS completamente gestito che puoi utilizzare per trasferire file da e verso i file system Amazon EFS tramite i seguenti protocolli:

- Secure Shell (SSH) File Transfer Protocol (SFTP) (AWS Transfer for SFTP)
- File Transfer Protocol Secure (FTPS) (AWS Transfer for FTPS)
- File Transfer Protocol (FTP) (AWS Transfer for FTP)

Utilizzando Transfer Family, puoi consentire a terze parti come fornitori, partner o clienti di accedere in modo sicuro ai tuoi file tramite i protocolli supportati su larga scala a livello globale, senza dover gestire alcuna infrastruttura. Inoltre, ora puoi accedere facilmente ai tuoi file system EFS da ambienti Windows, macOS e Linux utilizzando client SFTP, FTPS e FTP. Ciò consente di espandere l'accessibilità dei dati oltre i client e i punti di accesso NFS, agli utenti in più ambienti.

L'utilizzo di Transfer Family per trasferire dati nei file system Amazon EFS viene contabilizzato allo stesso modo dell'utilizzo di altri client. Per ulteriori informazioni, consultare Modalità di velocità di trasmissione effettiva e Quote e limiti di Amazon EFS.

Per ulteriori informazioni su AWS Transfer Family, consulta la Guida per l'utente di AWS Transfer Family.

> **Note**
>
> L'uso di Transfer Family con Amazon EFS è disabilitato per impostazione predefinita per Account AWS con file system EFS con policy che consentono l'accesso pubblico create prima del 6 gennaio 2021. Per abilitare l'utilizzo di Transfer Family per accedere al file system, contatta AWS Support.

Argomenti

- Prerequisiti per l'uso di AWS Transfer Family con Amazon EFS
- Configurazione del file system Amazon EFS per lavorare con AWS Transfer Family

# Prerequisiti per l'uso di AWS Transfer Family con Amazon EFS

Per utilizzare Transfer Family per accedere ai file del file system Amazon EFS, la configurazione deve soddisfare le seguenti condizioni:

- Il server Transfer Family e il file system Amazon EFS si trovano nella stessa Regione AWS.
- Le policy IAM sono configurate per consentire l'accesso al ruolo IAM utilizzato da Transfer Family. Per ulteriori informazioni, consulta Creazione di un ruolo e una policy IAM nella Guida per l'utente di AWS Transfer Family.
- (Facoltativo) Se il server Transfer Family è di proprietà di un account diverso, abilita l'accesso multi-account.
  - Assicurati che la policy del tuo file system non consenta l'accesso pubblico. Per ulteriori informazioni, consulta Blocco dell'accesso pubblico.
  - Modifica la policy del file system per abilitare l'accesso multi-account. Per ulteriori informazioni, consulta Configurazione dell'accesso multi-account per Transfer Family.

# Configurazione del file system Amazon EFS per lavorare con AWS Transfer Family

La configurazione di un file system Amazon EFS per l'utilizzo con Transfer Family richiede i seguenti passaggi:

- Fase 1:  Ottieni l'elenco degli ID POSIX assegnati agli utenti Transfer Family.
- Fase 2. Assicurati che le directory del tuo file system siano accessibili agli utenti di Transfer Family utilizzando gli ID POSIX assegnati agli utenti di Transfer Family.
- Fase 3. Configura IAM per consentire l'accesso al ruolo IAM utilizzato da Transfer Family.

## Impostazione delle autorizzazioni per file e directory per gli utenti di Transfer Family

Assicurati che gli utenti di Transfer Family abbiano accesso ai file e alle directory necessari sul tuo file system EFS. Assegna i permessi di accesso alla directory utilizzando l'elenco di ID POSIX assegnati agli utenti di Transfer Family. In questo esempio, un utente crea una directory denominata `transferFam` sotto il punto di montaggio EFS. La creazione di una directory è facoltativa, a seconda del caso d'uso. Se necessario, è possibile sceglierne il nome e la posizione nel file system EFS.

Assegnazione delle autorizzazioni per file e directory per gli utenti POSIX di Transfer Family

1. Esegui la connessione all'istanza Amazon EC2. Amazon EFS supporta solo il montaggio tramite istanze EC2 basate su Linux.
2. Monta il file system EFS se non è già montato sull'istanza EC2. Per ulteriori informazioni, consulta Montaggio dei file system EFS.
3. L'esempio seguente crea la directory sul file system EFS e ne modifica il gruppo nell'ID di gruppo POSIX per gli utenti di Transfer Family, che in questo esempio è 1101.

   a. Esegui i seguenti comandi per creare la directory `efs/transferFam`. In pratica, è possibile utilizzare un nome e una posizione nel file system di propria scelta.

   ```
   [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. Usa il seguente comando per cambiare il gruppo di `efs/transferFam` nel GID POSIX assegnato agli utenti Transfer Family.

   ```
   [ec2-user@ip-192-0-2-0 ~]$ sudo chown :1101 efs/transferFam/
   ```

   c. Conferma la modifica.

   ```
   [ec2-user@ip-192-0-2-0 ~]$ ls -l efs
   total 0
   drwxr-xr-x 2 root 1101 6 Jan  6 15:58 transferFam
   ```

## Consenso dell'accesso al ruolo IAM utilizzato da Transfer Family

In Transfer Family, crei una policy IAM basata sulle risorse e un ruolo IAM che definiscono l'accesso degli utenti al file system EFS. Per ulteriori informazioni, consulta Creazione di un ruolo e una policy IAM nella Guida per l'utente di AWS Transfer Family. È necessario concedere al ruolo IAM di Transfer Family l'accesso al file system EFS utilizzando una policy di identità IAM o una policy del file system.

Di seguito è riportato un esempio di policy del file system che concede l'accesso `ClientMount` (in lettura) e `ClientWrite` al ruolo `EFS-role-for-transfer` IAM.

```
{
    "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"
            ]
        }
    ]
}
```

Per ulteriori informazioni sulla creazione di una policy di file system, consulta Creazione di policy del file system. Per ulteriori informazioni sull'utilizzo delle policy IAM basate sull'identità per gestire l'accesso alle risorse EFS, consulta Policy basate su identità per Amazon EFS.

## Configurazione dell'accesso multi-account per Transfer Family

Se il server Transfer Family utilizzato per accedere al file system appartiene a un altro Account AWS, è necessario concedere a tale account l'accesso al file system. Inoltre, la policy del file system non deve essere pubblica. Per ulteriori informazioni sul blocco dell'accesso pubblico al file system, consulta Blocco dell'accesso pubblico.

È possibile concedere un accesso Account AWS diverso al file system nella policy del file system. Nella console Amazon EFS, utilizza la sezione Concedi autorizzazioni aggiuntive dell'Editor delle policy del file system per specificare Account AWS e il livello di accesso al file system che stai concedendo. Per ulteriori informazioni sulla creazione o modifica di una policy di file system, consulta Creazione di policy del file system.

Puoi specificare l'account utilizzando l'ID dell'account o l'account nome della risorsa Amazon (ARN). Per ulteriori informazioni sugli ARN, consulta ARN IAM nella Guida per l'utente IAM.

L'esempio seguente è una policy di file system non pubblica che concede l'accesso multi-account al file system. Contiene le due istruzioni seguenti:

1. La prima istruzione `NFS-client-read-write-via-fsmt` concede i privilegi di lettura, scrittura e root ai client NFS che accedono al file system utilizzando una destinazione di montaggio del file system.
2. La seconda istruzione `Grant-cross-account-access` concede solo i privilegi di lettura e scrittura a Account AWS 111122223333, ossia l'account proprietario del server Transfer Family che necessita dell'accesso a questo file system EFS nel tuo account.

```
{
    "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 seguente policy del file system aggiunge una dichiarazione che concede l'accesso al ruolo IAM utilizzato da 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"
            ]
        }
    ]
}
```

# Gestione dei file system Amazon EFS

Le attività di gestione dei file system si riferiscono alla creazione e all'eliminazione dei file system e alla gestione dei tag, dei backup dei file system, dell'accesso e dell'accessibilità alla rete con i target di montaggio dei file system esistenti.

È possibile eseguire queste attività di gestione del file system utilizzando o utilizzando programmaticamente AWS Command Line Interface (AWS CLI) o l'API, come illustrato nelle sezioni seguenti. AWS Management Console

Argomenti



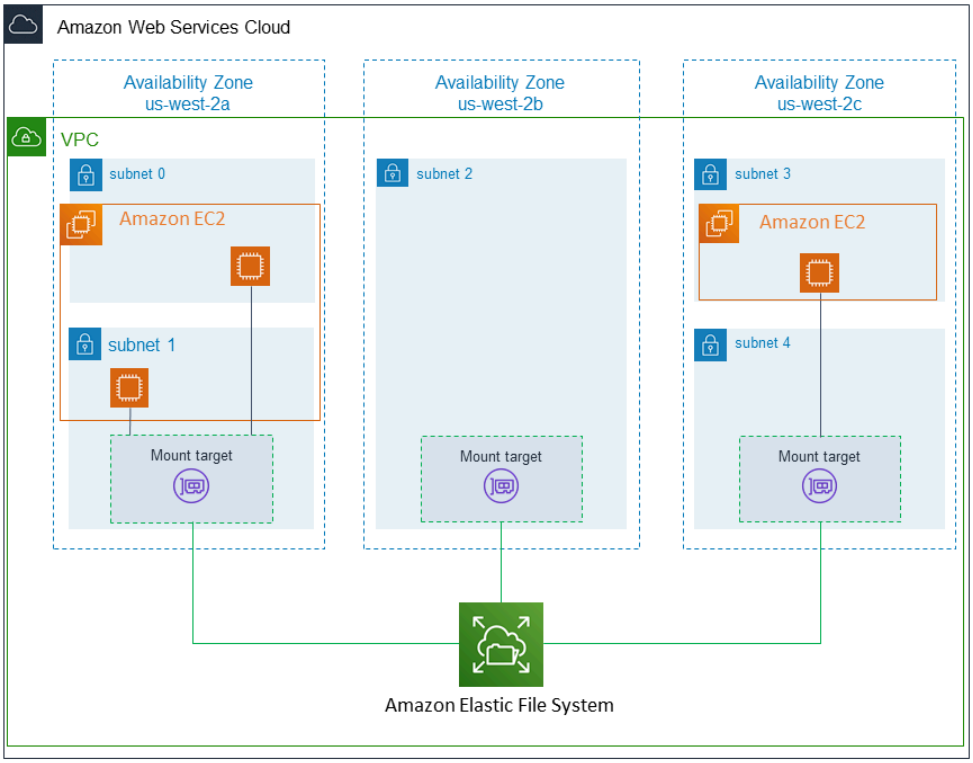
Se non conosci Amazon EFS, ti consigliamo di provare i seguenti esercizi che ti forniranno un' end-to-end esperienza diretta con un file system Amazon EFS:

- Nozioni di base— Questo esercizio fornisce una end-to-end configurazione basata su console in cui è possibile creare un file system, montarlo su un'istanza Amazon EC2 e testare la configurazione. La console si occupa di molte cose al posto tuo e quindi ti aiuta a configurare rapidamente l'esperienza. end-to-end
- Procedura dettagliata: Creazione di un file system Amazon EFS e montarlo su un'istanza Amazon EC2 utilizzandoAWS CLI— Questa procedura dettagliata è simile all'esercizio Guida introduttiva, ma la utilizza AWS CLI per eseguire la maggior parte delle attività. Poiché i comandi della CLI riproducono fedelmente l'API Amazon EFS, lo scenario può aiutare a familiarizzare con le API Amazon EFS.

# Gestione dell'accessibilità del file system dalla rete

Monti il tuo file system su Amazon EC2 o un'altra istanza di AWS calcolo nel tuo cloud privato virtuale (VPC) utilizzando una destinazione di montaggio che crei per il file system. La gestione dell'accessibilità di rete del file system fa riferimento alla gestione dei target di montaggio del sistema.

La figura seguente mostra il modo in cui le istanze EC2 in una VPC accedono a un file system Amazon EFS utilizzando un target di montaggio.




L'illustrazione mostra tre istanze EC2 avviate in diverse sottoreti della VPC che accedono a un file system Amazon EFS. Viene inoltre evidenziato un target di montaggio in ciascuna delle zone di disponibilità (indipendentemente dal numero di sottoreti in ciascuna zona di disponibilità).

È possibile specificare solo un target di montaggio per ogni zona di disponibilità. Se una zona di disponibilità possiede più sottoreti, come illustrato in una delle zone nell'illustrazione, è necessario creare un target di montaggio in una sola delle sottoreti. Disponendo di un target di montaggio in una zona di disponibilità, le istanze EC2 avviate in una qualsiasi delle sue sottoreti possono condividere lo stesso target di montaggio.

La gestione dei target di montaggio fa riferimento a queste attività:

- Creazione e cancellazione di target di montaggio in una VPC - È consigliabile creare almeno un target di montaggio in ciascuna zona di disponibilità da cui si desidera accedere al file system.

  > **Note**
  >
  > È consigliabile creare target di montaggio in tutte le zone di disponibilità. In tal caso, è possibile installare con facilità il file system su istanze EC2 che possono essere avviate in tutte le zone di disponibilità.

  Se si elimina un target di montaggio, l'operazione forza la cancellazione di tutti i montaggi del file system, con possibili conseguenze sulle istanze o sulle applicazioni che utilizzano tali montaggi. Per evitare il malfunzionamento delle applicazioni, arresta le applicazioni e disinstalla il file system prima di eliminare il target di montaggio.

  È possibile usare un file system solo in una sola VPC alla volta. Ciò significa che è possibile creare target di montaggio per il file system in una sola VPC alla volta. Se si desidera accedere al file system da un altro VPC, elimina prima il target di montaggio dall'attuale VPC. Crea quindi nuovi target di montaggio in un altro VPC.
- Aggiornamento della configurazione del target di montaggio – quando viene creato un target di montaggio, a esso vengono associati i gruppi di sicurezza. Un gruppo di sicurezza agisce come un firewall virtuale che controlla il traffico in ingresso e in uscita dal target di montaggio. È possibile aggiungere regole in entrata per controllare l'accesso ai target di montaggio e, di conseguenza, al file system. Dopo aver creato un target di montaggio, è possibile modificare i gruppi di sicurezza assegnati a esso.

  Ogni target di montaggio, inoltre, dispone di un indirizzo IP. Quando si crea un target di montaggio, è possibile scegliere un indirizzo IP dalla sottorete in cui si sta collocando il target di montaggio. Se si omette un valore, Amazon EFS seleziona un indirizzo IP non utilizzato da quella sottorete.

  Non esiste alcuna operazione Amazon EFS per modificare l'indirizzo IP dopo la creazione di un target di montaggio. Pertanto, non è possibile modificare l'indirizzo IP a livello di codice o utilizzando AWS CLI. Tuttavia, la console consente di modificare l'indirizzo IP. Dietro le quinte, la console elimina il target di montaggio e lo crea di nuovo.

> **Warning**
>
> Se si modifica l'indirizzo IP di un target di montaggio, si interrompono i montaggi dei file system ed è necessario rimontare tali file system.

Nessuna delle modifiche alla configurazione dell'accessibilità a un file system dalla rete ha effetto sul file system in sé. I file system e i dati rimangono intatti.

Le seguenti sezioni forniscono informazioni su come gestire l'accessibilità dei file system dalla rete.

Argomenti



## Creazione o eliminazione di target di montaggio in una VPC

Per accedere a un file system Amazon EFS in una VPC, è necessario disporre di target di montaggio. In caso di file system Amazon EFS, vale quanto segue:

- È possibile creare un target di montaggio per ogni zona di disponibilità.
- Se la VPC dispone di più sottoreti in una zona di disponibilità, è possibile creare un target di montaggio in una sola di tali sottoreti. Tutte le istanze EC2 nella zona di disponibilità possono condividere il singolo target di montaggio.

> **Note**
>
> È consigliabile creare un target di montaggio in ciascuna delle zone di disponibilità. Ci sono delle considerazioni di costo di cui tenere conto per il montaggio di un file system su un'istanza EC2 in una zona di disponibilità attraverso un target di montaggio creato in un'altra zona di disponibilità. Per ulteriori dettagli, consulta Amazon EFS. Inoltre, usando sempre un target di montaggio locale nella zona di disponibilità dell'istanza, è possibile eliminare lo scenario del fallimento parziale. Se la zona del target di montaggio diventa inutilizzabile, non sarà possibile accedere ai file system tramite tale target di montaggio.

È possibile eliminare i target di montaggio. La cancellazione di un target di montaggio forza la cancellazione di tutti i montaggi del file system eseguiti tramite tale target di montaggio, con possibili conseguenze sulle istanze e sulle applicazioni che utilizzano tali montaggi. Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

> **Note**
>
> Prima di eliminare un target di montaggio, smontare il file system. Per ulteriori informazioni, consulta Smontaggio dei file system.

Utilizzando AWS Management Console, the e l'API AWS CLI, puoi creare e gestire obiettivi di montaggio sui file system. Per i target di montaggio esistenti, è possibile aggiungere e rimuovere gruppi di sicurezza o eliminare il target di montaggio. Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

## Modifica della VPC per il target di montaggio

È possibile usare un file system Amazon EFS in un VPC basato sul servizio Amazon VPC alla volta. Ciò significa che è possibile creare target di montaggio in una VPC per i file system e utilizzare questi target di montaggio per fornire l'accesso ai file system.

È possibile montare il file system Amazon EFS a partire da questi target:

- Istanze Amazon EC2 nella stessa VPC
- Istanze EC2 in una VPC connessa tramite peering VPC
- Server locali utilizzando AWS Direct Connect
- Server locali su una rete privata AWS virtuale (VPN) utilizzando Amazon VPC

Una connessione peering VPC è una connessione di rete tra due VPC che ti consente di instradare il traffico tra essi. La connessione può utilizzare indirizzi IP versione 4 (IPv4) o indirizzi IP versione 6 (IPv6) privati. Per ulteriori informazioni su come funziona Amazon EFS con il peering VPC, consulta Montaggio di file system EFS da un altro Account AWS o da un VPC.

Per accedere al file system dalle istanze EC2 in un’altra VPC, devi:

- Eliminare i target di montaggio correnti.

- Cambiare VPC.
- Creare nuovi target di montaggio.

Per ulteriori informazioni sull'esecuzione di questi passaggi in AWS Management Console, consulta. Come modificare il VPC per un file system Amazon EFS (console)

### Utilizzo della CLI

Per utilizzare un file system in un altro VPC, elimina prima alcuni target di montaggio creati in precedenza in una VPC. Crea quindi nuovi target di montaggio in un altro VPC. Per comandi AWS CLI di esempio, consulta Gestione dei target di montaggio utilizzando AWS CLI.

## Aggiornamento della configurazione del target di montaggio

Dopo aver creato un target di montaggio per il file system, potrebbe essere necessario aggiornare i gruppi di sicurezza attivi. Non è possibile modificare l'indirizzo IP di un target di montaggio esistente. Per modificare un indirizzo IP, eliminare il target di montaggio e crearne uno nuovo con il nuovo indirizzo. L'eliminazione di un target di montaggio esistente interrompe tutti i montaggi del file system.

> **Note**
>
> Prima di eliminare un target di montaggio, smontare il file system.

### Modifica di un gruppo di sicurezza

I gruppi di sicurezza definiscono le possibilità di accesso in entrata e in uscita. Quando si modificano i gruppi di sicurezza associati a un target di montaggio, è necessario assicurarsi di autorizzare l'accesso in entrata e in uscita. In questo modo l'istanza EC2 potrà comunicare con il file system.

Per ulteriori informazioni sui gruppi di sicurezza, consulta Gruppi di sicurezza Amazon EC2 nella Guida per l'utente di Amazon EC2 per istanze Linux.

Per modificare il gruppo di sicurezza di un target di montaggio utilizzando il AWS Management Console, vedereGestione dei target di montaggio utilizzando la console di Amazon EFS.

Per modificare il gruppo di sicurezza di un target di montaggio utilizzando il AWS CLI, vedereGestione dei target di montaggio utilizzando AWS CLI.

# Gestione della velocità di trasmissione effettiva del file system

Elastic è la modalità di throughput predefinita ed è consigliata per la maggior parte dei casi d'uso. Il Throughput Elastic aumenta o riduce automaticamente le prestazioni di throughput per soddisfare le esigenze dell'attività del carico di lavoro. Se, tuttavia, conosci i modelli di accesso specifici per i tuoi carichi di lavoro (incluse velocità di trasmissione effettiva, latenza e esigenze di archiviazione), puoi scegliere di modificare la modalità di throughput.

Le altre modalità di throughput che puoi scegliere includono:

- Throughput con provisioning: è possibile specificare un livello di throughput che il file system è in grado di gestire indipendentemente dalle dimensioni del file system o dal saldo del credito burst.
- Throughput di bursting: il throughput varia in base alla quantità di storage presente nel file system e supporta il bursting a livelli superiori per un massimo di 12 ore al giorno.

Per ulteriori informazioni sulle modalità di throughput di Amazon EFS, consultaModalità di velocità di trasmissione effettiva.

> **Note**
>
> È possibile modificare la modalità di throughput e la quantità di throughput assegnata dopo che il file system è disponibile. Tuttavia, ogni volta che si passa al file system in modalità di throughput assegnato o si aumenta la quantità di throughput assegnata, è necessario attendere almeno 24 ore prima di poter modificare nuovamente la modalità di throughput o ridurre la quantità di throughput assegnata.

Puoi gestire la modalità di throughput del file system utilizzando la console Amazon EFS, AWS Command Line Interface (AWS CLI) e l'API Amazon EFS.

Gestione della velocità di trasmissione effettiva del file system (console)

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Nel riquadro di navigazione a sinistra, scegli File system per visualizzare l'elenco dei file system EFS presenti nel tuo account.
3. Scegli il file system per cui desideri modificare la modalità di throughput.

4. Nella pagina dei dettagli del file system, nella sezione Generale, scegli Modifica. Viene visualizzata la pagina Modifica.
5. Modifica l'impostazione della Modalità di throughput.

   - Per utilizzare il Throughput Elastic o Con provisioning, scegli Migliorato, quindi scegli Elastic o Con provisioning.

     Se scegli Provisioned, quindi, in Provisioned Throughput (MiB/s), inserisci la quantità di throughput da fornire per le richieste del file system. La quantità di Velocità di trasmissione effettiva massima in lettura compare a tre volte la quantità di velocità di trasmissione effettiva inserita. I file system EFS misurano le richieste di lettura a una velocità di un terzo rispetto alle altre richieste. Dopo aver inserito il throughput, viene mostrata una stima del costo mensile per il file system.

     > **Note**
     >
     > È possibile modificare la modalità di throughput e la quantità di throughput assegnata dopo che il file system è disponibile. Tuttavia, ogni volta che si modifica la velocità effettiva del file system in Provisioned o si aumenta la quantità di throughput assegnata, è necessario attendere almeno 24 ore prima di poter modificare nuovamente la modalità di throughput o diminuire la quantità assegnata.

   - Per utilizzare la velocità di trasmissione effettiva di Bursting, scegli Bursting.

   Per ulteriori informazioni sulla scelta della modalità di throughput corretta per le tue esigenze di prestazioni, consulta Modalità di velocità di trasmissione effettiva.
6. Per implementare le modifiche, scegli Salva modifiche.

Gestione della velocità di trasmissione effettiva del file system (CLI)

- Utilizza il comando update-file-systemCLI o l'azione UpdateFileSystem API per modificare la modalità di throughput di un file system.

# Gestione dello storage del file system

Per gestire i file system in modo che vengano archiviati in modo conveniente per tutto il loro ciclo di vita, utilizza la gestione del ciclo di vita che trasferisce automaticamente i dati tra le classi di storage

in base alla configurazione del ciclo di vita definita per il file system. La configurazione del ciclo di vita è un insieme di policy del ciclo di vita che definiscono quando trasferire i dati del file system a un'altra classe di storage.

## Policy del ciclo di vita

Le policy del ciclo di vita indicano alla gestione del ciclo di vita quando trasferire i file da e verso le classi di storage EFS Infrequent Access (IA) ed EFS Archive. Il tempo di transizione si basa sull'ultimo accesso ai file nella classe di storage Standard. Le policy del ciclo di vita si applicano all'intero file system EFS.

Le policy del ciclo di vita EFS sono:

- Transizione a IA: indica alla gestione del ciclo di vita quando spostare i file nello storage Infrequent Access, che è ottimizzato in termini di costi per i dati a cui si accede solo poche volte al trimestre. Per impostazione predefinita, i file a cui non si accede nello storage Standard per 30 giorni vengono trasferiti in IA.
- Transizione all'archiviazione: indica alla gestione del ciclo di vita quando spostare i file nella classe di storage Archive, che è ottimizzata in termini di costi per i dati a cui si accede solo poche volte all'anno o meno. Per impostazione predefinita, i file a cui non si accede nello storage Standard per 90 giorni vengono trasferiti in archivio.
- Transizione allo standard: indica alla gestione del ciclo di vita se trasferire i file da IA o Archive allo storage Standard, che fornisce latenze di lettura inferiori al millisecondo per i dati a cui si accede di frequente. Per impostazione predefinita, i file non vengono spostati nuovamente nello storage Standard e rimangono nella classe di storage IA o archivio. Per i casi d'uso sensibili alle prestazioni che richiedono le prestazioni di latenza più elevate (ad esempio applicazioni che funzionano con un grande volume di file di piccole dimensioni), scegli di trasferire i file nello storage Standard Al primo accesso.

Per ulteriori informazioni sulla configurazione delle policy del ciclo di vita per un file system, consulta Gestione delle policy del ciclo di vita per un file system.

Per determinare l'ora dell'ultimo accesso nella classe di archiviazione Standard, un timer interno tiene traccia dell'ultimo accesso a un file (non gli attributi del file system POSIX che sono visualizzabili pubblicamente). Ogni volta che si accede a un file in Standard, il timer di gestione del ciclo di vita viene reimpostato. Dopo che la gestione del ciclo di vita ha spostato un file nelle classi di storage IA o Archive, il file rimane lì a tempo indeterminato, a meno che non venga impostata la policy Transition

to Standard, che impone alla gestione del ciclo di vita di riportare i file alla versione Standard al momento dell'accesso.

Le operazioni sui metadati, ad esempio la creazione di un elenco di contenuti di una directory, non contano come accesso ai file. Durante il processo di transizione dei contenuti di un file allo storage IA o archivio, il file viene memorizzato nella classe di storage Standard e fatturato alla tariffa di storage Standard.

## Operazioni del file system per la gestione del ciclo di vita

Le operazioni del file system per la gestione del ciclo di vita hanno una priorità inferiore rispetto alle operazioni per i carichi di lavoro dei file system EFS. Il tempo necessario per il trasferimento dei file alla classe di storage IA e archivio varia in base alle dimensioni del file e ai carichi di lavoro dei file system.

I metadati del file, tra cui i nomi del file, le informazioni di proprietà e la struttura della directory del file system, sono sempre archiviati nello storage Standard per assicurare prestazioni coerenti dei metadati. Tutte le operazioni di scrittura sui file nelle classi di storage IA o archivio del file system vengono prima scritte nelle classi di storage Standard e possono quindi essere trasferite alla classe di storage applicabile dopo 24 ore.

## Gestione delle policy del ciclo di vita per un file system

Quando crei un file system Amazon EFS che utilizza le impostazioni consigliate del servizio utilizzando AWS Management Console, le politiche del ciclo di vita del file system utilizzano le seguenti impostazioni predefinite:

- Transizione a IA è impostato su 30 giorni dall'ultimo accesso.
- Transizione all’archivio è impostato su 90 giorni dall'ultimo accesso.
- Transizione a standard è impostato su Nessuno.

Per ulteriori informazioni sulla creazione di un file system con le impostazioni consigliate dal servizio, consulta Fase 1: Creazione di un file system Amazon EFS.

È possibile configurare le policy del ciclo di vita dopo la creazione del file system o durante la creazione di un file system con impostazioni personalizzate.

I valori possibili per le policy del ciclo di vita di Transizione a IA e Transizione all’archivio includono:

- Nessuno
- 1 giorno dall'ultimo accesso
- 7 giorni dall'ultimo accesso
- 14 giorni dall'ultimo accesso
- 30 giorni dall'ultimo accesso
- 60 giorni dall'ultimo accesso
- 90 giorni dall'ultimo accesso
- 180 giorni dall'ultimo accesso
- 270 giorni dall'ultimo accesso
- 365 giorni dall'ultimo accesso

I valori possibili per la policy del ciclo di vita di Transizione a standard includono:

- Nessuno
- Al primo accesso

Puoi configurare le politiche del ciclo di vita utilizzando AWS Management Console and AWS CLI, come descritto nelle seguenti procedure.

Gestione delle policy relative al ciclo di vita su un file system esistente (console)

È possibile utilizzare il AWS Management Console per impostare le politiche del ciclo di vita per un file system esistente.

1. Accedi AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Scegli File system per visualizzare l'elenco dei file system presenti nel tuo account.
3. Scegli il file system su cui desideri modificare le policy del ciclo di vita.
4. Nella pagina dei dettagli del file system, nella sezione Generale, scegli Modifica. Viene visualizzata la pagina Modifica.
5. Per la gestione del ciclo di vita, è possibile modificare le seguenti policy del ciclo di vita:

    - Imposta Transizione a IA su una delle impostazioni disponibili. Per interrompere lo spostamento dei file nello storage IA, scegli Nessuno.

- Imposta Transizione all'archivio su una delle impostazioni disponibili. Per interrompere lo spostamento dei file nello storage di archivio, scegli Nessuno.
- Imposta Transizione a standard su Al primo accesso per spostare i file che si trovano nello storage IA nello storage standard quando vi si accede per operazioni senza metadati.

  Per interrompere lo spostamento dei file da IA o archivio allo storage Standard al primo accesso, imposta Nessuno.

6. Per salvare le modifiche, scegli Salva modifiche.

Gestione delle policy relative al ciclo di vita su un file system esistente (CLI)

Puoi utilizzarlo AWS CLI per impostare o modificare le politiche del ciclo di vita di un file system.

- Esegui il `put-lifecycle-configuration` AWS CLI comando o il comando PutLifecycleConfiguration API, specificando l'ID del file system per il quale gestisci la gestione del ciclo di vita.

```
$  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
```

  Si ottiene la risposta seguente.

```
{
    "LifecyclePolicies": [
        {
            "TransitionToIA": "AFTER_60_DAYS"
        },
        {
            "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        },
        {
            "TransitionToArchive": "AFTER_90_DAYS"
        }
    ]
```

```
}
```

Arresto della gestione del ciclo di vita per un file system esistente (CLI)

- Esegui il comando `put-lifecycle-configuration` specificando l'ID del file system per il quale si desidera arrestare la gestione del ciclo di vita. Mantieni la proprietà `--lifecycle-policies` vuota.

```
$  aws efs put-lifecycle-configuration \
--file-system-id File-System-ID \
--lifecycle-policies \
--region us-west-2 \
--profile adminuser
```

Si ottiene la risposta seguente.

```
{
    "LifecyclePolicies": []
}
```

## Gestione dell'accesso ai file system crittografati

Utilizzando Amazon EFS, è possibile creare file system crittografati. Amazon EFS supporta due forme di crittografia per i file system, la crittografia dei dati in transito e la crittografia dei dati memorizzati su disco. Qualsiasi gestione delle chiavi richiesta è esclusivamente legata alla crittografia dei dati inattivi. Amazon EFS gestisce automaticamente le chiavi per la crittografia dei dati in transito.

Se si crea un file system che utilizza la crittografia dei dati memorizzati su disco, i dati e i metadati sono crittografati in locale. Amazon EFS utilizza AWS Key Management Service (AWS KMS) per la gestione delle chiavi. Quando si crea un file system utilizzando la crittografia dei dati inattivi, è necessario specificare AWS KMS key. La chiave KMS può essere `aws/elasticfilesystem` (quella Chiave gestita da AWS per Amazon EFS) o può essere una chiave gestita dal cliente che gestisci tu.

I dati dei file (i contenuti degli stessi) vengono crittografati utilizzando la chiave KMS specificata durante la creazione del file system. I metadati (nomi di file, nomi e contenuti delle directory) sono crittografati mediante una chiave gestita da Amazon EFS.

L'EFS Chiave gestita da AWS per il file system viene utilizzato come chiave KMS per crittografare i metadati nel file system, ad esempio nomi di file, nomi di directory e contenuti delle directory. L'utente è in possesso della chiave gestita dal cliente utilizzata per crittografare i dati dei file (i contenuti dei file) inattivi.

L'utente può gestire gli accessi alle chiavi KMS e ai contenuti dei file system crittografati. Questo accesso è controllato da entrambe le policy AWS Identity and Access Management (IAM) e. AWS KMS Le policy IAM controllano l'accesso di un utente alle azioni dell'API Amazon EFS. AWS KMS le politiche chiave controllano l'accesso di un utente alla chiave KMS specificata al momento della creazione del file system. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Utenti IAM nella Guida per l'utente IAM
- Utilizzo delle policy chiave AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service
- Utilizzo delle concessioni nella Guida per gli sviluppatori di AWS Key Management Service .

In qualità di amministratore di chiavi, puoi importare le chiavi esterne. Puoi anche modificare le chiavi abilitandole, disabilitandole o eliminandole. Lo stato della chiave KMS specificata (al momento della creazione del file system con crittografia dei dati memorizzati su disco) ha effetto sull'accesso ai relativi contenuti. La chiave KMS deve essere nello `enabled` stato in cui gli utenti possano accedere ai contenuti di un encrypted-at-rest file system crittografato utilizzando tale chiave.

## Esecuzione di operazioni di amministrazione nelle chiavi KMS di Amazon EFS

Di seguito, è possibile scoprire come abilitare, disabilitare o eliminare le chiavi KMS associate al file system Amazon EFS. È inoltre possibile scoprire di più su quale è il comportamento atteso del file system all'esecuzione di queste operazioni.

### Disabilitazione, eliminazione o revoca dell'accesso alla chiave KMS di un file system

È possibile disabilitare o eliminare le chiavi KMS gestite dal cliente oppure è possibile revocare l'accesso di Amazon EFS alle proprie chiavi KMS. La disabilitazione e la revoca delle autorizzazioni

di accesso alle chiavi da parte di Amazon EFS sono operazioni reversibili. Presta molta attenzione all'eliminazione delle chiavi KMS. L'eliminazione di una chiave KMS è un'operazione irreversibile.

Se si disabilita o si elimina la chiave KMS utilizzata per un file system montato, si verificano le seguenti conseguenze:

- Quella chiave KMS non può essere utilizzata come chiave per nuovi encrypted-at-rest file system.
- I encrypted-at-rest file system esistenti che utilizzano quella chiave KMS smettono di funzionare dopo un certo periodo di tempo.

Se si revoca l'accesso di Amazon EFS all'autorizzazione su un file system montato esistente, il comportamento è analogo a quello in caso di disabilitazione o eliminazione della chiave KMS associata. In altre parole, il encrypted-at-rest file system continua a funzionare, ma smette di funzionare dopo un certo periodo di tempo.

Puoi impedire l'accesso a un encrypted-at-rest file system montato con una chiave KMS a cui hai disabilitato, eliminato o revocato l'accesso ad Amazon EFS. Per eseguire questa operazione, disinstalla il file system ed elimina i target di montaggio Amazon EFS.

Non puoi eliminarlo immediatamente AWS KMS key, ma puoi pianificarne l'eliminazione in 7-30 giorni. Se una chiave KMS è pianificata per l'eliminazione, non è possibile utilizzarla per operazioni di crittografia. È anche possibile annullare la pianificazione dell'eliminazione della chiave KMS.

Per ulteriori informazioni su come disabilitare e riabilitare le chiavi KMS gestite dal cliente, consulta Abilitazione e disabilitazione delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service . Per informazioni su come pianificare l'eliminazione delle chiavi KMS gestite dal cliente, consulta Eliminazione delle chiavi KMS nella Guida per gli sviluppatori di AWS Key Management Service .

## Argomenti correlati

- Per ulteriori informazioni sui dati e metadati memorizzati su disco crittografati in Amazon EFS, consulta Crittografia dei dati in Amazon EFS.
- Per esempi di policy delle chiavi, consulta Politiche chiave di Amazon EFS per AWS KMS.
- Per un elenco delle voci di AWS CloudTrail registro associate a un file system crittografato, vedereVoci dei file di log di Amazon encrypted-at-rest EFS per i file system.

- Per ulteriori informazioni sulla definizione di quali account e servizi hanno accesso alle chiavi KMS, consulta Determinazione dell'accesso a AWS KMS key nella Guida per gli sviluppatori di AWS Key Management Service .

# Misurazione: come Amazon EFS calcola le dimensioni di file system e oggetti

Le seguenti sezioni descrivono come Amazon EFS riporta le dimensioni del file system e le dimensioni degli oggetti all'interno di un file system.

## Misurazione degli oggetti di un file system Amazon EFS

Gli oggetti che è possibile visualizzare in un sistema Amazon EFS comprendono file normali, directory, collegamenti simbolici e file speciali (FIFO e socket). Ognuno di questi oggetti è misurato partendo da 2 kibibytes (KiB) di metadati (per i suoi inode) e uno o più incrementi di 4 KiB di dati. L'elenco seguente illustra le dimensioni misurate dei dati per diversi tipi di oggetti del file system:

- File normali - La dimensione calcolata di un file normale è la dimensione logica del file arrotondata al successivo incremento di 4 KiB, anche se può essere inferiore per file sparsi.

  Un file sparse è un file nel quale i dati non vengono scritti in tutte le posizioni del file prima del raggiungimento della sua dimensione logica. Per un file sparse, in alcuni casi lo storage effettivo utilizzato è inferiore alla dimensione logica arrotondata al successivo incremento di 4 KiB. In questi casi, Amazon EFS segnala lo storage effettivo utilizzato come dimensione misurata dei dati.
- Directory - La dimensione calcolata di una directory è lo spazio di memorizzazione effettivamente utilizzato per le voci della cartella e la struttura di dati che le contiene, arrotondata al successivo incremento di 4 KiB. La dimensione calcolata dei dati non tiene conto dello spazio di memorizzazione effettivamente utilizzato dai file di dati.
- Collegamenti simbolici e file speciali - La dimensione calcolata di questi oggetti è sempre 4 KiB.

Quando Amazon EFS indica lo spazio utilizzato da un oggetto, tramite l'attributo NFSv4.1 `space_used`, questo include la dimensione calcolata attuale dei dati dell'oggetto, ma non quella dei suoi metadati. È possibile utilizzare due utilità per misurare l'utilizzo del disco di un file, l'utilità du e `stat`. Di seguito è riportato un esempio di come utilizzare l'duutilità su un file vuoto che include l'`-k`opzione per restituire l'output in kilobyte.

```
$ du -k file
4       file
```

L'esempio seguente mostra come utilizzare l'`stat`utilità su un file vuoto per restituire l'utilizzo del disco del file.

```
$ /usr/bin/stat --format="%b*%B" file | bc
4096
```

Per misurare le dimensioni di una directory, utilizzare l'utilità `stat`. Trovare il valore `Blocks` e moltiplicare tale valore per la dimensione del blocco. Segue un esempio di come utilizzare l'utilità `stat` in una directory vuota:

```
$ /usr/bin/stat --format="%b*%B" . | bc
4096
```

## Dimensioni misurate di un file system Amazon EFS

La dimensione misurata di un file system Amazon EFS include la somma delle dimensioni di tutti gli oggetti correnti in tutte le classi di storage EFS. La dimensione di ogni oggetto viene calcolata a partire da un campionamento rappresentativo della dimensione dell'oggetto durante l'ora di misurazione, ad esempio l'ora dalle 8.00 alle 9:00 di mattina.

Un file vuoto contribuisce per 6 KiB (2 KiB di metadati+4 KiB di dati) alla dimensione calcolata della dimensione del suo file system. Al momento della creazione, un file system presenta una singola cartelle principale e quindi restituisce una dimensione misurata di 6 KiB.

La dimensione misurata di uno specifico file system definisce l'utilizzo per il quale il proprietario dell'account viene tariffato per quel file system per quell'ora.

> **Note**
>
> La dimensione misurata non rappresenta uno snapshot coerente del file system in nessuno dei momenti che compongono tale ora. Il documento rappresenta le dimensioni degli oggetti esistenti nel file system in diversi momenti all'interno della stessa ora oppure dell'ora precedente. Tali dimensioni vengono sommate per determinare la dimensione del file system misurata per l'ora. La dimensione misurata di un file system risulta quindi alla fine coerente

con le dimensioni degli oggetti memorizzati al suo interno quando non ci sono operazioni di scrittura sul file system.

Puoi visualizzare la dimensione misurata per un file system Amazon EFS nei seguenti modi:

- Utilizzando il describe-file-systems AWS CLI comando e l'operazione DescribeFileSystemAPI, la risposta include quanto segue:

```
"SizeInBytes":{
            "Timestamp": 1403301078,
            "Value": 29313744866,
            "ValueInIA": 675432,
            "ValueInStandard": 29312741784
            "ValueInArchive": 327650
         }
```

  Dove la dimensione misurata di `ValueInStandard` viene utilizzata anche per determinare la linea di base del throughput di I/O e le frequenze di burst per i file system che utilizzano la modalità Bursting Throughput.

- Visualizza la `StorageBytes` CloudWatch metrica, che mostra la dimensione totale misurata dei dati in ciascuna classe di storage. Per ulteriori informazioni sul parametro `StorageBytes`, consulta CloudWatch Parametri Amazon per Amazon EFS.
- Esegui il comando `df` in Linux al prompt del terminale di un'istanza EC2.

  Non utilizzare il du comando nella directory principale del file system per scopi di misurazione dello storage, poiché la risposta non riflette l'intero set di dati utilizzato per misurare il file system.

> **Note**
>
> La dimensione misurata di `ValueInStandard` è utilizzata anche per determinare il throughput di I/O di base e le velocità di picco. Per ulteriori informazioni, consulta Velocità effettiva di espansione.

### Misurazione delle classi di storage Infrequent Access e Archive

Le classi di storage EFS Infrequent Access (IA) e Archive vengono misurate in incrementi di 4 KiB e hanno un costo di fatturazione minimo per file di 128 KiB. I metadati dei file IA e Archive (2 KB per file) vengono sempre archiviati e misurati nella classe di archiviazione Standard. Il supporto per file di dimensioni inferiori a 128 KiB è disponibile solo per le politiche relative al ciclo di vita aggiornate a partire dalle 12:00 PT del 26 novembre 2023. L'accesso ai dati per lo storage IA e Archive viene misurato in incrementi di 128 KB.

È possibile utilizzare la `StorageBytes` CloudWatch metrica per visualizzare la dimensione misurata dei dati in ciascuna delle classi di archiviazione. La metrica mostra anche il numero totale di byte utilizzati dall'arrotondamento di file di piccole dimensioni all'interno delle classi di archiviazione IA e Archive. Per ulteriori informazioni sulla visualizzazione delle metriche, consulta. CloudWatch Accesso alle CloudWatch metriche Per ulteriori informazioni sul parametro `StorageBytes`, consulta CloudWatch Parametri Amazon per Amazon EFS.

## Misurazione della velocità di trasmissione effettiva

Amazon EFS misura il throughput per le richieste di lettura a un terzo della velocità delle altre operazioni di I/O del file system. Ad esempio, se si utilizzano 30 mebibyte al secondo (MiBps) di velocità di lettura e scrittura, la parte di lettura conta come il 10% MiBps della velocità effettiva, la parte di scrittura conta 30 MiBps e la velocità effettiva misurata combinata è 40. MiBps Questo throughput combinato adeguato ai tassi di consumo si riflette nella metrica. `MeteredIOBytes` CloudWatch

### Misurazione della produttività elastica

Quando la modalità Elastic Throughput è abilitata per un file system, paghi solo per la quantità di metadati e dati letti o scritti sul file system. I file system Amazon EFS che utilizzano la modalità Elastic Throughput Mode, i metadati dei contatori e delle fatture vengono letti come operazioni di lettura e le scritture dei metadati come operazioni di scrittura. Le operazioni sui metadati vengono misurate con incrementi di 4 KiB e le operazioni sui dati vengono misurate con incrementi di 32 KiB.

### Misurazione della velocità di trasmissione effettiva con provisioning

Per i file system che utilizzano la modalità di throughput Provisioned, si paga solo per il periodo di tempo in cui il throughput è abilitato. Amazon EFS contabilizza i file system con la modalità di throughput Provisioned abilitata una volta all'ora. Per la misurazione quando la modalità di throughput

Provisioned è impostata per meno di un'ora, Amazon EFS calcola la media temporale con una precisione al millisecondo.

# Gestione dei costi del file system Amazon EFS utilizzandoAWSBudget

Puoi pianificare e gestire i costi del file system Amazon EFS utilizzandoAWSBudget.

Puoi utilizzare AWS Budgets dalla console AWS Billing and Cost Management. Per utilizzare AWS Budgets, puoi creare un budget dei costi mensili per i file system EFS. Puoi impostare il tuo budget se prevedi che i costi superino l'importo previsto e puoi quindi apportare rettifiche per mantenere il budget nei limiti desiderati.

Vi sono dei costi associati all'utilizzoAWSBudget. Per normaliAccount AWS, i primi due budget sono gratuiti Per ulteriori informazioni suAWSBudget, inclusi i costi, vediGestione dei costi con AWS BudgetsnellaAWS BillingGuida per l'utente di.

Puoi impostare budget personalizzati per i costi Amazon EFS e l'utilizzo sul conto,Regione AWSlivello di servizio o tag utilizzando i parametri di budget. Nella sezione seguente puoi trovare una descrizione di alto livello su come impostare un budget dei costi in un file system EFS con AWS Budgets. Puoi farlo utilizzando i tag di allocazione dei costi.

## Prerequisiti

Per eseguire le procedure a cui si fa riferimento nelle sezioni seguenti, assicurati di disporre di quanto segue:

- Un file system EFS
- Una policy AWS Identity and Access Management (IAM) con le seguenti autorizzazioni:
  - Accesso alla console AWS Billing and Cost Management.
  - Capacità di eseguire le operazioni `elasticfilesystem:CreateTags` e `elasticfilesystem:DescribeTags`.

## Creazione di un budget dei costi mensili per un file system EFS

La creazione di un budget dei costi mensili per il file system Amazon EFS utilizzando i tag è un processo che si articola in tre fasi.

Per creare un budget dei costi mensili per il file system EFS utilizzando i tag

1. Crea un tag da utilizzare per identificare il file system per il quale desideri monitorare i costi. Per scoprire come fare, consultare Aggiunta di tag alle risorse Amazon ECS.
2. Nella console di Billing and Cost Management, attiva il tag come tag di allocazione dei costi. Per una procedura dettagliata, consultaAttivazione dei tag di allocazione dei costi definiti dall'utentenellaAWS BillingGuida per l'utente di.
3. Nella console di Billing and Cost Management, inBudget, crea un budget dei costi mensili inAWSBudget. Per una procedura dettagliata, consultaCreazione di un budget dei costinellaAWS BillingGuida per l'utente di.

Dopo aver creato il budget dei costi mensili di EFS, puoi visualizzarlo nella pannello Budgets che visualizza i seguenti dati del budget:

- I costi e l'utilizzo già accumulati per un budget durante il periodo di budget
- I costi a budget per il periodo di budget.
- I costi previsti per il periodo di budget.
- Una percentuale che mostra i costi rispetto all'importo a budget
- Una percentuale che mostra i costi previsti rispetto all'importo a budget

Per ulteriori informazioni sulla visualizzazione del budget dei costi di EFS, consultaVisualizzazione dei tuoi budgetnellaAWS BillingGuida per l'utente di.

## Stato del file system

Puoi visualizzare lo stato dei file system Amazon EFS utilizzando la console Amazon EFS o AWS CLI. Un file system Amazon EFS può avere uno dei valori di stato descritti nella tabella seguente.

| Stato del file system | Descrizione |
| --- | --- |
| DISPONIBILE | Il file system è integro, raggiungibile e disponibile per l'uso. |
| CREAZIONE IN CORSO | Amazon EFS sta creando il nuovo file system. |

| Stato del file system | Descrizione |
| --- | --- |
| ELIMINAZIONE IN CORSO | Amazon EFS sta eliminando il file system in risposta a una richiesta di eliminazione avviata dall'utente. Per ulteriori informazioni, consulta Cancellazione di un file system Amazon EFS. |
| ELIMINATO | Amazon EFS ha eliminato il file system in risposta a una richiesta di eliminazione avviata dall'utente. Per ulteriori informazioni, consulta Cancellazione di un file system Amazon EFS. |
| AGGIORNAMENTO IN CORSO | Il file system è in fase di aggiornamento in risposta a una richiesta di aggiornamento avviata dall'utente. |
| ERRORE | Applicabile ai file system a zona singola, inclusi i file system in una configurazione di replica.<br><br>Il file system si trova in uno stato di errore ed è irreversibile. Per accedere ai dati del file system, ripristina un backup del file system non riuscito su un nuovo file system. Per ulteriori informazioni, consultare:<br><br>• Recupero di un punto di ripristino.<br>• Classi di storage EFS<br>• Replica dei file system |

# Monitoraggio di Amazon EFS

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon EFS e delle tue AWS soluzioni. Ti consigliamo di raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. Prima di iniziare il monitoraggio di Amazon EFS è tuttavia opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

La fase successiva consiste nello stabilire una baseline per le prestazioni normali di Amazon EFS nell'ambiente, misurando le prestazioni in diversi momenti e con condizioni di carico differenti. Quando esegui il monitoraggio di Amazon EFS, prendi in considerazione l'archiviazione dei dati storici sul monitoraggio. Questi dati archiviati forniranno una baseline rispetto ai quali confrontare i dati sulle prestazioni correnti e identificare i normali modelli o le anomalie di prestazioni e ideare metodi per risolvere i problemi.

Ad esempio, con Amazon EFS, è possibile monitorare il throughput della rete, il volume di I/O per le operazioni di scrittura, lettura e/o i metadati, le connessioni dei client e i saldi dei crediti di burst per i file system. Quando le prestazioni non rientrano all'interno della baseline stabilita, potrebbe essere necessario modificare le dimensioni del file system o il numero di client collegati per ottimizzare il file system rispetto al carico di lavoro.

Per stabilire una baseline, devi monitorare almeno gli elementi seguenti:

- Il throughput di rete dei file system.
- Numero di connessioni client a un file system.
- Il numero di byte per ciascuna operazione del file system, tra cui la lettura e la scrittura di dati oltre alle operazioni di metadati.

# Strumenti di monitoraggio

AWS fornisce diversi strumenti che puoi utilizzare per monitorare Amazon EFS. Alcuni di questi strumenti possono essere configurati in modo che eseguano automaticamente il monitoraggio, mentre altri richiedono l'intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

## Strumenti di monitoraggio automatici

Per controllare Amazon EFS e segnalare l'eventuale presenza di problemi, puoi usare i seguenti strumenti di monitoraggio automatici:

- Amazon CloudWatch Alarms: monitora una singola metrica in un periodo di tempo specificato ed esegui una o più azioni in base al valore della metrica rispetto a una determinata soglia in diversi periodi di tempo. L'azione è una notifica inviata a un argomento di Amazon Simple Notification Service (Amazon SNS) o a una policy di Amazon EC2 Auto Scaling. CloudWatch gli allarmi non richiamano azioni solo perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per ulteriori informazioni, consulta Monitoraggio di Amazon EFS con Amazon CloudWatch.
- Amazon CloudWatch Logs: monitora, archivia e accedi ai tuoi file di registro da AWS CloudTrail o altre fonti. Per ulteriori informazioni, consulta Monitoring Log Files nella Amazon CloudWatch User Guide.
- Amazon CloudWatch Events: abbina gli eventi e li indirizza a una o più funzioni o stream di destinazione per apportare modifiche, acquisire informazioni sullo stato e intraprendere azioni correttive. Per ulteriori informazioni, consulta What is Amazon CloudWatch Events nella Amazon CloudWatch User Guide.
- AWS CloudTrail Monitoraggio dei log: condividi i file di CloudTrail registro tra account, monitora i file di registro in tempo reale inviandoli a CloudWatch Logs, scrivi applicazioni di elaborazione dei log in Java e verifica che i file di registro non siano cambiati dopo la consegna da parte di. CloudTrail Per ulteriori informazioni, consulta Lavorare con i file di CloudTrail registro nella Guida per l'AWS CloudTrail utente.

## Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio di Amazon EFS riguarda il monitoraggio manuale degli elementi non coperti dagli CloudWatch allarmi di Amazon. Amazon EFS e altri AWS Management

Console pannelli di controllo forniscono una at-a-glance panoramica dello stato del tuo AWS ambiente. CloudWatch Ti consigliamo anche di controllare i file di log nel file system.

- Dalla console Amazon EFS è possibile verificare le seguenti voci associate ai file system:
  - L'attuale dimensione misurata
  - Il numero di target di montaggio
  - Lo stato del ciclo di vita
- CloudWatch la home page mostra:
  - Stato e allarmi attuali
  - Grafici degli allarmi e delle risorse
  - Stato di integrità dei servizi

  Inoltre, è possibile utilizzare CloudWatch per effettuare le seguenti operazioni:
  - Creare pannelli di controllo personalizzati per monitorare i servizi utilizzati.
  - Crea grafici dei dati dei parametri per la risoluzione di problemi e il rilevamento di tendenze.
  - Cerca e sfoglia tutte le metriche AWS delle tue risorse.
  - Crea e modifica gli allarmi per ricevere le notifiche dei problemi.

# Monitoraggio di Amazon EFS con Amazon CloudWatch

Puoi monitorare i file system utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi da Amazon EFS in metriche leggibili quasi in tempo reale. Queste statistiche vengono registrate per un periodo di 15 mesi, per offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web.

Per impostazione predefinita, i dati dei parametri di Amazon EFS vengono inviati automaticamente CloudWatch a periodi di 1 minuto, a meno che non sia indicato per alcuni parametri individuali. La console Amazon EFS mostra una serie di grafici basati sui dati grezzi di Amazon CloudWatch. A seconda delle tue esigenze, potresti preferire ottenere i dati per i tuoi file system CloudWatch anziché dai grafici nella console.

Per ulteriori informazioni su Amazon CloudWatch, consulta la Amazon CloudWatch User Guide.

Argomenti

- CloudWatch Parametri Amazon per Amazon EFS

- Come si utilizzano i parametri di Amazon EFS?
- Utilizzo della matematica dei parametri con Amazon EFS
- Monitoraggio dello stato di successo o di fallimento del tentativo di montaggio
- Accesso alle CloudWatch metriche
- Creazione di CloudWatch allarmi per monitorare Amazon EFS

## CloudWatch Parametri Amazon per Amazon EFS

I parametri Amazon EFS utilizzano lo spazio dei nomi `EFS` e forniscono parametri per la singola dimensione `FileSystemId`. Un ID del file system è disponibile nella console di gestione Amazon EFS e assume la forma di `fs-abcdef0123456789a`.

Lo spazio dei nomi `AWS/EFS` include i parametri descritti di seguito.

**`TimeSinceLastSync`**

Mostra la quantità di tempo trascorso dall'ultima sincronizzazione riuscita con il file system di destinazione in una configurazione di replica. Tutte le modifiche ai dati sul file system di origine apportate prima di `TimeSinceLastSync` sono state replicate correttamente. Qualsiasi modifica all'origine apportata dopo `TimeSinceLastSync` potrebbe non essere replicata completamente.

Unità: secondi

Statistiche valide: `Minimum`, `Maximum`, `Average`

**`PercentIOLimit`**

Mostra quanto manca a un file system per raggiungere il limite di I/O della modalità prestazioni Per scopi generici.

Unità: percentuale

Statistiche valide: `Minimum`, `Maximum`, `Average`

**`BurstCreditBalance`**

Numero di crediti di burst di cui dispone un file system. I crediti di burst consentono al file system di raggiungere livelli di throughput superiori a un livello base del file system per determinati periodi di tempo.

La statistica `Minimum` è il saldo dei crediti di burst più piccolo per qualsiasi minuto durante il periodo. La statistica `Maximum` è il saldo dei crediti di burst più grande per qualsiasi minuto durante il periodo. La statistica `Average` è il saldo dei crediti di burst medio durante il periodo.

Unità: byte

Statistiche valide: `Minimum`, `Maximum`, `Average`

**`PermittedThroughput`**

La quantità massima di throughput consentita a un file system.

- Per i file system che utilizzano la velocità effettiva elastica, questo valore riflette la velocità massima di scrittura del file system.
- Per i file system che utilizzano il throughput Provisioned, se la quantità di dati archiviati nella classe di storage EFS Archive consente al file system di ottenere un throughput superiore a quello fornito, questa metrica riflette il throughput più elevato anziché la quantità assegnata.
- Per i file system in modalità Bursting Throughput, questo valore è una funzione della dimensione del file system e. `BurstCreditBalance`

La statistica `Minimum` è il throughput minimo consentito per qualsiasi minuto durante il periodo. La statistica `Maximum` è il throughput massimo consentito per qualsiasi minuto durante il periodo. La statistica `Average` è il throughput medio durante il periodo.

> **Note**
>
> Le operazioni di lettura vengono misurate a un terzo della velocità delle altre operazioni.

Unità: byte al secondo

Statistiche valide: `Minimum`, `Maximum`, `Average`

**`MeteredIOBytes`**

Il numero di byte misurati per ogni operazione del file system, incluse le operazioni di lettura, scrittura dei dati e metadati, con operazioni di lettura misurate a un terzo della frequenza delle altre operazioni.

È possibile creare un'espressione matematica CloudWatch metrica da confrontare con. `MeteredIOBytes` `PermittedThroughput` Se questi valori sono uguali, stai consumando

l'intera quantità di throughput allocata al tuo file system. In questa situazione, potreste prendere in considerazione la possibilità di modificare la modalità di trasmissione del file system per ottenere un throughput più elevato.

La statistica `Sum` è il numero totale di byte misurati associato a tutte le operazioni del file system. La statistica `Minimum` è la dimensione dell'operazione più piccola durante il periodo. La statistica `Maximum` è la dimensione dell'operazione più grande durante il periodo. La statistica `Average` è la dimensione media di un'operazione durante il periodo. La statistica `SampleCount` fornisce il numero di tutte le operazioni.

Unità:

- Byte per le statistiche `Minimum`, `Maximum`, `Average` e `Sum`.
- Conteggio per `SampleCount`.

Statistiche valide: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

**`TotalIOBytes`**

Il numero di byte per ciascuna operazione del file system, tra cui la lettura e la scrittura di dati, oltre alle operazioni di metadati. Si tratta della quantità effettiva generata dall'applicazione e non della velocità di trasmissione effettiva misurata dal file system. Potrebbe essere superiore alle cifre mostrate in `PermittedThroughput`.

La statistica `Sum` è il numero totale di byte associato a tutte le operazioni del file system. La statistica `Minimum` è la dimensione dell'operazione più piccola durante il periodo. La statistica `Maximum` è la dimensione dell'operazione più grande durante il periodo. La statistica `Average` è la dimensione media di un'operazione durante il periodo. La statistica `SampleCount` fornisce il numero di tutte le operazioni.

> **Note**
>
> Per calcolare le operazioni medie al secondo per un periodo, dividi la statistica `SampleCount` per il numero di secondi in quel periodo. Per calcolare il throughput medio (byte al secondo) per un periodo, dividi la statistica `Sum` per il numero di secondi in quel periodo.

Unità:

- Byte per le statistiche `Minimum`, `Maximum`, `Average` e `Sum`.

- Conteggio per `SampleCount`.

Statistiche valide: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

**`DataReadIOBytes`**

Numero di byte per ciascuna operazione di lettura del file system.

La statistica `Sum` è il numero totale di byte associato alle operazioni di lettura. La statistica `Minimum` è la dimensione dell'operazione di lettura più piccola durante il periodo. La statistica `Maximum` è la dimensione dell'operazione di lettura più grande durante il periodo. La statistica `Average` è la dimensione media delle operazioni di lettura durante il periodo. La statistica `SampleCount` fornisce il numero di operazioni di lettura.

Unità:

- Byte per `Minimum`, `Maximum`, `Average` e `Sum`.
- Conteggio per `SampleCount`.

Statistiche valide: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

**`DataWriteIOBytes`**

Numero di byte per ciascuna operazione di scrittura del file system.

La statistica `Sum` è il numero totale di byte associato alle operazioni di scrittura. La statistica `Minimum` è la dimensione dell'operazione di scrittura più piccola durante il periodo. La statistica `Maximum` è la dimensione dell'operazione di scrittura più grande durante il periodo. La statistica `Average` è la dimensione media delle operazioni di scrittura durante il periodo. La statistica `SampleCount` fornisce il numero di operazioni di scrittura.

Unità:

- I byte sono le unità per le statistiche `Minimum`, `Maximum`, `Average` e `Sum`.
- Conteggio per `SampleCount`.

Statistiche valide: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

**`MetadataIOBytes`**

Numero di byte per ciascuna operazione di metadati.

La statistica `Sum` è il numero totale di byte associato alle operazioni di metadati. La statistica `Minimum` è la dimensione dell'operazione di metadati più piccola durante il periodo. La statistica

`Maximum` è la dimensione dell'operazione di metadati più grande durante il periodo. La statistica `Average` è la dimensione dell'operazione di metadati media durante il periodo. La statistica `SampleCount` fornisce il numero di operazioni di metadati.

Unità:

- I byte sono le unità per le statistiche `Minimum`, `Maximum`, `Average` e `Sum`.
- Conteggio per `SampleCount`.

Statistiche valide: `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

**`ClientConnections`**

Numero di connessioni client a un file system. Quando si utilizza un client standard, è presente una connessione per istanza Amazon EC2 installata.

> **Note**
>
> Per calcolare la media di `ClientConnections` per periodi superiori a un minuto, dividi la statistica `Sum` per il numero di minuti in quel periodo.

Unità: numero di connessioni client

Statistiche valide: `Sum`

**`StorageBytes`**

La dimensione del file system in byte, inclusa la quantità di dati archiviati nelle classi di storage EFS. Questa metrica viene emessa ogni 15 minuti. CloudWatch

La `StorageBytes` metrica ha le seguenti dimensioni:

- `Total`è la dimensione misurata (in byte) dei dati memorizzati nel file system, in tutte le classi di archiviazione. Per le classi di storage EFS Infrequent Access ed EFS Archive, i file di dimensioni inferiori a 128 KiB vengono arrotondati a 128 KiB.
- `Standard`è la dimensione misurata (in byte) dei dati archiviati nella classe di storage EFS Standard.
- `IA`è la dimensione misurata (in byte) dei dati archiviati nella classe di storage EFS Infrequent Access.

- `IASizeOverhead`è la differenza (in byte) tra la dimensione effettiva dei dati nella classe di storage EFS Infrequent Access (indicata nella `IA` dimensione) e la quantità arrotondata a 128 KiB, se il file system è inferiore a 128 KiB.
- `Archive`è la dimensione misurata (in byte) dei dati nella classe di storage EFS Archive. Questo numero riflette la dimensione effettiva dei dati archiviati nello storage Archive, prima di arrotondare i file di piccole dimensioni a 128 KiB.
- `ArchiveSizeOverhead`è la differenza (in byte) tra la dimensione effettiva dei dati nella classe di storage EFS Archive (indicata nella `Archive` dimensione) e la quantità arrotondata a 128 KiB, se il file system è inferiore a 128 KiB.

Unità: byte

Statistiche valide: `Minimum`, `Maximum`, `Average`

> **Note**
>
> `StorageBytes` compare nella pagina delle Metriche del file system della console Amazon EFS utilizzando unità di base 1024 (kibibyte, mebibyte, gibibyte e tebibyte).

### Byte riportati in CloudWatch

Le CloudWatch metriche di Amazon EFS sono riportate come byte non elaborati. I byte non sono arrotondati a un multiplo decimale o binario dell'unità. Tenere presente questo aspetto quando si calcola la velocità di burst utilizzando i dati provenienti dalle misurazioni. Per ulteriori informazioni sul bursting, consulta Velocità effettiva di espansione.

## Come si utilizzano i parametri di Amazon EFS?

I parametri forniti da Amazon EFS offrono informazioni che possono essere analizzate in diversi modi. L'elenco seguente mostra alcuni usi comuni dei parametri. Questi suggerimenti sono solo introduttivi e non costituiscono un elenco completo.

| Come...? | Parametri rilevanti |
| --- | --- |
| Come posso determinare il throughput? | Per determinare il throughput, è possibile monitorare le statistiche `Sum` giornaliere del parametro `TotalIOBytes` . |

| Come...? | Parametri rilevanti |
| --- | --- |
| Come è possibile monitorare il numero di istanze Amazon EC2 connesse a un file system? | Basta monitorare la statistica `Sum` del parametro `ClientConnections` . Per calcolare la media di `ClientConnections` per periodi superiori a un minuto, dividere la somma per il numero di minuti nel periodo. |
| Come è possibile visualizzare il saldo dei crediti di burst? | È possibile visualizzare il saldo monitorando il parametro `BurstCreditBalance` associato al file system. Per ulteriori informazioni sul bursting e sui crediti di burst, consultare Velocità effettiva di espansione. |

## Utilizzo delle CloudWatch metriche per monitorare le prestazioni del throughput

Le CloudWatch metriche per il monitoraggio del throughput—`TotalIOBytes`, `ReadIOBytesWriteIOBytes`, e `MetadataIOBytes` — rappresentano la velocità effettiva che state determinando sul vostro file system. La metrica `MeteredIOBytes` rappresenta il calcolo del throughput complessivo misurato che stai determinando. Puoi utilizzare il grafico di Utilizzo del throughput (%) nella sezione Monitoraggio della console Amazon EFS per monitorare l'utilizzo del throughput. Se utilizzi CloudWatch dashboard personalizzati o un altro strumento di monitoraggio, puoi creare un'espressione matematica CloudWatch metrica da confrontare con. `MeteredIOBytes` `PermittedThroughput`

`PermittedThroughput` misura la quantità di velocità di trasmissione effettiva consentita per il file system. Questo valore si basa su uno dei seguenti metodi:

- Per i file system con throughput elastico, questo valore riflette la velocità massima di scrittura del file system.
- Per i file system che utilizzano il throughput Provisioned, se la quantità di dati archiviati nella classe di storage EFS Archive consente al file system di ottenere un throughput superiore a quello fornito, questa metrica riflette il throughput più elevato anziché la quantità assegnata.
- Per i file system che utilizzano il throughput Bursting, questo valore è una funzione della dimensione del file system e. `BurstCreditBalance` Effettua il monitoraggio di `BurstCreditBalance` per assicurarti che il file system funzioni alla frequenza di burst anziché alla frequenza di base. Se il saldo è costantemente pari o prossimo allo zero, prendi in considerazione la possibilità di passare alla velocità effettiva elastica o alla velocità effettiva garantita per ottenere una velocità effettiva aggiuntiva.

Quando i valori di `MeteredIOBytes` e `PermittedThroughput` sono uguali, il file system consuma tutta la velocità di trasmissione effettiva disponibile. Per i file system che utilizzano il throughput Provisioned, è possibile fornire un throughput aggiuntivo.

## Utilizzo della matematica dei parametri con Amazon EFS

Utilizzando la matematica metrica, puoi interrogare più CloudWatch metriche e utilizzare espressioni matematiche per creare nuove serie temporali basate su queste metriche. Puoi visualizzare le serie temporali risultanti nella CloudWatch console e aggiungerle ai dashboard. Ad esempio, è possibile usare i parametri Amazon EFS per calcolare il conteggio del campione delle operazioni di `DataRead` diviso 60. Il risultato è il numero medio di letture al secondo sul file system per un determinato periodo di 1 minuto. Per ulteriori informazioni sulla matematica dei parametri, consulta Use Metric Math nella Amazon User Guide. CloudWatch

Qui di seguito è possibile trovare alcune utili espressioni matematiche calcolate sui parametri di Amazon EFS.

Argomenti

- Matematica metrica: velocità effettiva in MiBps
- Operazione matematica sui parametri: Percentuale di throughput
- Matematica dei parametri: percentuale di utilizzo del throughput consentito
- Operazione matematica sui parametri: Throughput IOPS
- Operazione matematica sui parametri: Percentuale di IOPS
- Operazione matematica sui parametri: dimensione media dell'I/O in KiB
- Utilizzo di operazioni matematiche su un modello AWS CloudFormation per Amazon EFS

### Matematica metrica: velocità effettiva in MiBps

Per calcolare il throughput medio (in MiBps) per un periodo di tempo, scegliete innanzitutto una statistica di somma (`DataReadIOBytes`,, `DataWriteIOBytes` o). `MetadataIOBytes` `TotalIOBytes` Quindi convertire il valore in MiB e dividerlo per il numero di secondi nel periodo.

Supponiamo che la logica di esempio sia questa: (somma di `TotalIOBytes` ÷ 1048576 (per la conversione in MiB)) ÷ secondi nel periodo

Quindi le informazioni sulle CloudWatch metriche sono le seguenti.

| ID | Parametri utilizzabili | Statistic | Periodo |
| --- | --- | --- | --- |
| m1 | • `DataReadIOBytes`<br>• `DataWriteIOBytes`<br>• `MetadataIOBytes`<br>• `TotalIOBytes` | sum | 1 minuto |

L'ID dell'operazione matematica sui parametri e l'espressione sono i seguenti.

| ID | Expression |
| --- | --- |
| e1 | `(m1/1048576)/PERIOD(m1)` |

## Operazione matematica sui parametri: Percentuale di throughput

Questa espressione matematica metrica calcola la percentuale del throughput complessivo utilizzato per i diversi tipi di I/O, ad esempio la percentuale del throughput totale determinato dalle richieste di lettura. Per calcolare la percentuale di throughput di vari tipi di I/O (`DataReadIOBytes`, `DataWriteIOBytes` o `MetadataIOBytes`) per un periodo di tempo, moltiplica prima di tutto la corrispondente statistica derivante da una somma per 100. Quindi, dividi il risultato per la statistica derivante dalla somma di `TotalIOBytes` per lo stesso periodo.

Supponiamo che la logica di esempio sia questa: (somma di `DataReadIOBytes` x 100 (per la conversione in percentuale)) ÷ somma di `TotalIOBytes`

Quindi le informazioni sulla CloudWatch metrica sono le seguenti.

| ID | Parametro o parametri utilizzabili | Statistic | Periodo |
| --- | --- | --- | --- |
| m1 | • `TotalIOBytes` | sum | 1 minuto |

| ID | Parametro o parametri utilizzabili | Statistic | Periodo |
|---|---|---|---|
| m2 | • `DataReadIOBytes` | sum | 1 minuto |

L'ID dell'operazione matematica sui parametri e l'espressione sono i seguenti.

| ID | Expression |
|---|---|
| e1 | `(m2*100)/m1` |

## Matematica dei parametri: percentuale di utilizzo del throughput consentito

Per calcolare la percentuale di utilizzo del throughput consentito (`MeteredIOBytes`) per un periodo di tempo, moltiplicate innanzitutto il throughput per 100. MiBps Quindi dividi il risultato per la statistica media di `PermittedThroughput` convertito in MiB per lo stesso periodo.

Supponiamo che la logica di esempio sia questa: (espressione matematica metrica per la velocità effettiva in MiBps x 100 (da convertire in percentuale)) ÷ (somma di `PermittedThroughput` ÷ 1.048.576 (per convertire i byte in MiB))

Quindi CloudWatch le informazioni metriche sono le seguenti.

| ID | Parametro o parametri utilizzabili | Statistic | Periodo |
|---|---|---|---|
| m1 | `MeteredIOBytes` | sum | 1 minuto |
| m2 | `PermittedThroughput` | average | 1 minuto |

L'ID dell'operazione matematica sui parametri e l'espressione sono i seguenti.

| ID | Expression |
| --- | --- |
| e1 | (m1/1048576)/PERIOD(m1) |
| e2 | m2/1048576 |
| e3 | `((e1)*100)/(e2)` |

## Operazione matematica sui parametri: Throughput IOPS

Per calcolare le operazioni medie al secondo (IOPS) di un periodo di tempo, dividere la statistica derivata dal conteggio (`DataReadIOBytes`, `DataWriteIOBytes`, `MetadataIOBytes` o `TotalIOBytes`) per il numero di secondi del periodo.

Supponiamo che la logica di esempio sia questa: conteggio del campione di `DataWriteIOBytes` ÷ secondi nel periodo

Quindi le informazioni sulla CloudWatch metrica sono le seguenti.

| ID | Parametri utilizzabili | Statistic | Periodo |
| --- | --- | --- | --- |
| m1 | • `DataReadIOBytes`<br>• `DataWriteIOBytes`<br>• `MetadataIOBytes`<br>• `TotalIOBytes` | Conteggio del campione | 1 minuto |

L'ID dell'operazione matematica sui parametri e l'espressione sono i seguenti.

| ID | Expression |
| --- | --- |
| e1 | `m1/PERIOD(m1)` |

## Operazione matematica sui parametri: Percentuale di IOPS

Per calcolare la percentuale di IOPS al secondo dei vari tipi di I/O (`DataReadIOBytes`, `DataWriteIOBytes` o `MetadataIOBytes`) per un periodo di tempo, moltiplicare prima di tutto la corrispondente statistica derivante dal conteggio del campione per 100. Quindi dividere il risultato per la statistica derivante dal conteggio del campione di `TotalIOBytes` per lo stesso periodo.

Supponiamo che la logica di esempio sia questa: (conteggio del campione di `MetadataIOBytes` x 100 (per la conversione in percentuale)) ÷ conteggio del campione di `TotalIOBytes`

Quindi le informazioni sulla CloudWatch metrica sono le seguenti.

| ID | Parametri utilizzabili | Statistic | Periodo |
|---|---|---|---|
| m1 | • `TotalIOBytes` | Conteggio del campione | 1 minuto |
| m2 | • `DataReadIOBytes`<br>• `DataWriteIOBytes`<br>• `MetadataIOBytes` | Conteggio del campione | 1 minuto |

L'ID dell'operazione matematica sui parametri e l'espressione sono i seguenti.

| ID | Expression |
|---|---|
| e1 | (m2*100)/m1 |

## Operazione matematica sui parametri: dimensione media dell'I/O in KiB

Per calcolare la dimensione media di I/O (in KiB) per un periodo, dividere la rispettiva statistica derivante dalla somma per il parametro `DataReadIOBytes`, `DataWriteIOBytes` o `MetadataIOBytes` per la statistica derivante dal conteggio del campione dello stesso parametro.

Supponiamo che la logica di esempio sia: (somma di `DataReadIOBytes` ÷ 1.024 (per la conversione in KiB)) ÷ conteggio del campione di `DataReadIOBytes`

Quindi le informazioni sulla CloudWatch metrica sono le seguenti.

| ID | Parametri utilizzabili | Statistic | Periodo |
|---|---|---|---|
| m1 | • `DataReadIOBytes`<br>• `DataWriteIOBytes`<br>• `MetadataIOBytes` | sum | 1 minuto |
| m2 | • `DataReadIOBytes`<br>• `DataWriteIOBytes`<br>• `MetadataIOBytes` | Conteggio del campione | 1 minuto |

L'ID dell'operazione matematica sui parametri e l'espressione sono i seguenti.

| ID | Expression |
|---|---|
| e1 | `(m1/1024)/m2` |

## Utilizzo di operazioni matematiche su un modello AWS CloudFormation per Amazon EFS

Puoi anche creare espressioni matematiche metriche tramite modelli. AWS CloudFormation Uno di questi modelli può essere scaricato e personalizzato per essere utilizzato dai tutorial di Amazon EFS in poi. GitHub Per ulteriori informazioni sull'uso dei AWS CloudFormation modelli, consulta Working with AWS CloudFormation Templates nella Guida per l'AWS CloudFormation utente.

# Monitoraggio dello stato di successo o di fallimento del tentativo di montaggio

Puoi utilizzare Amazon CloudWatch Logs per monitorare e segnalare il successo o il fallimento dei tentativi di montaggio per i tuoi file system EFS da remoto senza dover accedere ai client. Utilizza la seguente procedura per configurare l'istanza EC2 in modo che utilizzi CloudWatch Logs per monitorare il successo o il fallimento dei tentativi di montaggio del file system.

Per abilitare la notifica di successo o fallimento del tentativo di montaggio nei log CloudWatch

1. Installa `amazon-efs-utils` sull'istanza EC2 montando il file system. Per ulteriori informazioni, consulta Utilizzo di AWS Systems Manager per installare o aggiornare automaticamente i client Amazon EFS o Installazione manuale del client Amazon EFS.
2. Installa `botocore` sull'istanza EC2 che monterà il file system. Per ulteriori informazioni, consulta Installazione di `botocore`.
3. Abilita la funzionalità CloudWatch Logs in. `amazon-efs-utils` Quando si utilizza AWS Systems Manager per l'installazione e la configurazione`amazon-efs-utils`, CloudWatch la registrazione viene eseguita automaticamente. Quando installi il pacchetto `amazon-efs-utils` manualmente, devi aggiornare manualmente il file `/etc/amazon/efs/efs-utils.conf` di configurazione rimuovendo i commenti dalla riga `# enabled = true` sezione nella sezione `cloudwatch-log`. Utilizzate uno dei seguenti comandi per abilitare i CloudWatch registri manualmente.

   Per le istanze Linux:

   ```
   sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/}' /etc/
   amazon/efs/efs-utils.conf
   ```

   Per le istanze 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
   ```

   Per le istanze 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. Facoltativamente, è possibile configurare CloudWatch i nomi dei gruppi di log e impostare i giorni di conservazione dei log nel file. `efs-utils.conf` Se desideri avere gruppi di log separati CloudWatch per ogni file system montato, aggiungi `/{fs_id}` alla fine del `log_group_name` campo nel `efs-utils.conf` file, come segue:

   ```
   [cloudwatch-log]
   log_group_name = /aws/efs/utils/{fs_id}
   ```

5. Collega la policy `AmazonElasticFileSystemsUtils` AWS gestita al ruolo IAM che hai collegato all'istanza EC2 o alle AWS credenziali configurate sull'istanza. A tale scopo è possibile utilizzare Systems Manager. Per ulteriori informazioni, consulta Fase 1: Configurazione di un profilo di istanza IAM con le autorizzazioni richieste.

Di seguito sono riportati alcuni esempi di voci del registro dello stato dei tentativi di montaggio:

```
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"
```

Per visualizzare lo stato di montaggio nei registri CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli Gruppi di log dalla barra di navigazione a sinistra.
3. Scegli il gruppo di log /aws/efs/utils. Vedrai un flusso di log per ogni combinazione di istanza Amazon EC2 e file system EFS.
4. Scegli un flusso di log per visualizzare eventi di log specifici, incluso lo stato di successo o di fallimento del tentativo di montaggio.

## Accesso alle CloudWatch metriche

Puoi visualizzare i parametri di Amazon EFS CloudWatch in diversi modi:

- Nella console Amazon EFS
- Nella console CloudWatch

- Utilizzo della CloudWatch CLI
- Utilizzando l'API CloudWatch

Le procedure seguenti illustrano come accedere ai parametri utilizzando tali strumenti.

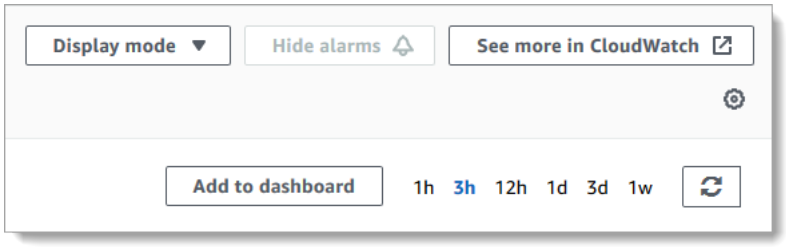
Per visualizzare CloudWatch metriche e allarmi nella console Amazon EFS

1. Accedi AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Seleziona File system.
3. Scegli il file system di cui desideri visualizzare le CloudWatch metriche.
4. Scegli Monitoraggio per visualizzare la pagina delle Metriche del file system.

   La pagina Metriche del file system mostra un set predefinito di CloudWatch metriche per il file system. Tutti gli CloudWatch allarmi configurati vengono visualizzati anche con queste metriche. Per i file system che utilizzano la modalità di prestazioni I/O max, il set di parametri predefinito include il saldo di crediti Burst al posto del limite IO in %. È possibile sovrascrivere le impostazioni predefinite utilizzando la finestra di dialogo delle impostazioni delle metriche, accessibile aprendo le impostazioni.

   > **Note**
   >
   > La metrica di utilizzo del throughput (%) non è una metrica, ma è derivata utilizzando la CloudWatch matematica metrica. CloudWatch

5. È possibile regolare il modo in cui vengono visualizzati i parametri e gli allarmi utilizzando i controlli nella pagina delle Metriche del file system, come segue.




   - Passa alla modalità di visualizzazione tra Serie temporali o Valore singolo.
   - Mostra o nasconde gli CloudWatch allarmi configurati per il file system.
   - Scegli Vedi di più in CloudWatch per visualizzare le metriche in. CloudWatch

- Scegli Aggiungi alla dashboard per aprire la CloudWatch dashboard e aggiungere le metriche visualizzate.
- Modifica la finestra temporale delle metriche visualizzata da 1 ora a 1 settimana.

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Seleziona il namespace EFS.
4. (Facoltativo) Per visualizzare un parametro, digita il suo nome nel campo di ricerca.
5. (Facoltativo) Per filtrare per dimensione, seleziona FileSystemId.

Per accedere alle metriche da AWS CLI

- Utilizza il comando `list-metrics` con il namespace `--namespace "AWS/EFS"`. Per ulteriori informazioni, consulta la sezione relativa alle informazioni di riferimento ai comandi di AWS CLI.

Per accedere alle metriche dall'API CloudWatch

- Chiama `GetMetricStatistics`. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

## Creazione di CloudWatch allarmi per monitorare Amazon EFS

Puoi creare un CloudWatch allarme che invia un messaggio Amazon SNS quando l'allarme cambia stato. Un allarme monitora un singolo parametro per un periodo di tempo specificato. L'allarme esegue una o più operazioni basate sul valore del parametro relativo a una soglia prestabilita per un certo numero di periodi. L'operazione corrisponde all'invio di una notifica a un argomento di Amazon SNS o a una policy di Auto Scaling.

Gli allarmi richiamano azioni solo per cambiamenti di stato sostenuti. CloudWatch gli allarmi non richiamano azioni solo perché si trovano in uno stato particolare; lo stato deve essere cambiato ed essere stato mantenuto per un determinato numero di periodi.

Un uso importante degli CloudWatch allarmi per Amazon EFS consiste nell'applicare la crittografia a riposo per il file system. È possibile abilitare la crittografia dei dati memorizzati su disco per un

file system Amazon EFS alla sua creazione. Per applicare encryption-at-rest le policy relative ai dati per i file system Amazon EFS, puoi utilizzare Amazon CloudWatch AWS CloudTrail per rilevare la creazione di un file system e verificare che la crittografia a riposo sia abilitata. Per ulteriori informazioni, consulta Procedura passo per passo: Applicazione della crittografia dei dati memorizzati su disco su un file system Amazon EFS.

> **Note**
>
> Al momento, non è possibile imporre la crittografia dei dati in transito.

Le seguenti procedure illustrano come creare allarmi per Amazon EFS.

Per impostare allarmi utilizzando la console CloudWatch

1. Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli Crea allarme. Viene avviata la procedura guidata per la creazione di allarmi.
3. Scegli Parametri EFS per scorrere i parametri Amazon EFS e individuare quello per il quale si desidera creare un allarme. Per visualizzare unicamente i parametri di Amazon EFS in questa finestra di dialogo, effettua la ricerca in base all'ID del file system. Seleziona il parametro per il quale si intende creare un allarme e scegli Avanti.
4. Compila i valori Nome, Descrizione, Qualsiasi momento per il parametro.
5. Se desideri CloudWatch inviarti un'e-mail quando viene raggiunto lo stato di allarme, nel campo Ogni volta che si verifica questo allarme:, scegli State is ALARM. Nel campo Invia notifica a:, seleziona un argomento SNS esistente. Se selezioni Crea argomento, puoi impostare il nome e gli indirizzi e-mail per un nuovo elenco di sottoscrizioni e-mail. Questo elenco viene salvato e visualizzato nel campo per allarmi futuri.

   > **Note**
   >
   > Se usi Crea argomento per creare un nuovo argomento Amazon SNS, gli indirizzi e-mail devono essere verificati prima di poter ricevere le notifiche. Le e-mail sono inviate solo quando viene attivato lo stato di allarme. Se lo stato cambia prima della verifica degli indirizzi e-mail, questi non riceveranno una notifica.

6. A questo punto, l'area Anteprima allarme consente di vedere un'anteprima dell'allarme che stai per creare. Scegli Crea allarme.

Per impostare una sveglia utilizzando il AWS CLI

- Chiama `put-metric-alarm`. Per ulteriori informazioni, consulta la sezione relativa alle informazioni di riferimento ai comandi di AWS CLI.

Per impostare un allarme utilizzando l' CloudWatch API

- Chiama `PutMetricAlarm`. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

# Registrazione delle chiamate API Amazon EFS con AWS CloudTrail

Amazon EFS è integrato conAWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon EFS. CloudTrail acquisisce tutte le chiamate API per Amazon EFS come eventi, incluse le chiamate dalla console Amazon EFS e le chiamate di codice alle operazioni dell'API Amazon EFS.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon EFS. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon EFS, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni, consulta la AWS CloudTrailGuida per l'utente di .

## Informazioni su Amazon EFS in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in Amazon EFS, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuoAccount AWS, compresi gli eventi per Amazon EFS, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regione AWS. Il percorso registra gli eventi da tutte le Regioni AWS nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di AWS CloudTrail:

- Panoramica della creazione di un percorso
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le chiamate API Amazon EFS vengono registrate da CloudTrail. Ad esempio, le chiamate a `CreateMountTarget` e `CreateTags` le operazioni generano voci nei file di CloudTrail registro. `CreateFileSystem`

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o AWS Identity and Access Management (utente IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, vedete l'elemento CloudTrail UserIdentity nella Guida per l'AWS CloudTrailutente.

## Comprendere le voci dei file di registro di Amazon EFS

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di

registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra il `CreateTags` funzionamento quando viene creato un tag per un file system dalla console.


```
{
 "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"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`DeleteTags`azione che si verifica quando un tag per un file system viene eliminato dalla console.


```
{
 "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"
}
```


## Voci di registro per i ruoli collegati al servizio EFS

Il ruolo collegato al servizio Amazon EFS effettua chiamate API alle AWS risorse. Verranno visualizzate le voci di CloudTrail registro `username:AWSServiceRoleForAmazonElasticFileSystem` relative alle chiamate effettuate dal ruolo

collegato al servizio EFS. Per ulteriori informazioni su EFS e sui ruoli collegati ai servizi, vedere. [Utilizzo di ruoli collegati ai servizi per Amazon EFS]

L'esempio seguente mostra una voce di CloudTrail registro che mostra un'`CreateServiceLinkedRole`azione quando Amazon EFS crea il ruolo collegato al AWSServiceRoleForAmazonElasticFileSystem servizio.


```
{
    "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"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che mostra un'`CreateNetworkInterface`azione eseguita dal ruolo AWSServiceRoleForAmazonElasticFileSystem collegato al servizio, annotato in. `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": "20You 19-10-23T22:50:05Z",
    "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"
}
```

## Voci di registro per l'autenticazione EFS

Autorizzazione Amazon EFS per le emissioni `NewClientConnection` e `UpdateClientConnection` CloudTrail gli eventi dei client NFS. Un evento `NewClientConnection` viene emesso quando una connessione è autorizzata subito dopo una connessione iniziale e subito dopo una riconnessione. Un `UpdateClientConnection` viene emesso quando una connessione viene nuovamente autorizzata e l'elenco delle azioni consentite è cambiato. L'evento viene emesso anche quando il nuovo elenco di azioni consentite non include. `ClientMount` Per ulteriori informazioni sull'autorizzazione EFS, vedereUtilizzo di IAM per controllare l'accesso ai dati del file system.

L'esempio seguente mostra una voce di CloudTrail registro che illustra 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-aee3-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"
    }
}
```

## Voci dei file di log di Amazon encrypted-at-rest EFS per i file system

Amazon EFS ti offre la possibilità di utilizzare la crittografia a riposo, la crittografia in transito o entrambe per i tuoi file system. Per ulteriori informazioni, consulta Crittografia dei dati in Amazon EFS.

Amazon EFS invia il contesto di crittografia quando effettua richieste AWS KMS API per generare chiavi di dati e decrittografare i dati Amazon EFS. L'ID del file system è il contesto di crittografia per tutti i file system con crittografia dei dati inattivi. Nel `requestParameters` campo di una voce di CloudTrail registro, il contesto di crittografia è simile al seguente.

```
"EncryptionContextEquals": {}
"aws:elasticfilesystem:filesystem:id" : "fs-4EXAMPLE"
```

# Prestazioni Amazon EFS

Le sezioni seguenti forniscono una panoramica delle prestazioni Amazon EFS e descrivono in che modo la configurazione del file system influisce sulle dimensioni prestazionali chiave. Forniamo anche alcuni importanti suggerimenti e raccomandazioni per ottimizzare le prestazioni del tuo file system.

Argomenti



## Riepilogo delle prestazioni

Le prestazioni del file system vengono generalmente misurate utilizzando le dimensioni di latenza, velocità effettiva e operazioni di input/output al secondo (IOPS). Le prestazioni di Amazon EFS in queste dimensioni dipendono dalla configurazione del file system. Le seguenti configurazioni influiscono sulle prestazioni di un file system Amazon EFS:

- Tipo di file system: regionale o a zona singola
- Modalità prestazioni: a scopi generali o I/O max

> **Important**
>
> La modalità Prestazioni I/O max ha latenze per operazione più elevate rispetto alla modalità di prestazioni a scopi generali. Per prestazioni più veloci, si consiglia di utilizzare sempre la modalità di prestazioni a scopi generali. Per ulteriori informazioni, consulta Modalità prestazionali.

- Modalità Throughput: Elastic, Provisioned o Bursting

La tabella seguente descrive le specifiche delle prestazioni per i file system che utilizzano la modalità di prestazioni General Purpose e le possibili diverse combinazioni di tipo di file system e modalità di throughput.

Specifiche prestazionali per i file system che utilizzano la modalità di prestazioni General Purpose

| Configurazione dello storage e della velocità di trasmissione effettiva | | Latenza | | Numero massimo di IOPS | | Velocità di trasmissione effettiva massima | | |
|---|---|---|---|---|---|---|---|---|
| Tipo di file system | Modalità di velocità di trasmissione effettiva | Operazioni di lettura | Operazioni di scrittura | Operazioni di lettura | Operazioni di scrittura | P er-file-system read [1] | P er-file-system scrivi [1] | Lettura/scrittura per client |
| Regionale | Elastic | A partire da 250 µs | As low as 2.7 ms | 90,000–250,000[2] | 50,000 | 3—20 GiBps | 1—5 GiBps | 500 MiBps |
| Regionale | Provisioned | A partire da 250 µs | As low as 2.7 ms | 55,000 | 25,000 | 3—10 GiBps | 1—3,33 GiBps | 500 MiBps |
| Regionale | Bursting | A partire da 250 µs | As low as 2.7 ms | 35,000 | 7,000 | 3—5 GiBps | 1—3 GiBps | 500 MiBps |
| Zona singola | Elastic, Provisioned, or Bursting | A partire da 250 | A partire da 1,6 | 35,000 | 7,000 | 3-5 gibibyteal | 1—3 GiBps | 500 mebibytesper |

| Configurazione dello storage e della velocità di trasmissione effettiva | Latenza | | Numero massimo di IOPS | Velocità di trasmissione effettiva massima | |
|---|---|---|---|---|---|
| | microsecondi (µs) | millisecondi (ms) | | secondo () GiBps | second (MiBps) |

> **Note**
>
> Note a piè di pagina:
>
> 1. La velocità massima di lettura e scrittura dipende da Regione AWS. Una velocità di trasmissione effettiva superiore a quella massima di Regione AWS richiede un aumento della quota di velocità di trasmissione effettiva. Qualsiasi richiesta di throughput aggiuntivo viene presa in considerazione dal case-by-case team di assistenza di Amazon EFS. L'approvazione potrebbe dipendere dal tipo di carico di lavoro. Per ulteriori informazioni sulla richiesta di aumenti di quota, consulta Quote e limiti di Amazon EFS.
> 2. I file system che utilizzano la velocità effettiva elastica possono generare un massimo di 90.000 operazioni di lettura per i dati a cui si accede raramente e 250.000 IOPS di lettura per i dati ad accesso frequente. Per raggiungere il massimo degli IOPS si applicano raccomandazioni aggiuntive. Per ulteriori informazioni, consulta the section called “Ottimizzazione dei carichi di lavoro che richiedono throughput e IOPS elevati”.

## Classi di storage

Le classi di storage Amazon EFS sono progettate per lo storage più efficace a seconda dei casi d'uso.

- La classe di storage EFS Standard utilizza storage SSD (Solid State Drive) per offrire i livelli di latenza più bassi per i file a cui si accede di frequente. Questa classe di storage fornisce latenze di primo byte di appena 250 us per le letture e 2,7 ms per le scritture.

- Le classi di storage EFS Infrequent Access (IA) ed EFS Archive archiviano i dati a cui si accede meno frequentemente che non richiedono le prestazioni di latenza richieste dai dati a cui si accede di frequente. Queste classi di storage forniscono latenze di primo byte di decine di millisecondi.

Per ulteriori informazioni sulle classi di storage EFS, consulta the section called “Classi di storage EFS”.

## Modalità prestazionali

Amazon EFS offre due modalità prestazionali: a scopi generali e I/O max.

- La modalità General Purpose ha la latenza per operazione più bassa ed è la modalità di prestazioni predefinita per i file system. I file system One Zone utilizzano sempre la modalità di prestazioni General Purpose. Per prestazioni più veloci, si consiglia di utilizzare sempre la modalità di prestazioni a scopi generali.
- La Modalità I/O max è un tipo di prestazioni della generazione precedente progettata per carichi di lavoro altamente parallelizzati in grado di tollerare latenze più elevate rispetto alla modalità a scopi generali. La modalità I/O max non è supportata per i file system a zona singola o per i file system che utilizzano la velocità di trasmissione effettiva Elastic.

> **Important**
>
> A causa delle più elevate latenze per operazione con I/O max, consigliamo di utilizzare la modalità prestazionale a scopi generali per tutti i file system.

Per garantire che il carico di lavoro rimanga entro il limite di IOPS disponibile per i file system che utilizzano la modalità di prestazioni General Purpose, puoi monitorare la `PercentIOLimit` CloudWatch metrica. Per ulteriori informazioni, consulta CloudWatch Parametri Amazon per Amazon EFS.

Le applicazioni possono scalare i propri IOPS in modo elastico fino al limite associato alla modalità a prestazioni. Gli IOPS non vengono fatturati separatamente; sono inclusi nella contabilità della velocità di trasmissione effettiva di un file system. Ogni richiesta di Network File System (NFS) viene contabilizzata come 4 kilobyte (KB) di throughput o come dimensione effettiva di richiesta e risposta, a seconda di quale tra i due sia maggiore.

# Modalità di velocità di trasmissione effettiva

La modalità di velocità di trasmissione effettiva del file system determina la velocità di trasmissione effettiva disponibile per il file system. Amazon EFS offre tre modalità di throughput: Elastic, Provisioned e Bursting. La velocità effettiva di lettura è scontata per consentirti di aumentare la velocità di lettura rispetto alla velocità effettiva di scrittura. La velocità effettiva massima disponibile con ciascuna modalità di throughput dipende da Regione AWS. Per ulteriori informazioni sulla velocità effettiva massima del file system nelle diverse regioni, consulta Quote e limiti di Amazon EFS.

Il file system può raggiungere una velocità combinata del 100% della velocità di lettura e scrittura. Ad esempio, se il file system utilizza il 33% del limite di velocità effettiva di lettura, il file system può raggiungere contemporaneamente fino al 67% del limite di velocità di scrittura. È possibile monitorare l'utilizzo della velocità effettiva del file system nel grafico di Utilizzo della velocità effettiva (%) nella pagina Dettagli del file system della console. Per ulteriori informazioni, consulta Utilizzo delle CloudWatch metriche per monitorare le prestazioni del throughput.

## Scelta della modalità di throughput corretta per un file system

La scelta della modalità di throughput corretta per il file system dipende dai requisiti prestazionali del carico di lavoro.

- Throughput elastico (consigliato): utilizza il throughput elastico predefinito in caso di carichi di lavoro con picchi o imprevedibili e requisiti di prestazioni difficili da prevedere o quando l'applicazione aumenta il throughput con un rapporto del 5% o inferiore. average-to-peak Per ulteriori informazioni, consulta Throughput elastico.
- Throughput assegnato: utilizza il throughput assegnato se conosci i requisiti prestazionali del tuo carico di lavoro o quando l'applicazione aumenta il throughput con un rapporto del 5% o più. average-to-peak Per ulteriori informazioni, consulta Throughput assegnato.
- Throughput bursting: utilizza Bursting throughput quando desideri un throughput scalabile in base alla quantità di storage presente nel file system.

  Se, dopo aver utilizzato la velocità effettiva di bursting, scopri che la tua applicazione è soggetta a vincoli di throughput (ad esempio, utilizza più dell'80% della velocità effettiva consentita o hai utilizzato tutti i crediti di burst), allora dovresti utilizzare il throughput Elastic o Provisioned. Per ulteriori informazioni, consulta Velocità effettiva di espansione.

Puoi usare Amazon CloudWatch per determinare il average-to-peak rapporto del tuo carico di lavoro confrontando la metrica con la `MeteredIOBytes` metrica. `PermittedThroughput` Per ulteriori informazioni sulle metriche di Amazon EFS, consulta CloudWatch Parametri Amazon per Amazon EFS.

## Throughput elastico

Per i file system che utilizzano la velocità effettiva elastica, Amazon EFS aumenta o riduce automaticamente le prestazioni di throughput per soddisfare le esigenze dell'attività del carico di lavoro. Il throughput elastico è la modalità di throughput migliore per carichi di lavoro con picchi o imprevedibili con requisiti di prestazioni difficili da prevedere o per applicazioni che incrementano il throughput al 5% o meno del throughput di picco in media (il rapporto). average-to-peak

Poiché le prestazioni di throughput per i file system con Elastic Throughput si scalano automaticamente, non è necessario specificare o fornire la capacità di throughput per soddisfare le esigenze delle applicazioni. Paghi solo per la quantità di metadati e dati letti o scritti e non accumuli né utilizzi crediti burst durante l'utilizzo di Elastic Throughput.

> **Note**
>
> Il throughput elastico è disponibile solo per i file system che utilizzano la modalità di prestazioni General Purpose.

Per informazioni sui limiti di throughput elastico per regione, consulta. Quote per Amazon EFS che è possibile incrementare

## Throughput assegnato

Con Provisioned Throughput, è possibile specificare un livello di throughput che il file system è in grado di gestire indipendentemente dalle dimensioni del file system o dal saldo del credito residuo. Utilizza Provisioned Throughput se conosci i requisiti prestazionali del tuo carico di lavoro o se la tua applicazione aumenta il throughput al 5% o più del rapporto. average-to-peak

Per i file system che utilizzano il throughput Provisioned, viene addebitata la quantità di throughput abilitata per il file system. L'importo della velocità effettiva fatturata in un mese si basa sulla velocità effettiva fornita in eccesso rispetto alla velocità effettiva di base inclusa nel file system dallo storage Standard, fino ai limiti di throughput di base prevalenti di Bursting previsti in Regione AWS.

Se la velocità effettiva di base del file system supera la quantità di throughput di base di Provisioned, utilizza automaticamente la velocità effettiva di bursting consentita per il file system (fino ai limiti di throughput di base prevalenti di\ Bursting). Regione AWS

Per informazioni sui limiti per velocità effettiva, vedere. RegionProvisioned Quote per Amazon EFS che è possibile incrementare

## Velocità effettiva di espansione

Il bursting throughput è consigliato per carichi di lavoro che richiedono un throughput scalabile in base alla quantità di storage presente nel file system. Con Bursting Throughput, il throughput di base è proporzionato alla dimensione del file system nella classe di storage Standard, a una velocità di 50 per KiBps ogni GiB di storage. I crediti burst vengono accumulati quando il file system consuma al di sotto della velocità di throughput di base e vengono detratti quando il throughput supera la velocità di base.

Quando sono disponibili crediti burst, un file system può aumentare il throughput fino a 100 per MiBps TiB di storage, fino al Regione AWS limite, con un minimo di 100. MiBps Se non sono disponibili crediti burst, un file system può gestire fino a 50 unità MiBps per TiB di storage, con un minimo di 1. MiBps

Per informazioni sulla velocità effettiva di bursting per regione, consulta. General resource quotas that cannot be changed

Informazioni sui crediti di burst di Amazon EFS

Con il bursting throughput, ogni file system guadagna crediti burst nel tempo a una velocità di base determinata dalla dimensione del file system archiviato nella classe di storage EFS Standard. La frequenza di base è di 50 MiBps per tebibyte [TiB] di storage (equivalente a 50 KiBps per GiB di storage). Amazon EFS misura le operazioni di lettura fino a un terzo della velocità delle operazioni di scrittura, permettendo al file system di raggiungere una velocità di base fino a 150 per KiBps GiB di velocità effettiva di lettura o 50 per KiBps GiB di velocità effettiva di scrittura.

Un file system può incrementare la velocità effettiva alla velocità misurata di base in modo continuo. Un file system accumula crediti burst ogni volta che è inattivo o porta il throughput al di sotto della velocità misurata di base. I crediti per i burst accumulati offrono al file system la possibilità di incrementare il throughput al di sopra della velocità di base.

Ad esempio, un file system con 100 GiB di dati misurati nella classe di storage Standard ha un throughput di base di 5. MiBps In un periodo di inattività di 24 ore, il file system guadagna 432.000

MiB di credito (5 MiB × 86.400 secondi = 432.000 MiB), che possono essere utilizzati per raggiungere i 100 MiB per 72 minuti (432.000 MiB ÷ 100 = 72 minuti). MiBps MiBps

I file system di dimensioni superiori a 1 TiB possono sempre sfruttare dei burst per il 50 per cento del tempo se rimangono inattivi per il restante 50 per cento.

La tabella riportata di seguito fornisce degli esempi di comportamento in tema di burst.

| Dimensione del file system | Throughput di burst | Throughput di base |
|---|---|---|
| 100 GiB di dati misurati nello storage Standard | • Burst to 300 () in sola lettura per un massimo di 72 minuti al giorno, oppure MiBps<br>• Passa a 100 in MiBps sola scrittura per un massimo di 72 minuti al giorno | • Fino a 15 unità in modalità di sola lettura ininterrottamente MiBps<br>• Fino a 5 unità di sola scrittura ininterrottamente MiBps |
| 1 TiB di dati misurati nello storage Standard | • Passa a 300 in MiBps sola lettura per 12 ore al giorno, oppure<br>• Passa a 100 in sola MiBps scrittura per 12 ore al giorno | • Drive 150 in sola lettura ininterro ttamente MiBps<br>• Drive 50 in modalità di sola scrittura continua MiBps |
| 10 TiB di dati misurati nello storage Standard | • Passa a 3 in GiBps sola lettura per 12 ore al giorno, oppure<br>• Passa a 1 sola GiBps scrittura per 12 ore al giorno | • Drive 1.5 in modalità di sola lettura continua GiBps<br>• Drive 500 in modalità di sola scrittura continua MiBps |
| In genere, file system di dimensioni maggiori | • Passa a 300 unità di MiBps sola lettura per TiB di storage per 12 ore al giorno, oppure<br>• Passa a 100 unità di MiBps sola scrittura per TiB di storage per 12 ore al giorno | • Gestisci 150 unità di MiBps sola lettura per TiB di storage in modo continuo<br>• Gestisci 50 unità di MiBps sola scrittura per TiB di storage in modo continuo |

> **Note**
>
> Amazon EFS fornisce un throughput misurato pari MiBps a 1 per tutti i file system, anche se la frequenza di base è inferiore.
> La dimensione del file system utilizzata per determinare la velocità di base e quella di burst è la stessa dimensione `ValueInStandard` misurata disponibile tramite l'operazione API DescribeFileSystems.
> I file system possono guadagnare crediti fino a un saldo massimo di 2,1 TiB per file system di dimensioni inferiori a 1 TiB, o fino a 2,1 TiB per TiB memorizzato in caso di file system di dimensioni superiori a 1 TiB. Questo approccio implica che i file system possano accumulare un numero sufficiente di crediti per aumentare le prestazioni fino a 12 ore in modo continuo.

## Restrizioni al cambio di velocità effettiva e alla modifica della quantità assegnata

È possibile cambiare la modalità di throughput di un file system esistente e modificare la quantità di throughput. Tuttavia, dopo aver cambiato la modalità di throughput in Provisioned Throughput o modificato l'importo del throughput fornito, le seguenti azioni sono limitate per un periodo di 24 ore:

- Passaggio dalla modalità di throughput Provisioned alla modalità di throughput Elastic o Bursting.
- Diminuzione della quantità di throughput fornita.

# Suggerimenti per le prestazioni Amazon EFS

Quando si utilizza Amazon EFS, è necessario ricordare i seguenti suggerimenti sulle prestazioni.

## Dimensione media di I/O

La natura distribuita di Amazon EFS offre alti livelli di disponibilità, durabilità e scalabilità. Grazie all'architettura distribuita, la latenza per ciascuna operazione sui file è minima. Grazie alla latenza per operazione, il throughput generale si incrementa assieme all'incremento delle dimensioni medie delle operazioni di I/O, perché l'overhead viene ammortizzato su una maggiore quantità di dati.

# Ottimizzazione dei carichi di lavoro che richiedono throughput e IOPS elevati

Per i carichi di lavoro che richiedono un throughput e IOPS elevati, utilizza i file system regionali configurati con la modalità di prestazioni General Purpose e il throughput elastico.

> **Note**
>
> Per raggiungere il massimo di 250.000 IOPS in lettura per i dati a cui si accede di frequente, il file system deve utilizzare la velocità effettiva elastica.

Per raggiungere i massimi livelli di prestazioni, è necessario sfruttare la parallelizzazione configurando l'applicazione o il carico di lavoro come segue.

1. Distribuisci il carico di lavoro in modo uniforme su tutti i client e le directory, con almeno lo stesso numero di directory del numero di client utilizzati.
2. Riduci al minimo le controversie allineando i singoli thread a set di dati o file distinti.
3. Distribuisci il carico di lavoro su 10 o più client NFS, con almeno 64 thread per client in un unico target di montaggio.

## Connessioni simultanee

Puoi montare i file system Amazon EFS su un massimo di migliaia di Amazon EC2 e altre istanze di AWS calcolo contemporaneamente. È possibile ottenere livelli di throughput più elevati sul file system in aggregato tra le istanze di elaborazione se si può parallelizzare l'applicazione su più istanze.

## Modello di richiesta

Se si abilitano le scritture asincrone sul file system, le operazioni di scrittura in sospeso vengono bufferizzate sull'istanza Amazon EC2 prima di essere scritte su Amazon EFS in modo asincrono. Le scritture asincrone presentano generalmente delle latenze inferiori. Quando si eseguono delle scritture asincrone, il kernel utilizza della memoria aggiuntiva per la memorizzazione nella cache.

Un file system che ha abilitato le scritture sincrone, o uno che apre i file usando un'opzione che bypassa la cache (ad esempio, `O_DIRECT`), emette richieste sincrone ad Amazon EFS. Ogni operazione implica una richiesta e una risposta tra client ed Amazon EFS.

> **Note**
>
> La modalità di richiesta presenta compromessi in termini di consistenza (se si utilizzano molteplici istanze Amazon EC2) e di velocità. L'utilizzo delle scritture sincrone offre una maggiore coerenza dei dati completando ogni transazione di richiesta di scrittura prima di elaborare la richiesta successiva. L'utilizzo delle scritture asincrone offre una maggiore velocità di trasmissione mediante il buffering delle operazioni di scrittura in sospeso.

## Impostazioni di installazione del client NFS

Verifica di utilizzare le opzioni di montaggio raccomandate come descritto in Montaggio dei file system EFS e in Ulteriori considerazioni sul montaggio.

Quando si installano i file system sulle istanze Amazon EC2, Amazon EFS supporta i protocolli Network File System versione 4.0 e 4.1 (NFSv4). NFSv4.1 offre prestazioni migliori per le operazioni di lettura parallela di file di piccole dimensioni (più di 10.000 file al secondo) rispetto a NFSv4.0 (meno di 1.000 file al secondo). Per le istanze macOS di Amazon EC2 che eseguono macOS Big Sur, è supportato solo NFSv4.0.

Non utilizzare le seguenti opzioni di installazione:

- `noac`, `actimeo=0`, `acregmax=0`, `acdirmax=0`: queste opzioni disattivano la cache degli attributi, il che ha un impatto molto importante sulle prestazioni.
- `lookupcache=pos`, `lookupcache=none`: queste opzioni disattivano la cache di ricerca del nome file, il che ha un impatto molto importante sulle prestazioni.
- `fsc`: questa opzione abilita la memorizzazione nella cache locale dei file, ma non modifica la coerenza della cache NFS e non riduce le latenze.

> **Note**
>
> Quando si installa il file system, è possibile aumentare le dimensioni del buffer in lettura e in scrittura per il client NFS fino a 1 MB.

## Ottimizzazione delle prestazioni dei file di piccole dimensioni

È possibile migliorare le prestazioni dei file di piccole dimensioni riducendo al minimo le riaperture dei file, aumentando il parallelismo e raggruppando i file di riferimento ove possibile.

- Riduci al minimo il numero di accessi al server.

  Non chiudere inutilmente i file se ne hai bisogno in un secondo momento in un flusso di lavoro. Mantenere aperti i descrittori di file consente l'accesso diretto alla copia locale nella cache. Le operazioni di apertura, chiusura e metadati dei file in genere non possono essere eseguite in modo asincrono o tramite una pipeline.

  Quando si leggono o si scrivono file di piccole dimensioni, i due passaggi aggiuntivi sono significativi.

  Ogni passaggio (file aperto, file chiuso) può richiedere tanto tempo quanto la lettura o la scrittura di megabyte di dati in blocco. È più efficiente aprire un file di input o output una sola volta, all'inizio del processo di elaborazione, e tenerlo aperto per l'intera durata del lavoro.
- Utilizza il parallelismo per ridurre l'impatto dei passaggi.
- Raggruppa i file di riferimento in un file `.zip`. Alcune applicazioni utilizzano un ampio set di file di riferimento di piccole dimensioni, per lo più di sola lettura. Il raggruppamento di questi file in un unico file `.zip` consente di leggere molti file con un solo passaggio di apertura e chiusura.

  Il formato `.zip` consente l'accesso casuale a singoli file.

## Ottimizzazione delle prestazioni della directory

Quando si esegue un elenco (ls) su directory molto grandi (oltre 100.000 file) che vengono modificate contemporaneamente, i client Linux NFS possono bloccarsi e non restituire una risposta. Questo problema è stato risolto nel kernel 5.11, che è stato portato sui kernel Amazon Linux 2 4.14, 5.4 e 5.10.

Ti consigliamo di mantenere il numero di directory sul file system a meno di 10.000, se possibile. Usa sottodirectory annidate il più possibile.

Quando elenchi una directory, evita di ottenere gli attributi dei file se non sono richiesti, perché non sono memorizzati nella directory stessa.

# Ottimizzazione della dimensione read_ahead_kb di NFS

L'attributo `read_ahead_kb` NFS definisce il numero di kilobyte per cui il kernel Linux deve effettuare la lettura anticipata o il recupero preliminare durante un'operazione di lettura sequenziale.

Per le versioni del kernel Linux precedenti alla 5.4.*, il valore `read_ahead_kb` viene impostato moltiplicando `NFS_MAX_READAHEAD` per il valore `rsize` (la dimensione del buffer di lettura configurata dal client impostata nelle opzioni di montaggio). Quando si utilizzano le opzioni di montaggio consigliate, questa formula imposta `read_ahead_kb` su 15 MB.

> **Note**
>
> A partire dalle versioni del kernel Linux 5.4.*, il client Linux NFS utilizza un valore `read_ahead_kb` predefinito di 128 KB. Si consiglia di aumentare questo valore a 15 MB.

L'helper di montaggio di Amazon EFS disponibile nella versione `amazon-efs-utils` 1.33.2 e successive modifica automaticamente il valore `read_ahead_kb` per renderlo uguale a 15 * `rsize`, o 15 MB, dopo il montaggio del file system.

Per i kernel Linux 5.4 o successivi, se non utilizzi l'helper di montaggio per installare i tuoi file system, valuta la possibilità di impostare `read_ahead_kb` manualmente su 15 MB per migliorare le prestazioni. Dopo aver montato il file system, è possibile reimpostare il valore `read_ahead_kb` utilizzando il comando seguente. Prima di usare questo comando, sostituisci i seguenti valori:

- Sostituisci *`read-ahead-value-kb`* con la dimensione desiderata in kilobyte.
- Sostituisci *`efs-mount-point`* con il punto di montaggio del file system.

```
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"
```

Ad esempio, di seguito viene impostata la dimensione `read_ahead_kb` su 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"
```

# Backup dei file system di Amazon EFS

AWS Backup è un modo semplice ed economico per proteggere i dati eseguendo il backup dei file system Amazon EFS. AWS Backup è un servizio di backup unificato progettato per semplificare la creazione, la migrazione, il ripristino e l'eliminazione dei backup, fornendo al contempo report e audit migliorati. AWS Backup semplifica lo sviluppo di una strategia di backup centralizzata per la conformità legale, normativa e professionale. AWS Backup semplifica inoltre la protezione dei volumi di AWS storage, dei database e dei file system fornendo una posizione centrale in cui è possibile eseguire le seguenti operazioni:

- Configura e controlla le AWS risorse di cui desideri eseguire il backup
- Automatizzare la pianificazione dei backup
- Impostare le policy di conservazione
- Monitorare tutte le attività recenti di backup e ripristino

Amazon EFS è integrato nativamente con AWS Backup. È possibile utilizzare la console EFS, l'API e AWS Command Line Interface (AWS CLI) per abilitare i backup automatici per il file system. I backup automatici utilizzano un piano di backup predefinito con le impostazioni AWS Backup consigliate per i backup automatici. Per ulteriori informazioni, consulta Backup automatici. È inoltre possibile AWS Backup impostare manualmente i propri piani di backup specificando la frequenza di backup, quando eseguire il backup, per quanto tempo conservare i backup e una politica del ciclo di vita per i backup. Puoi assegnare i file system Amazon EFS o altre risorse AWS al piano di backup.

## Backup incrementali

AWS Backup esegue backup incrementali dei file system EFS. Nel backup iniziale viene creata una copia dell'intero file system. Nei backup successivi di quel file system, vengono copiati solo i file e le directory che sono stati modificati, aggiunti o rimossi. Con ogni backup incrementale, AWS Backup conserva i dati di riferimento necessari per consentire un ripristino completo. Questo approccio riduce il tempo necessario per completare il backup e consente di risparmiare sui costi di storage, perché i dati non vengono duplicati.

## Coerenza del backup

Amazon EFS è progettato per garantire un'elevata disponibilità. È possibile accedere ai file system Amazon EFS e modificarli durante l'esecuzione del backup in AWS Backup. Se apporti modifiche

al file system durante l'esecuzione del backup, possono tuttavia verificarsi incoerenze, ad esempio dati duplicati, disallineati o esclusi. Le modifiche includono la scrittura, l'assegnazione di un nuovo nome, lo spostamento o l'eliminazione. Per garantire backup coerenti, ti consigliamo di sospendere le applicazioni o i processi che modificano il file system per la durata del processo di backup. In alternativa, pianifica i tuoi backup in modo che avvengano nei periodi in cui il file system non viene modificato.

## Prestazioni di backup

In generale, puoi aspettarti le seguenti velocità di backup e ripristino con AWS Backup. Le tariffe potrebbero essere inferiori per alcuni carichi di lavoro, ad esempio quelli contenenti file o directory di grandi dimensioni.

- Velocità di backup di 1.000 file al secondo o 300 megabyte al secondo (MBps), a seconda di quale sia la più lenta.
- Velocità di ripristino di 500 file al secondo o 150 MBps, a seconda di quale sia la più lenta.

La durata massima di un'operazione di backup in AWS Backup è di 30 giorni.

L'utilizzo AWS Backup non consuma crediti burst accumulati e non rientra nei limiti di funzionamento dei file in modalità prestazioni General Purpose. Per ulteriori informazioni, consulta Quote per i file system Amazon EFS.

## Finestre di completamento del backup

È possibile specificare una finestra di completamento per un backup. Questa finestra definisce il periodo di tempo in cui un backup deve essere completato. Se specifichi una finestra di completamento, assicurati di prendere in considerazioni le prestazioni previste, le dimensioni e la composizione del file system. In questo modo puoi assicurarti che il backup possa essere completato nella finestra.

I backup non completati nella finestra indicata vengono contrassegnati con lo stato incompleto. Durante il successivo backup pianificato, AWS Backup riprende dal punto in cui era stato interrotto. È possibile visualizzare lo stato di tutti i backup nella Console di gestione di AWS Backup.

# Classi di storage EFS

È possibile utilizzare AWS Backup per eseguire il backup di tutti i dati in un file system EFS, indipendentemente dalla classe di storage in cui si trovano i dati. Non ti sarà addebitato alcun costo di accesso ai dati durante il backup di un file system EFS per cui è abilitata la gestione del ciclo di vita e con i dati nella classe di storage ad accesso infrequente (IA).

Quando si ripristina un punto di ripristino, vengono ripristinati tutti i file nella classe di storage standard. Per ulteriori informazioni sulle classi di storage, consulta Classi di storage EFS e Gestione dello storage del file system.

# Autorizzazioni IAM per la creazione e il ripristino dei backup

Puoi utilizzare le azioni `elasticfilesystem:backup` e `elasticfilesystem:restore` per consentire o negare a un'entità IAM (ad esempio, un utente, un gruppo o un ruolo) la possibilità di creare o ripristinare backup di un file system EFS. È possibile utilizzare queste azioni in una policy del file system o in una policy IAM basata sull'identità. Per ulteriori informazioni, consultare Gestione dell'identità e degli accessi per Amazon Elastic File System e Utilizzo di IAM per controllare l'accesso ai dati del file system.

# Backup on-demand

Utilizzando la console di gestione AWS Backup o l'interfaccia a riga di comando, è possibile salvare una singola risorsa in un vault di backup on demand. A differenza dei backup pianificati, non è necessario creare un piano di backup per avviare un backup on demand. È comunque possibile assegnare un ciclo di vita al backup, che sposta automaticamente il punto di ripristino sul livello di cold storage e annota quando eliminarlo.

# Backup simultanei

AWS Backup limita i backup a un backup simultaneo per risorsa. Di conseguenza, i backup pianificati, oppure on-demand, possono non andare a buon fine se è già in corso un processo di backup. Per ulteriori informazioni sui limiti di AWS Backup , consulta Limiti di AWS Backup nella Guida per sviluppatori di AWS Backup .

# Backup automatici

Quando crei un file system utilizzando la console Amazon EFS, i backup automatici vengono attivati per impostazione predefinita. È possibile attivare i backup automatici dopo aver creato il file system utilizzando la CLI o l'API. Il piano di backup EFS predefinito utilizza le impostazioni AWS Backup consigliate per i backup automatici, ovvero backup giornalieri con un periodo di conservazione di 35 giorni. I backup creati utilizzando il piano di backup EFS predefinito vengono archiviati in un archivio di backup EFS predefinito, anch'esso creato da EFS per conto dell'utente. Non è possibile eliminare il piano e il vault di backup predefiniti. È possibile modificare le impostazioni del piano di backup predefinito utilizzando la console. AWS Backup Per ulteriori informazioni, consulta Opzione 3: Creazione di piani automatici di backup nella Guida per gli sviluppatori di AWS Backup . È possibile visualizzare tutti i backup automatici e modificare le impostazioni del piano di backup EFS predefinito utilizzando la console AWS Backup. Puoi disattivare i backup automatici in qualsiasi momento utilizzando la console Amazon EFS o la CLI, descritta nella sezione seguente.

Amazon EFS applica la chiave `aws:elasticfilesystem:default-backup` del tag di sistema con un valore pari a `enabled` ai file system EFS quando i backup automatici sono abilitati.

> **Note**
>
> I backup automatici sono esenti dalla configurazione di opt-out del AWS Backup servizio. Per ulteriori informazioni, consulta Nozioni di base su AWS Backup nella AWS Backup Guida per gli sviluppatori.

## Attivazione o disattivazione dei backup automatici per i file system esistenti

Dopo aver creato un file system, puoi attivare o disattivare i backup automatici utilizzando la console, la CLI o l'API EFS.

Attivazione o disattivazione dei backup automatici per i file system esistenti (console)

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Nella pagina File system, scegli il file system per cui desideri attivare o disattivare i backup automatici e visualizza la pagina dei Dettagli del file system.
3. Scegli Modifica nel pannello delle impostazioni Generale.
4. • Per attivare i backup automatici, seleziona Abilita i backup automatici.

- Per disattivare i backup automatici, deseleziona Abilita i backup automatici.

5. Seleziona Salvataggio delle modifiche.

Attivazione o disattivazione dei backup automatici per i file system esistenti (CLI)

- Utilizza il comando `put-backup-policy` CLI (l'operazione API corrispondente è PutBackupPolicy) per attivare o disattivare i backup automatici per un file system esistente.

  - Utilizza il comando seguente per attivare i backup automatici.

    ```
    $ aws efs put-backup-policy --file-system-id fs-01234567 \
    --backup-policy Status="ENABLED"
    ```

    EFS risponde con la nuova policy di backup.

    ```
    {
       "BackupPolicy": {
          "Status": "ENABLING"
       }
    }
    ```

  - Utilizza il comando seguente per disattivare i backup automatici.

    ```
    $ aws efs put-backup-policy --file-system-id fs-01234567 \
    --backup-policy Status="DISABLED"
    ```

    EFS risponde con la nuova policy di backup.

    ```
    {
       "BackupPolicy": {
          "Status": "DISABLING"
       }
    }
    ```

# Utilizzo AWS Backup per configurare manualmente i backup

Quando si utilizza AWS Backup per configurare manualmente i backup del file system, è innanzitutto necessario creare un piano di backup. Il piano di backup definisce la pianificazione e la finestra del

backup, la policy di conservazione e del ciclo di vita e i tag. È possibile creare un piano di backup utilizzando la console di AWS Backup gestione AWS CLI, o l' AWS Backup API. Nell'ambito di un piano di backup, puoi definire quanto segue:

- Pianificazione: quando viene eseguito il backup
- Finestra di backup: la finestra temporale durante la quale deve iniziare il backup
- Ciclo di vita: quando spostare un punto di ripristino in cold storage e quando eliminarlo
- Vault di backup: quale vault viene utilizzato per organizzare i punti di ripristino creati dalla regola di Backup

Dopo aver creato il piano di backup, devi assegnare i file system Amazon EFS specifici al piano utilizzando i tag o l'ID del file system Amazon EFS. Dopo l'assegnazione di un piano, AWS Backup inizia a effettuare automaticamente il backup del file system Amazon EFS per proprio conto in base al piano di backup definito. È possibile utilizzare la AWS Backup console per gestire le configurazioni di backup o monitorare l'attività di backup. Per ulteriori informazioni, consulta la Guida per gli sviluppatori di AWS Backup .

> **Note**
>
> I socket e le pipe con nomi non sono supportati e sono omessi dai backup.

## Recupero di un punto di ripristino

Tramite la Console AWS Backup o l'utilizzo della CLI, è possibile recuperare un punto di ripristino in un nuovo file system EFS o nel file system di origine. È possibile eseguire un ripristino completo, che consente di ripristinare l'intero file system. In alternativa, è possibile ripristinare file e directory specifici utilizzando un ripristino parziale. Per ripristinare un file o una directory specifici, è necessario specificare il percorso relativo al punto di montaggio. Ad esempio, se il file system è montato in `/user/home/myname/efs` e il percorso del file è `user/home/myname/efs/file1`, immettere `/file1`. I percorsi fanno distinzione tra maiuscole e minuscole e non possono contenere caratteri speciali, caratteri jolly e stringhe di espressioni regolari (regex).

> **Note**
>
> Per recuperare un punto di ripristino, gli utenti devono disporre dell'autorizzazione `backup:StartRestoreJob`.

Quando si esegue un ripristino completo o parziale, il punto di ripristino viene ripristinato nella directory di ripristino, `aws-backup-restore_`*`timestamp-of-restore`*. Al termine del ripristino, è possibile visualizzare la directory di ripristino nella radice del file system. Se si tenta di eseguire più ripristini per lo stesso percorso, potrebbero esistere diverse directory contenenti gli elementi ripristinati. Se il ripristino non va a buon fine, è possibile consultare la directory `aws-backup-failed-restore_`*`timestamp-of-restore`*. È necessario eliminare manualmente le directory `restore` e `failed-restore` quando si finisce di utilizzarle.

> **Note**
>
> Per i ripristini parziali su un file system EFS esistente, AWS Backup ripristina i file e le directory in una nuova directory nella directory principale del file system. La gerarchia completa degli elementi specificati viene mantenuta nella directory di ripristino. Ad esempio, se la directory A contiene le sottodirectory B, C e D, AWS Backup mantiene la struttura gerarchica quando A, B, C e D.

Dopo il ripristino di un punto di ripristino, i frammenti di dati che non possono essere ripristinati nella giusta directory vengono inseriti nella directory `aws-backup-lost+found`. I frammenti potrebbero essere spostati in questa directory se si apportano modifiche al file system durante l'esecuzione del backup.

## Eliminazione di backup

La policy di accesso al vault di backup EFS predefinita è impostata per negare l'eliminazione dei punti di ripristino. Per eliminare i backup esistenti dei file system EFS, è necessario modificare la policy di accesso al vault. Se si tenta di eliminare un punto di ripristino EFS senza modificare la policy di accesso al vault, viene visualizzato il seguente messaggio di errore:

```
"Access Denied: Insufficient privileges to perform this action. Please consult with the
 account administrator for necessary permissions."
```

Per modificare la policy di accesso predefinita del backup vault, è necessario disporre delle autorizzazioni per modificare le policy. Per ulteriori informazioni, consulta Consenti tutte le azioni IAM (accesso amministratore) nella Guida per l'utente IAM.

Per eliminare un punto di ripristino EFS in AWS Backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegli Vault di backup.
3. Nell'elenco Backup vault, scegli automatic-backup-vaultaws/efs/.
4. Nella pagina dei dettagli del vault, seleziona Gestisci accesso nell'angolo in alto a destra della pagina. Viene visualizzata la pagina Modifica policy di accesso.
5. Per consentire tutte le azioni sul vault di backup EFS, trova la riga `"Effect": "Deny",` nell'editor JSON e modifica la riga per leggere `"Effect": "Allow",`.
6. Scegli Salva per salvare le modifiche.
7. Nella pagina dei dettagli del vault, scorri verso il basso fino alla sezione Backup e seleziona i punti di ripristino che desideri eliminare dall'elenco dei Backup. Scegli Azioni, quindi Elimina.
8. Segui le istruzioni per confermare l'eliminazione. Quindi, scegli Elimina punti di ripristino.

# Replica dei file system

È possibile creare una replica del file system EFS nella modalità Regione AWS preferita. Quando abiliti la replica su un file system EFS, Amazon Elastic File System (Amazon EFS) replica automaticamente e in modo trasparente i dati e i metadati del file system di origine in un file system di destinazione. In caso di emergenza o durante l'esecuzione di esercitazioni quotidiane, puoi eseguire il failover sul file system di replica e tornare al file system principale per riprendere le operazioni. Per gestire il processo di creazione del file system di destinazione e mantenerlo sincronizzato con il file system di origine, Amazon EFS utilizza una configurazione di replica. Per ulteriori informazioni sulla creazione di una configurazione di replica per un file system, consulta Configurazione di replica.

Dopo aver creato una configurazione di replica per un file system, Amazon EFS mantiene automaticamente sincronizzati i file system di origine e di destinazione. Le modifiche apportate al file system di origine non vengono trasferite al file system di destinazione in modo point-in-time coerente, ma vengono invece trasferite in base all'ora dell'ultima sincronizzazione per la replica. L'ora dell'ultima sincronizzazione indica quando è stata completata l'ultima sincronizzazione riuscita tra l'origine e la destinazione. Le modifiche apportate al file system di origine a partire dall'ultima ora di sincronizzazione vengono replicate nel file system di destinazione, mentre le modifiche apportate al file system di origine dopo l'ultima ora di sincronizzazione potrebbero non essere replicate. Per ulteriori informazioni, consulta Monitoraggio dello stato di replica.

La replica è disponibile in ogni Regioni AWS in cui è disponibile EFS. Per utilizzare la replica in una regione disabilitata per impostazione predefinita, è necessario prima attivare la regione. Per ulteriori informazioni, consulta Gestione di Regioni AWS nella Guida di riferimento generale di AWS. Se successivamente decidi di rinunciare a una regione, Amazon EFS sospende tutte le attività di replica per quella regione. Per riprendere le attività di replica per la regione, devi attivare nuovamente Regione AWS.

> **Note**
>
> La replica non supporta l'uso dei tag per il controllo degli accessi basato su attributi (ABAC).

Argomenti

- Configurazione di replica
- Creazione di una configurazione di replica
- Visualizzazione di configurazioni di replica

- Eliminazione di configurazioni di replica
- Monitoraggio dello stato di replica

# Configurazione di replica

Quando si crea la configurazione di replica per il file system, si sceglie Regione AWS in cui creare la replica e se eseguire la replica su un file system di destinazione nuovo o esistente.

> **Note**
>
> Un file system può far parte di una sola configurazione di replica. Non è possibile utilizzare un file system di destinazione come file system di origine in un'altra configurazione di replica.

## Replica in un nuovo file system

Amazon EFS crea automaticamente un nuovo file system e copia i dati e i metadati del file system di origine in un nuovo file system di destinazione di sola lettura in Regione AWS di propria scelta. Il file system di destinazione viene creato con le seguenti proprietà:

- Tipo di file system: il tipo di file system determina la disponibilità e la durabilità con cui il file system Amazon EFS archivia i dati all'interno di Regione AWS.
  - Scegli Regionale per creare un file system che archivia dati e metadati in modo ridondante in tutte le zone di disponibilità all'interno di Regione AWS.
  - Scegli Zona singola per creare un file system che archivia dati e metadati in modo ridondante in tutte le zone di disponibilità all'interno di una singola zona di disponibilità.

  Per ulteriori informazioni sui tipi di file system, consulta Tipi di file system EFS.
- Crittografia: tutti i file system di destinazione vengono creati con la crittografia a riposo abilitata. È possibile specificare la chiave AWS Key Management Service (AWS KMS) utilizzata per crittografare il file system di destinazione. Se non specifichi una chiave KMS, viene utilizzata la chiave KMS gestita dai servizi per Amazon EFS.

> **Important**
>
> Dopo aver creato il file system di destinazione, non è possibile modificare la chiave KMS.

- Backup automatici: per i file system di destinazione che utilizzano lo storage a zona singola, i backup automatici sono abilitati per impostazione predefinita. Dopo aver creato il file system, è possibile modificare l'impostazione di backup automatico. Per ulteriori informazioni, consultare Backup automatici
- modalità prestazioni: la modalità di prestazioni del file system di destinazione corrisponde a quella del file system di origine, a meno che il file system di destinazione non utilizzi lo storage One Zone. In tal caso, viene utilizzata la modalità Prestazioni a scopi generali. La modalità Prestazioni non può essere modificata.
- modalità throughput: la modalità di throughput del file system di destinazione corrisponde a quella del file system di origine. Dopo aver creato il file system, è possibile modificare la modalità.

  Se la modalità di throughput del file system di origine è Provisioned, la quantità di throughput assegnata al file system di destinazione corrisponde a quella del file system di origine, a meno che la quantità assegnata al file di origine non superi il limite per la regione del file system di destinazione. Se l'importo assegnato al file system di origine supera il limite della regione per il file system di destinazione, l'importo del throughput assegnato al file system di destinazione è il limite della regione. Per ulteriori informazioni, consulta Quote per Amazon EFS che è possibile incrementare.

- gestione del ciclo di vita: la gestione del ciclo di vita non è abilitata nel file system di destinazione. Puoi abilitarla dopo aver creato il file system di destinazione. Per ulteriori informazioni, consulta Gestione dello storage del file system.

## Replica su un file system esistente

EFS replica i dati e i metadati del file system di origine nel file system di destinazione e Regione AWS a scelta dell'utente. Durante la replica, EFS identifica le differenze di dati tra i file system e le applica al file system di destinazione.

Durante la replica su un file system esistente, si applicano i seguenti requisiti.

- La protezione da sovrascrittura della replica del file system di destinazione deve essere disabilitata. La protezione da sovrascrittura della replica impedisce che il file system venga utilizzato come destinazione in una configurazione di replica. Per ulteriori informazioni sulla disattivazione della protezione consulta Protezione del file system.

La disabilitazione della protezione da sovrascrittura da replica richiede le autorizzazioni per elasticfilesystem: action. UpdateFileSystemProtection Per ulteriori informazioni, consulta AWSpolitica gestita: AmazonElasticFileSystemFullAccess.

- Se il file system di origine è crittografato, anche il file system di destinazione deve essere crittografato. Inoltre, se il file di origine non è crittografato e il file system di destinazione è crittografato, non è possibile eseguire il failback alla destinazione di origine dopo aver eseguito il failover. Per ulteriori informazioni sulla crittografia, consulta Crittografia dei dati in Amazon EFS.

## Protezione del file system

Quando crei un file system Amazon EFS, la protezione da sovrascrittura della replica è abilitata per impostazione predefinita. La protezione da sovrascrittura della replica impedisce che il file system venga utilizzato come destinazione in una configurazione di replica. Prima di poter utilizzare il file system come destinazione in una configurazione di replica, è necessario disabilitare la protezione. Se si elimina la configurazione di replica, la protezione da sovrascrittura del file system viene riattivata e il file system diventa scrivibile.

La disabilitazione della protezione da sovrascrittura della replica richiede le autorizzazioni per l'azione `elasticfilesystem:UpdateFileSystemProtection`. Per ulteriori informazioni, consulta AWSpolitica gestita: AmazonElasticFileSystemFullAccess.

Lo stato della protezione da sovrascrittura della replica per un file system Amazon EFS può avere uno dei valori descritti nella tabella seguente.

| Stato del file system | Descrizione |
| --- | --- |
| ABILITATO | Non è possibile utilizzare un file system come file system di destinazione in un'altra configurazione di replica. Il file system è scrivibile. La protezione da sovrascrittura della replica è `ENABLED` per impostazione predefinita. |
| DISABILITATO | È possibile utilizzare un file system come file system di destinazione in una configurazione di replica. |

| Stato del file system | Descrizione |
| --- | --- |
| REPLICA | Il file system è in uso come file system di destinazione in una configurazione di replica. Il file system è di sola lettura e viene modificato solo da Amazon EFS durante la replica. |

Disabilitazione della protezione da sovrascrittura della replica (console)

1. Accedi a AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Nel pannello di navigazione a sinistra, scegli File system.
3. Nell'elenco File system, scegli il file system Amazon EFS che desideri usare come file system di destinazione in una configurazione di replica.
4. Nella sezione Protezione del file system, disattiva Protezione da sovrascrittura della replica.

## Autorizzazioni richieste

Amazon EFS utilizza il ruolo collegato al servizio EFS denominato `AWSServiceRoleForAmazonElasticFileSystem` per sincronizzare lo stato della replica tra i file system di origine e di destinazione. Per utilizzare la replica EFS, è necessario configurare le seguenti autorizzazioni per consentire a un'entità IAM (ad esempio un utente, un gruppo o un ruolo) di creare un ruolo collegato ai servizi, una configurazione di replica e un file system.

- `elasticfilesystem:CreateReplicationConfiguration`*
- `elasticfilesystem:DeleteReplicationConfiguration`*
- `elasticfilesystem:DescribeFileSystem`
- `elasticfilesystem:DescribeReplicationConfigurations`*
- `elasticfilesystem:CreateFileSystem`*
- `iam:CreateServiceLinkedRole`: vedi l'esempio in Utilizzo di ruoli collegati ai servizi per Amazon EFS.

> **Note**
>
> * È possibile utilizzare invece la policy `AmazonElasticFileSystemFullAccess` gestita per ottenere automaticamente tutte le autorizzazioni EFS richieste. Per ulteriori informazioni, consulta AWSpolitica gestita: AmazonElasticFileSystemFullAccess.

## Costi

Per facilitare la replica, Amazon EFS crea directory e metadati nascosti sul file system di destinazione. Questi equivalgono a circa 12 MiB di dati misurati, che vengono fatturati. Per ulteriori informazioni sulla misurazione dello storage per i file system EFS, consulta Misurazione: come Amazon EFS calcola le dimensioni di file system e oggetti.

## Prestazioni

Quando crei nuove repliche o inverti la direzione delle repliche esistenti durante il processo di failback, Amazon EFS esegue una sincronizzazione iniziale, che include una serie di azioni di configurazione una tantum per supportare la replica. Il tempo necessario per completare la sincronizzazione iniziale dipende da fattori quali la dimensione del file system di origine e il numero di file in esso contenuti.

Al termine della replica iniziale, Amazon EFS mantiene un Obiettivo del punto di ripristino (RPO) di 15 minuti per la maggior parte dei file system. Tuttavia, se il file system di origine presenta file che vengono modificati molto frequentemente e contiene più di 100 milioni di file o file di dimensioni superiori a 100 GB, la replica potrebbe richiedere più di 15 minuti. Per informazioni sul monitoraggio del completamento dell'ultima replica, consulta Monitoraggio dello stato di replica.

Puoi monitorare quando è avvenuta l'ultima sincronizzazione riuscita utilizzando la console, AWS Command Line Interface (AWS CLI), l'API e Amazon CloudWatch. Nel CloudWatch, usa la metrica TimeSinceLastSyncEFS. Per ulteriori informazioni, consulta Monitoraggio dello stato di replica.

## Installazione di un file system di destinazione

Amazon EFS non crea alcun target di montaggio quando crea il file system di destinazione. Per installare un file system di destinazione, devi creare uno o più target di montaggio. Per ulteriori informazioni, consultare Monta il file system utilizzando l'helper di montaggio di EFS

Poiché un file system di destinazione è di sola lettura mentre fa parte di una configurazione di replica, qualsiasi operazione di scrittura su di esso avrà esito negativo. Tuttavia, è possibile utilizzare il file system di destinazione per casi d'uso di sola lettura, inclusi test e sviluppo.

## Failover e failback del file system

In caso di emergenza o quando si eseguono esercitazioni quotidiane, è possibile eseguire il failover sul file system di replica eliminando la configurazione di replica. Dopo l'eliminazione della configurazione di replica, la replica diventa scrivibile ed è possibile iniziare a utilizzarla nel flusso di lavoro dell'applicazione. Quando l'emergenza viene mitigata o l'esercitazione è terminata, è possibile continuare a utilizzare la replica come file system primario o eseguire un failback per riprendere le operazioni sul file system primario originale.

Durante il processo di failback, è possibile scegliere di annullare le modifiche apportate al file system di replica o di conservarle copiandole nuovamente nel file primario.

- Per annullare le modifiche apportate alla replica durante il failover, ricrea la configurazione di replica originale sul file system principale, dove il file system di replica è la destinazione della replica. Durante la replica, Amazon EFS sincronizza i file system aggiornando i dati del file system di replica in modo che corrispondano a quelli del file system principale.
- Per replicare le modifiche apportate alla replica durante il failover, crea una configurazione di replica sul file system della replica, dove il file system primario è la destinazione della replica. Durante la replica, Amazon EFS identifica e trasferisce le differenze dal file system di replica al file system principale. Una volta completata la replica, puoi riprendere a replicare il file system principale ricreando la configurazione di replica originale o creando una nuova configurazione.

Il tempo necessario ad Amazon EFS per completare il processo di replica varia e dipende da fattori quali la dimensione del file system e il numero di file in esso contenuti. Per ulteriori informazioni, consulta Prestazioni.

# Creazione di una configurazione di replica

Puoi utilizzare la console Amazon EFS, l'API o AWS CLI per replicare un file system EFS. Le seguenti sezioni forniscono istruzioni dettagliate per l'utilizzo di ciascuno di questi metodi.

## Creazione di una configurazione di replica (console)

1. Accedi a AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/ec2/.
2. Apri il file system che desideri replicare:
   a. Nel pannello di navigazione a sinistra, scegli File system.
   b. Nell'elenco File system, scegli il file system Amazon EFS che desideri replicare. Non è possibile utilizzare un file system scelto come file system di origine o destinazione in un'altra configurazione di replica esistente.
3. Scegli la scheda Replica, quindi, nella sezione Replica, scegli Create replica. Viene visualizzata la pagina Crea replica.
4. Nella sezione Impostazioni di replica, definisci le impostazioni di replica:
   a. Per la Configurazione di replica, scegli se replicare il file system su un file system nuovo o esistente.
   b. Per Destinazione Regione AWS, scegli Regione AWS in cui replicare il file system.
5. Se stai eseguendo la replica su un nuovo file system di destinazione, nella sezione Impostazioni del file system di destinazione, definisci le impostazioni del file system di destinazione.
   a. Per Tipo di file system, scegli un'opzione di archiviazione per il file system.
      - Scegli Regione AWSRegionale per creare un file system che archivia dati in modo ridondante in più zone di disponibilità geograficamente separate all'interno di .
      - Scegli Zona singola per creare un file system che archivia dati in modo ridondante in una singola zona di disponibilità all'interno di Regione AWS, quindi seleziona la zona di disponibilità.

        Per ulteriori informazioni, consulta Tipi di file system EFS.

        > **Note**
        > I file system a zona singola non sono disponibili in tutte le zone di disponibilità in Regioni AWS dove è disponibile Amazon EFS.

   b. Per la Crittografia, la crittografia dei dati a riposo viene abilitata automaticamente nel file system di destinazione. Per impostazione predefinita, EFS utilizza la tua chiave

di servizio AWS Key Management Service (AWS KMS) per Amazon EFS (`aws/elasticfilesystem`). Per utilizzare una chiave KMS diversa, scegli una chiave KMS o inserisci l'ARN per una chiave esistente.

> **Important**
>
> Dopo aver creato il file system, non è possibile modificare la chiave KMS.

6. Se stai eseguendo la replica su un file system di destinazione esistente, scegli Sfoglia EFS, quindi seleziona il file system. Il percorso del file system di destinazione viene visualizzato nella casella Destinazione.

   Se la protezione da sovrascrittura della replica è abilitata sul file system, viene visualizzato un avviso che richiede di disabilitare la protezione. Per disabilitare la protezione, scegli Disabilita protezione, quindi disattiva la Protezione da sovrascrittura di replica. Dopo aver disabilitato la protezione, fai clic sul pulsante Aggiorna per cancellare il messaggio.

7. Scegli Crea replica. Se si esegue la replica su un nuovo file system, viene visualizzato un messaggio che richiede di confermare la replica. Digita Conferma nella casella di input, quindi fai clic su Crea replica.

   Viene visualizzata la sezione Replica, che mostra i dettagli della replica. Il valore Stato di replica è inizialmente Attivato e Ultima sincronizzazione è vuoto. Dopo che lo stato è impostato su Abilitato, Ultima sincronizzazione mostra Sincronizzazione iniziale in corso.

8. Per visualizzare le informazioni di configurazione del file system di destinazione, scegli l'ID del file system sopra File system di destinazione. La pagina Dettagli del file system per il file system di destinazione viene visualizzata in una nuova scheda del browser (a seconda delle impostazioni del browser).

## Creazione di una configurazione di replica (CLI)

Per creare la configurazione di replica, utilizza il comando CLI `create-replication-configuration`. Il comando API equivalente è CreateReplicationConfiguration.

Example : crea una configurazione di replica per un file system di destinazione regionale

Nell'esempio seguente viene creata una configurazione di replica per il file system *`fs-0123456789abcdef1`*. Questo esempio utilizza il parametro `Region` per creare un file system

di destinazione in *eu-west-2* Regione AWS. Il parametro `KmsKeyId` specifica l'ID della chiave KMS da utilizzare per crittografare il file system di destinazione.

```
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\"}]"
```

Le risposte AWS CLI sono le seguenti:

```
{
    "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 : crea una configurazione di replica per un file system di destinazione a zona singola

Nell'esempio seguente viene creata una configurazione di replica per il file system *fs-0123456789abcdef1*. Questo esempio utilizza il parametro `AvailabilityZoneName` per creare un file system di destinazione a zona singola nella zona di disponibilità *us-west-2a*. Poiché non viene specificata alcuna chiave KMS, il file system di destinazione viene crittografato utilizzando la chiave AWS KMS di servizio predefinita dell'account per Amazon EFS (`aws/elasticfilesystem`).

```
aws efs create-replication-configuration \
--source-file-system-id fs-0123456789abcdef1 \
--destinations AvailabilityZoneName=us-west-2a
```

# Visualizzazione di configurazioni di replica

Per visualizzare la configurazione di replica di un file system, puoi utilizzare la console Amazon EFS o AWS CLI.

## Visualizzazione di una configurazione di replica (console)

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Nel pannello di navigazione a sinistra, scegli File system.
3. Seleziona un file system dall'elenco.
4. Scegli la scheda Replica per visualizzare la sezione Replica.

   Nella sezione Replica, è possibile visualizzare le seguenti informazioni per la configurazione di replica:

   - Lo Stato di replica può essere In attivazione, Attivato, In eliminazione, In pausa, Interrotto o Errore.

     Lo stato Interrotto si verifica a seguito della disattivazione della regione di origine o di destinazione dopo la creazione della configurazione di replica. Per riprendere la replica per la regione, devi attivare nuovamente Regione AWS. Per ulteriori informazioni, consulta Gestione di Regioni AWS nella Guida di riferimento generale di AWS.

     Lo stato In replica si verifica dopo la creazione di una replica, con il file system come file system di origine o di destinazione.

     Lo stato di Errore si verifica quando il file system di origine o di destinazione (o entrambi) si trova in uno stato di errore irreversibile. Per ulteriori informazioni, consulta Monitoraggio dello stato di replica. Per il ripristino, è necessario eliminare la configurazione di replica e ripristinare il backup più recente del file system non riuscito (di origine o di destinazione) su un nuovo file system.
   - La Direzione di replica mostra la direzione in cui i dati vengono replicati. Il primo file system elencato è l'origine e i relativi dati vengono replicati nel secondo file system elencato, che è la destinazione.
   - Ultima sincronizzazione mostra quando è avvenuta l'ultima sincronizzazione riuscita nel file system di destinazione. Tutte le modifiche ai dati sul file system di origine apportate prima di questo periodo sono state replicate correttamente nel file system di destinazione. Qualsiasi modifica apportata dopo questo periodo potrebbe non essere replicata completamente.

- I File system di replica elencano ogni file system nella configurazione di replica in base al relativo ID del file system, al ruolo che ricopre nella configurazione di replica (origine o destinazione), a Regione AWS in cui si trova e alla sua Autorizzazione. Un file system di origine ha l'autorizzazione In scrittura e un file system di destinazione ha l'autorizzazione di Sola lettura.

## Visualizzazione di una configurazione di replica (CLI)

Per visualizzare la configurazione di replica, utilizza il comando CLI `describe-replication-configurations`. È possibile visualizzare la configurazione di replica per un file system specifico o tutte le configurazioni di replica per un particolare Account AWS in Regione AWS. Il comando API equivalente è DescribeReplicationConfigurations.

Per visualizzare la configurazione di replica per un file system, utilizza il parametro di richiesta `file-system-id` URI. È possibile specificare l'ID di un file system di origine o di destinazione.

```
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"
                }
            ]
        }
    ]
}
```

Per visualizzare tutte le configurazioni di replica per un account in Regione AWS, non specificare il parametro `file-system-id`.

```
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
                }
            ]
        }
    ]
```

```
}
```

# Eliminazione di configurazioni di replica

Se devi eseguire il failover sul file system di destinazione, elimina la configurazione di replica di cui è membro. Dopo aver eliminato una configurazione di replica, il file system di destinazione diventa scrivibile e la relativa protezione dalla sovrascrittura della replica viene riattivata. Per ulteriori informazioni, consulta Failover e failback del file system.

L'eliminazione di una configurazione di replica e la modifica del file system di destinazione in modo che sia scrivibile possono richiedere diversi minuti. Dopo l'eliminazione della configurazione, Amazon EFS potrebbe scrivere alcuni dati in una directory `lost+found` nella directory principale del file system di destinazione, utilizzando la seguente convenzione di denominazione:

```
efs-replication-lost+found-source-file-system-id-TIMESTAMP
```

> **Note**
>
> Non è possibile eliminare un file system che fa parte di una configurazione di replica. È necessario eliminare la configurazione di replica prima di eliminare il file system.

Puoi eliminare una configurazione di replica esistente dal file system di origine o di destinazione utilizzando la console, la CLI o l'API.

## Eliminazione di una configurazione di replica (console)

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Nel pannello di navigazione a sinistra, scegli File system.
3. Scegli il file system di origine o quello di destinazione presente nella configurazione di replica che desideri eliminare.
4. Scegli la scheda Replica per visualizzare la sezione Replica.
5. Scegli Elimina replica per eliminare la configurazione di replica. Quando richiesto, conferma la scelta.

### Eliminazione di una configurazione di replica (CLI)

Per eliminare la configurazione di replica, utilizza il comando CLI `delete-replication-configuration`. Il comando API equivalente è DeleteReplicationConfiguration.

Per specificare la configurazione di replica da eliminare, utilizza il parametro `source-file-system-id`.

```
aws efs --region us-west-2 delete-replication-configuration \
--source-file-system-id fs-0123456789abcdef1
```

## Monitoraggio dello stato di replica

È possibile monitorare l'ora in cui è stata completata l'ultima sincronizzazione riuscita in una configurazione di replica. Tutte le modifiche ai dati sul file system di origine apportate prima di questo periodo sono state replicate correttamente nel file system di destinazione. Qualsiasi modifica apportata dopo questo periodo potrebbe non essere replicata completamente. Per monitorare quando l'ultima replica è stata completata correttamente, puoi utilizzare la console, la CLI, l'API o Amazon. CloudWatch

- Nella console: la proprietà Ultima sincronizzazione nella sezione Dettagli del file system > Replica mostra l'ora in cui è stata completata l'ultima sincronizzazione riuscita tra l'origine e la destinazione.
- Nella CLI o nell'API: la proprietà `LastReplicatedTimestamp` nell'oggetto `Destination` mostra l'ora in cui è stata completata l'ultima sincronizzazione riuscita. Per accedere a questa proprietà, utilizza il comando `describe-replication-configurations` CLI. DescribeReplicationConfigurations è l'operazione API equivalente.
- In CloudWatch: la `TimeSinceLastSync` CloudWatch metrica per Amazon EFS mostra il tempo trascorso dal completamento dell'ultima sincronizzazione riuscita. Per ulteriori informazioni, consulta CloudWatch Parametri Amazon per Amazon EFS.

È inoltre possibile monitorare lo stato di una configurazione di replica utilizzando la console, la CLI o l'API. Una configurazione di replica può avere uno dei valori di stato descritti nella tabella qui di seguito.

| Stato di replica | Descrizione |
| --- | --- |
| `ENABLED` | La configurazione di replica è integra ed è disponibile per l'uso. |

| Stato di replica | Descrizione |
| --- | --- |
| ENABLING | Amazon EFS sta creando la configurazione di replica. |
| DELETING | Amazon EFS sta eliminando la configurazione di replica in risposta a una richiesta di eliminazione avviata dall'utente. |
| PAUSING | Amazon EFS è in procinto di sospendere la replica a seguito della disattiva zione della regione per uno o entrambi i file system nella configurazione di replica. |
| PAUSED | La replica viene sospesa seguito della disattivazione della regione per uno o entrambi i file system nella configurazione di replica. Per riprendere la replica, devi attivare nuovamente Regione AWS. Per ulteriori informazioni, consulta Gestione di Regioni AWS nella Guida di riferimento generale di AWS. |
| ERROR | Uno (o entrambi) dei file system nella configurazione di replica si trova in uno stato di errore e non è ripristinabile. Per accedere ai dati del file system, ripristina un backup del file system non riuscito su un nuovo file system. Per ulteriori informazioni, consulta Recupero di un punto di ripristino. |

# Procedure scenari su Amazon Elastic File System

Questa sezione fornisce scenari che è possibile utilizzare per esplorare Amazon EFS e testare il processo completo di configurazione.

Argomenti



## Procedura dettagliata: Creazione di un file system Amazon EFS e montarlo su un'istanza Amazon EC2 utilizzandoAWS CLI

Questa procedura dettagliata utilizza laAWS CLIper esplorare l'API Amazon EFS. In questo schema, verrà creato un file system Amazon EFS crittografato, sarà montato su un'istanza Amazon EC2 nella VPC e sarà testata la configurazione.

> **Note**
>
> Questo scenario è simile all'esercitazione sulle nozioni di base. NellaNozioni di basePer esercizi, si utilizza la console per creare le risorse EC2 e Amazon EFS. In questa procedura dettagliata, si utilizza laAWS CLIPer eseguire le stesse operazioni, principalmente per acquisire familiarità con l'API Amazon EFS.

In questa procedura dettagliata viene creata la seguente procedura dettagliataAWSrisorse presenti nel tuo account:

- Risorse Amazon EC2:
  - Due gruppi di sicurezza (per l'istanza EC2 e per il file system Amazon EFS).

    È possibile aggiungere regole a questi gruppi di sicurezza per autorizzare un accesso in ingresso e in uscita appropriato. Ciò consente all'istanza EC2 di eseguire la connessione al file system tramite la destinazione di montaggio utilizzando una porta TCP NFSv4.1 standard.
  - Un'istanza Amazon EC2 nella VPC.
- Risorse Amazon EFS:
  - Un file system.
  - Una destinazione di montaggio per il file system.

    Per montare il file system su un'istanza EC2 è necessario creare una destinazione di montaggio nella VPC. È possibile creare una destinazione di montaggio in ogni zona di disponibilità nella propria VPC. Per ulteriori informazioni, consultare Amazon EFS: come funziona.

Quindi, si potrà testa il file system sull'istanza EC2. La fase di pulizia alla fine dello scenario fornisce informazioni che consentono di rimuovere queste risorse.

Tutte le risorse dello scenario sono create nella regione Stati Uniti occidentali (Oregon) (Stati Uniti occidentali) (`us-west-2`). Qualunque cosaRegione AWSUtilizzare, assicurarsi di utilizzarlo in maniera sistematica. Tutte le risorse, la VPC, le risorse EC2 e le risorse Amazon EFS, devono risiedere nelle stesse risorseRegione AWS.

## Prima di iniziare

- È possibile utilizzare le credenziali root del tuoAccount AWSPer accedere alla console e provare a seguire l'esercitazione sulle nozioni di base. Tuttavia,AWS Identity and Access Management(IAM) sconsiglia di utilizzare le credenziali root dellaAccount AWS. Al contrario, è necessario creare un utente amministratore nell'account e utilizzare tali credenziali per gestire le risorse nel proprio account. Per ulteriori informazioni, consultare Configurazione.
- È possibile usare una VPC di default o una VPC personalizzata creata all'interno dell'account. Per questo scenario, va bene la configurazione di default della VPC. Tuttavia, se si utilizza una VPC personalizzata, verificare quanto segue:

  - I nomi host DNS sono abilitati. Per ulteriori informazioni, consultare Visualizzazione e aggiornamento del supporto DNS per il VPC nella Guida per l'utente di Amazon VPC.
  - Il gateway Internet è connesso alla VPC. Per ulteriori informazioni, consultare la sezione relativa ai gateway Internet nella Guida per l'utente di Amazon VPC.
  - Le sottoreti della VPC sono configurate per richiedere indirizzi IP pubblici per le istanze avviate nelle sottoreti della VPC. Per ulteriori informazioni, consultare la sezione relativa all'indirizzamento IP nel VPC nella Guida per l'utente di Amazon VPC.
  - La tabella di routing della VPC include una regola per l'invio di tutto il traffico Internet-verso il gateway Internet.
- È necessario configurare la AWS CLI e aggiungere il profilo adminuser.

## Configurazione di AWS CLI

Seguire le seguenti istruzioni per configurare la AWS CLI e il profilo utente.

Per configurare la AWS CLI

1. Scarica e configura AWS CLI. Per le istruzioni, consulta i seguenti argomenti nella Guida per l'utente di AWS Command Line Interface.

   Preparazione della configurazione con l'interfaccia a riga di comando AWS

   Installazione dell'interfaccia a riga di comando di AWS

   Configurazione dell'interfaccia a riga di comando di AWS
2. Impostazione dei profili.

   Le credenziali utente verranno archiviate nel file di configurazione `config` di AWS CLI. I comandi della CLI di esempio in questo scenario specificano il profilo adminuser. Creare il profilo adminuser nel file `config`. È anche possibile impostare il profilo utente amministratore come predefinito nel file `config` come mostrato.

   ```
   [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
```

Anche il profilo precedente imposta il valore predefinitoRegione AWS. Se non si specifica una regione nel comando CLI, viene dato per assunta l'utilizzo della regione us-west-2.

3. Verificare la configurazione digitando i comandi riportati di seguito al prompt dei comandi. Poiché entrambi questi comandi non forniscono credenziali in modo esplicito, vengono utilizzate le credenziali del profilo di default.

   - Provare a utilizzare il comando help

     È anche possibile specificare il profilo utente in modo esplicito aggiungendo il parametro `--profile`.

     ```
     aws help
     ```

     ```
     aws help \
     --profile adminuser
     ```

Approfondimenti

Fase 1: Creazione delle risorse Amazon EC2

# Fase 1: Creazione delle risorse Amazon EC2

In questa fase si effettuano le operazioni seguenti:

- Creare due gruppi di sicurezza.
- Aggiungere le regole ai gruppi di sicurezza per autorizzare un accesso aggiuntivo.
- Avvio di un'istanza EC2. Nella fase successiva si crea e si monta un file system Amazon EFS su questa istanza.

Argomenti

## Fase 1.1: Creazione di due gruppi di sicurezza

In questa sezione, vengono creati dei gruppi di sicurezza nella VPC da associare all'istanza EC2 e alla destinazione di montaggio di Amazon EFS. Successivamente nello schema, questi gruppi di sicurezza saranno assegnati ad un'istanza EC2 e ad una destinazione di montaggio di Amazon EFS. Per informazioni sui gruppi di sicurezza, consulta.Gruppi di sicurezza per EC2-VPCnellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.

Per creare i gruppi di sicurezza

1. Creare due gruppi di sicurezza tramite il comando CLI `create-security-group`:

   a. Creare un gruppo di sicurezza (`efs-walkthrough1-ec2-sg`) per l'istanza EC2 e fornire l'ID 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
   ```

   Annotare l'ID del gruppo di sicurezza. Di seguito è riportata una risposta di esempio.

   ```
   {
       "GroupId": "sg-aexample"
   }
   ```

   È possibile trovare l'ID VPC utilizzando il seguente comando.

   ```
   $ aws  ec2 describe-vpcs
   ```

   b. Creazione di un gruppo di sicurezza (`efs-walkthrough1-mt-sg`) per il tuo target di montaggio Amazon EFS. È necessario fornire l'ID della 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
```

Annotare l'ID del gruppo di sicurezza. Di seguito è riportata una risposta di esempio.

```
{
    "GroupId": "sg-aexample"
}
```

2. Verifica dei gruppi di sicurezza.

```
aws ec2 describe-security-groups \
--group-ids list of security group IDs separated by space \
--profile adminuser \
--region us-west-2
```

Entrambi i gruppi di sicurezza dovrebbero avere solo una regola in uscita che consenta l'uscita di tutto il traffico.

Nella sezione successiva è necessario autorizzare un accesso aggiuntivo che consenta quanto segue:

- Permetta di connettersi all'istanza EC2.
- Abilitare il traffico tra un'istanza EC2 e una destinazione di montaggio Amazon EFS (alla quale saranno associati questi gruppi di sicurezza più tardi in questo schema).

## Fase 1.2: Aggiungere le regole ai gruppi di sicurezza per autorizzare l'accesso in ingresso/uscita

In questa fase sia aggiungono le regole ai gruppi di sicurezza per autorizzare un accesso in ingresso/uscita.

Per aggiungere le regole

1. Autorizzare le connessioni SSH (Secure Shell) in entrata nel gruppo di sicurezza dell'istanza EC2 (`efs-walkthrough1-ec2-sg`) in modo da potersi connettere all'istanza EC2 utilizzando SSH da qualsiasi 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
```

Verificare che il gruppo di sicurezza includa la regola in ingresso e in uscita che è stata aggiunta.

```
aws ec2 describe-security-groups \
--region us-west-2 \
--profile adminuser \
--group-id security-group-id
```

2. Autorizzare l'accesso in ingresso al gruppo di sicurezza della destinazione di montaggio Amazon EFS (`efs-walkthrough1-mt-sg`).

   Nel prompt dei comandi, eseguire il seguente comando AWS CLI `authorize-security-group-ingress` utilizzando il profilo adminuser per aggiungere la regola in ingresso.

```
$ 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. Verificare che entrambi i gruppi di sicurezza autorizzino l'accesso in ingresso.

```
aws ec2 describe-security-groups \
--group-names efs-walkthrough1-ec2-sg   efs-walkthrough1-mt-sg \
--profile adminuser \
--region us-west-2
```

## Fase 1.3: Avvio di un'istanza EC2

In questa fase, avviare un'istanza EC2.

Per avviare un'istanza EC2

1. Raccogliere le seguenti informazioni necessarie quando si avvia un'istanza EC2:

- Nome della coppia di chiavi
  - Per informazioni generali, consulta.Impostazione di Amazon EC2nellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.
  - Per istruzioni su come creare un file .pem, consultaCrea una coppia di chiavinellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.
- L'ID dell'Amazon Machine Image (AMI) che si desidera avviare.

  Il comando AWS CLI utilizzato per avviare un'istanza EC2 richiede l'ID dell'AMI che si desidera distribuire come parametro. L'esercitazione utilizza l'AMI Amazon Linux HVM.

  > **Note**
  >
  > È possibile utilizzare la maggior parte delle AMI Linux per uso generale. Se si utilizza un'altra AMI Linux, è necessario assicurarsi di utilizzare lo strumento di gestione del pacchetto responsabile della distribuzione per installare il client NFS sull'istanza. Inoltre, è possibile aggiungere pacchetti software quando se ne ha bisogno.

  Per quanto riguarda l'AMI Amazon Linux HVM, è possibile trovare gli ultimi ID su Amazon Linux AMI. È possibile scegliere il valore dell'ID dalla seguente tabella degli ID delle AMI Amazon Linux:
  - Scegli la regione US West Oregon (Stati Uniti occidentali Oregon). Questo scenario presuppone la creazione di tutte le risorse nella regione Stati Uniti occidentali (Oregon) (us-west-2).
  - Scegliere il tipo EBS-backed HVM 64-bit (perché nel comando CLI si specifica il tipo di istanza `t2.micro` che non supporta l'instance store).
- ID del gruppo di sicurezza creato per l'istanza EC2.
- Regione AWS. Questo scenario è basato sulla regione us-west-2.
- L'ID della sottorete della VPC all'interno della quale si desidera avviare l'istanza. È possibile ottenere un elenco delle sottoreti utilizzando il comando `describe-subnets`.

```
$ aws ec2 describe-subnets \
--region us-west-2 \
--filters "Name=vpc-id,Values=vpc-id" \
```

```
--profile adminuser
```

Dopo aver scelto l'ID della sottorete, annotare i seguenti valori del risultato di `describe-subnets`:

- ID sottoreteQuesto valore è necessario per la creazione della destinazione di montaggio. In questa esercitazione, si crea una destinazione di montaggio nella stessa sottorete in cui si avvia l'istanza EC2.
- Zona di disponibilità della sottorete— Questo valore è necessario per il costruire il nome DNS della destinazione di montaggio, che viene usato per montare un file system sull'istanza EC2.

2. Eseguire il seguente comando AWS CLI `run-instances` per avviare un'istanza 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. Annotare l'ID dell'istanza ritornato dal comando `run-instances`.
4. L'istanza EC2 creata deve disporre di un nome DNS pubblico da utilizzare per connettersi all'istanza EC2 e montare il file system su di essa. Il nome DNS pubblico assume il formato:

```
ec2-xx-xx-xx-xxx.compute-1.amazonaws.com
```

Eseguire i seguenti comandi CLI e annotare il nome DNS pubblico.

```
aws ec2 describe-instances \
--instance-ids EC2 instance ID \
--region us-west-2 \
--profile adminuser
```

Se non si trova il nome DNS pubblico, controllare la configurazione della VPC in cui è stata avviata l'istanza EC2. Per ulteriori informazioni, consultare Prima di iniziare.

5. (Opzionale) Assegnare un nome all'istanza EC2 creata. A tale scopo, aggiungere un tag con il nome della chiave e il valore impostato sul nome che si desidera assegnare all'istanza. A tale scopo, eseguire questo comando `create-tags` AWS CLI:

```
$  aws ec2 create-tags \
--resources  EC2-instance-ID \
--tags Key=Name,Value=Provide-instance-name  \
--region us-west-2 \
--profile adminuser
```

Approfondimenti

Fase 2: Creazione delle risorse Amazon EFS

# Fase 2: Creazione delle risorse Amazon EFS

In questa fase si effettuano le operazioni seguenti:

- Creazione di un file system Amazon EFS crittografato.
- Abilitare la gestione del ciclo di vita.
- Creare una destinazione di montaggio nella zona di disponibilità in cui è stata avviata l'istanza EC2.

Argomenti



## Fase 2.1: Creare un file system Amazon EFS

In questa fase, viene creato un file system Amazon EFS. Annotare il `FileSystemId` da utilizzare nella fase successiva durante la creazione delle destinazioni di montaggio del file system.

Per creare un file system

- Creare un file system con il tag facoltativo `Name`.

a. Dal prompt dei comandi, eseguire le operazioni seguenti:AWSCLI`create-file-system`comando.

```
$  aws efs create-file-system \
--encrypted \
--creation-token FileSystemForWalkthrough1 \
--tags Key=Name,Value=SomeExampleNameValue \
--region us-west-2 \
--profile adminuser
```

Si ottiene la risposta seguente.

```
{
    "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. Annotare il valore `FileSystemId`. Questo valore è necessario durante la creazione di una destinazione di montaggio per questo file system in Fase 2.3: Crea un target di montaggio.

## Fase 2.2: Abilitare la gestione del ciclo di vita

In questa fase, abilitare la gestione del ciclo di vita per il file system in modo da utilizzare la classe di storage Accesso non frequente. Per ulteriori informazioni, consultare Gestione dello storage del file system e Classi di storage EFS.

Come abilitare la gestione del ciclo di vita

- Nel prompt dei comandi, eseguire il seguente comando AWS CLI `put-lifecycle-configuration`.

```
$  aws efs put-lifecycle-configuration \
--file-system-id fs-c657c8bf \
--lifecycle-policies TransitionToIA=AFTER_30_DAYS \
--region us-west-2 \
--profile adminuser
```

Si ottiene la risposta seguente.

```
{
  "LifecyclePolicies": [
    {
        "TransitionToIA": "AFTER_30_DAYS"
    }
  ]
}
```

## Fase 2.3: Crea un target di montaggio

In questa fase, si crea una destinazione di montaggio per il file system nella zona di disponibilità in cui è stata avviata l'istanza EC2.

1. Assicurarsi di disporre delle informazioni riportate qui di seguito:
   - L'ID del file system (ad esempio, `fs-example`) per il quale si sta creando la destinazione di montaggio.
   - L'ID della sottorete della VPC in cui è stata avviata l'istanza EC2 nella Fase 1.

Per questo scenario, è necessario creare la destinazione di montaggio nella stessa sottorete in cui è stata avviata l'istanza EC2, pertanto è necessario disporre dell'ID della sottorete (ad esempio, `subnet-example`).

- L'ID del gruppo di sicurezza creato per la destinazione di montaggio nella fase precedente.

2. Nel prompt dei comandi, eseguire il seguente comando AWS CLI `create-mount-target`.

```
$ 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
```

Si ottiene la risposta seguente.

```
{
    "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. È inoltre possibile utilizzare il comando `describe-mount-targets` per ottenere le descrizioni delle destinazioni di montaggio create su un file system.

```
$ aws efs describe-mount-targets \
--file-system-id file-system-id \
--region us-west-2 \
--profile adminuser
```

Approfondimenti

[Fase 3: Montare il file system sull'istanza EC2 e testare]

# Fase 3: Montare il file system sull'istanza EC2 e testare

In questa fase si effettuano le operazioni seguenti:

Argomenti



## Fase 3.1: Raccolta delle informazioni

Assicurarsi di disporre delle seguenti informazioni per procedere con le fasi di questa sezione:

- Nome DNS pubblico dell'istanza EC2 nel formato seguente:

  ```
  ec2-xx-xxx-xxx-xx.aws-region.compute.amazonaws.com
  ```

- Nome DNS del file system. È possibile costruire questo nome DNS utilizzando il seguente formato generico:

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

  L'istanza EC2 su cui montare il file system attraverso la destinazione di montaggio è in grado di risolvere il nome DNS del file system per ricavare l'indirizzo IP della destinazione di montaggio.

> **Note**
>
> Amazon EFS non richiede che l'istanza Amazon EC2 disponga di un indirizzo IP pubblico né di un nome DNS pubblico. I requisiti elencati in precedenza sono limitati a questo scenario di esempio per garantire che sia possibile connettersi all'istanza tramite SSH dall'esterno del VPC.

## Fase 3.2: Installa il client NFS sull'istanza EC2

È possibile connettersi all'istanza EC2 da Windows o da un computer che esegue Linux o Mac OS X o qualsiasi altra variante Unix.

Per installare un client NFS

1. Connettiti all'istanza EC2:

   - Per connettersi all'istanza da un computer che esegue Mac OS o Linux, è necessario specificare il file .pem per il comando SSH con l'opzione `-i` e il percorso della chiave privata.
   - Per connettersi all'istanza da un computer che esegue Windows, è possibile usare MindTerm o PuTTY. Se si prevede di usare PuTTY, è necessario installarlo e usare la procedura seguente per convertire il file .pem in un file .ppk.

   Per ulteriori informazioni, consulta gli argomenti seguenti nellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux:

   - Connessione all'istanza Linux da Windows tramite PuTTY
   - Connessione all'istanza Linux tramite SSH
2. Eseguire i seguenti comandi sull'istanza EC2 tramite la sessione SSH:

   a. (Facoltativo) Scaricare gli aggiornamenti e riavviare.

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

   Riconnettersi all'istanza EC2 dopo averla riavviata.

   b. Installare il client NFS.

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

   > **Note**
   >
   > Se scegli laAMI Amazon Linux 2016.03.0AMI Amazon Linux quando si avvia l'istanza Amazon EC2, non è necessario eseguire l'installazione`nfs-utils`perché è già incluso nell'AMI per impostazione predefinita.

## Fase 3.3: Montare il file system sull'istanza EC2 e testare

Ora è possibile montare il file system sull'istanza EC2.

1. Creare una cartella ("efs-mount-point").

```
$ mkdir ~/efs-mount-point
```

2. Montare il file system Amazon EFS.

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

L'istanza EC2 è in grado di risolvere il nome DNS della destinazione di montaggio per ricavare l'indirizzo IP. È possibile specificare direttamente l'indirizzo IP della destinazione di montaggio.

```
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-ip:/  ~/efs-mount-point
```

3. Dopo aver montato il file system Amazon EFS sull'istanza EC2, è possibile creare i file.

   a. Cambiare la cartella di lavoro.

```
$ cd ~/efs-mount-point
```

   b. Elencare i contenuti della cartella.

```
$ ls -al
```

   Dovrebbe essere vuota.

```
drwxr-xr-x 2 root     root     4096 Dec 29 22:33 .
drwx------ 4 ec2-user ec2-user 4096 Dec 29 22:54 ..
```

   c. La cartella principale di un file system, al momento della creazione, è di proprietà ed è scrivibile da parte dell'utente root quindi, per poter aggiungere dei file, è necessario modificare le autorizzazioni.

```
$ sudo chmod go+rw .
```

Ora, se si esegue il comando `ls -al` è possibile notare che le autorizzazioni sono cambiate.

```
drwxrwxrwx 2 root     root     4096 Dec 29 22:33 .
drwx------ 4 ec2-user ec2-user 4096 Dec 29 22:54 ..
```

d. Creare un file di testo .

```
$ touch test-file.txt
```

e. Elencare i contenuti della cartella.

```
$ ls -l
```

A questo punto un file system Amazon EFS è stato creato e montato correttamente sull'istanza EC2 nella VPC.

Il file system montato non rimane persistente in caso di riavvio. Per rimontare automaticamente la directory, è possibile utilizzare il file `fstab`. Per ulteriori informazioni, consultare Rimontaggio automatico al riavvio. Se si sta usando un gruppo Auto Scaling per avviare le istanze EC2, è anche possibile impostare gli script in una configurazione di avvio. Per un esempio, consultare Procedura dettagliata: configurazione di un server Web Apache e sulla connessione dei file Amazon EFS.

Approfondimenti

Fase 4: Elimina

## Fase 4: Elimina

Se le risorse create non sono più necessarie, dovrebbero essere eliminate. È possibile farlo tramite la CLI.

- Eliminare le risorse EC2 (l'istanza EC2 e i due gruppi di sicurezza). Quando si elimina la destinazione di montaggio, Amazon EFS elimina l'interfaccia di rete.
- Eliminare le risorse Amazon EFS (file system, destinazione di montaggio).

Per eliminareAWSrisorse create in questa procedura dettagliata

1. Terminare l'istanza EC2 creata per questo scenario.

   ```
   $ aws ec2 terminate-instances \
   --instance-ids instance-id \
   --profile adminuser
   ```

   È possibile eliminare le risorse EC2 anche utilizzando la console. Per istruzioni, consultaCessazione di un'istanzanellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.

2. Eliminare la destinazione di montaggio.

   Prima di eliminare il file system, è necessario eliminare la destinazione di montaggio creata per il file system. È possibile ottenere un elenco delle destinazioni di montaggio utilizzando il comando CLI `describe-mount-targets`.

   ```
   $  aws efs describe-mount-targets \
   --file-system-id file-system-ID \
   --profile adminuser \
   --region aws-region
   ```

   Quindi è possibile eliminare la destinazione di montaggio utilizzando il comando CLI `delete-mount-target`.

   ```
   $ aws efs delete-mount-target \
   --mount-target-id ID-of-mount-target-to-delete \
   --profile adminuser \
   --region aws-region
   ```

3. (Facoltativo) Eliminare i due gruppi di sicurezza creati. La creazione dei gruppi di sicurezza non ha costo.

   Prima di eliminare il gruppo di sicurezza dell'istanza EC2, è necessario eliminare il gruppo di sicurezza della destinazione di montaggio. Il gruppo di sicurezza della destinazione di montaggio include una regola che fa riferimento al gruppo di sicurezza dell'istanza EC2. Pertanto, non è possibile eliminare per primo il gruppo di sicurezza dell'istanza EC2.

Per istruzioni, consultaEliminazione di un gruppo di sicurezzanellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.

4. Eliminare il file system utilizzando il comando CLI `delete-file-system`. È possibile ottenere un elenco dei file system utilizzando il comando CLI `describe-file-systems`. È possibile ricavare l'ID del file system dalla risposta.

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

Eliminare il file system fornendo l'ID del file system.

```
$ aws efs delete-file-system \
--file-system-id ID-of-file-system-to-delete \
--region aws-region \
--profile adminuser
```

# Procedura dettagliata: configurazione di un server Web Apache e sulla connessione dei file Amazon EFS

Puoi fare in modo che le istanze EC2 eseguano il server web Apache che servano i file archiviati nel tuo file system Amazon EFS. Può trattarsi di un'istanza EC2 o, se la tua applicazione ne ha bisogno, puoi avere più istanze EC2 che servono file dal tuo file system Amazon EFS. Sono descritte le seguenti procedure.

- Configurazione di un server Web Apache su un'istanza &EC2.
- Impostazione di un server Web Apache su più istanze di EC2 mediante la creazione di un gruppo auto scaling. Puoi creare più istanze EC2 utilizzando Amazon EC2 Auto Scaling, unAWS servizio che consente di aumentare o diminuire il numero di istanze EC2 in un gruppo in base alle esigenze dell'applicazione. Quando si dispone di più server Web, è inoltre necessario disporre di un sistema di bilanciamento del carico per distribuire il traffico delle richieste tra di essi.

> **Note**
>
> Per entrambe le istanze, vengono create tutte le risorse nella regione Stati Uniti occidentali (Oregonus-west-2).

## File che servono file a singola istanza EC2

Segui i passaggi per configurare un server Web Apache su un'istanza EC2 per servire i file che crei nel tuo file system Amazon EFS.

1. Seguire le istruzioni dell'esercitazione sulle nozioni di base per disporre di una configurazione funzionante costituita dai seguenti elementi:

   - File system Amazon EFS
   - Istanza EC2
   - File system montato sull'istanza EC2

   Per istruzioni, consulta Guida introduttiva ad Amazon Elastic File System. Durante lo svolgimento della procedura, prendere nota di quanto segue:

   - Il nome pubblico sul DNS dell'istanza EC2.
   - Il nome pubblico sul DNS della destinazione di montaggio creata nella stessa zona di disponibilità in cui è stata avviata l'istanza EC2.
2. (Facoltativo), È possibile scegliere di smontare il file system dal punto di montaggio creato nell'esercitazione sulle nozioni di base.

   ```
   $ sudo umount  ~/efs-mount-point
   ```

   In questo scenario, viene creato un altro punto di montaggio per il file system.
3. Nell'istanza EC2, installare il server Web Apache e configurarlo come segue:

   a. Collegarsi all'istanza EC2 e installare il server Web Apache.

      ```
      $ sudo yum -y install httpd
      ```

   b. Avviare il servizio.

```
$ sudo service httpd start
```

c. Creare un punto di montaggio.

   In primo luogo notiamo che `DocumentRoot` nel file `/etc/httpd/conf/httpd.conf` punta a `/var/www/html` (`DocumentRoot "/var/www/html"`).

   Monterai il tuo file system Amazon EFS su una sottodirectory sotto la radice del documento.

   Crea una sottodirectory denominata`efs-mount-point` da utilizzare come punto di montaggio per il tuo file system, sotto`/var/www/html`.

```
$ sudo mkdir /var/www/html/efs-mount-point
```

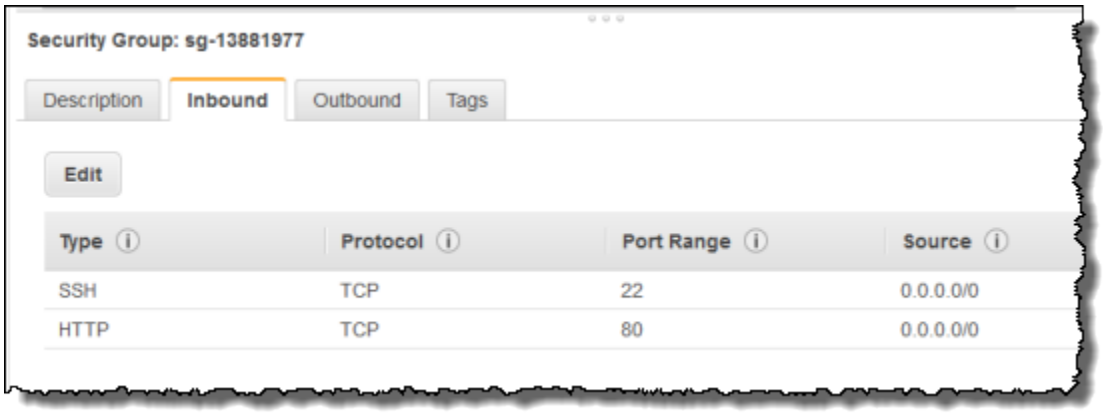
d. Monta il tuo file system Amazon EFS utilizzando il seguente comando. sostituiscilo`file-system-id` con l'ID del tuo file system.

```
$ sudo mount -t efs file-system-id:/ /var/www/html/efs-mount-point
```

4. Testare l'impostazione.

a. Aggiungere una regola al gruppo di sicurezza dell'istanza EC2, creato nell'esercitazione sulle nozioni di base, per autorizzare il traffico HTTP sulla porta TCP 80 proveniente da qualunque origine.

   Dopo aver aggiunto la regola, il gruppo di sicurezza dell'istanza EC2 avrà le seguenti regole in entrata.




   Per istruzioni, consulta Creazione di gruppi di sicurezza tramite AWS Management Console.

b. Creare un file html di esempio.

i. Cambia cartella in base al punto di montaggio.

```
$ cd /var/www/html/efs-mount-point
```

ii. Crea una sottodirectory chiamata`sampledir` e modifica la proprietà.

```
$  sudo mkdir sampledir
$  sudo chown  ec2-user sampledir
$  sudo chmod -R o+r sampledir
```

Cambia cartella in modo da poter creare file nella`sampledir` sottodirectory.

```
$  cd sampledir
```

iii. Creare un file `hello.html` di esempio.

```
$ echo "<html><h1>Hello from Amazon EFS</h1></html>" > hello.html
```

c. Aprire una finestra del browser e immettere l'URL per accedere al file (è il nome pubblico sul DNS dell'istanza EC2 seguito dal nome file). Ad esempio:

```
http://EC2-instance-public-DNS/efs-mount-point/sampledir/hello.html
```

Ora stai servendo pagine Web archiviate in un file Amazon EFS.

> **Note**
>
> Questa configurazione non configura l'istanza EC2 per avviare automaticamente il server Web (httpd) all'avvio e inoltre non monta il file system all'avvio. Nel prossimo scenario, verrà creata una configurazione per impostare tali aspetti.

## Più istanze EC2 che servono file

Segui i passaggi per distribuire gli stessi contenuti nel tuo file system Amazon EFS da più istanze EC2 per migliorare la scalabilità o la disponibilità.

1. Segui i passaggi dell'Fase 1: Creazione di un file system Amazon EFSesercizio in modo da creare e testare un file system Amazon EFS.

   > **Important**
   >
   > Per questo scenario, non si utilizza l'istanza EC2 creata nell'esercitazione sulle nozioni di base. Al contrario, è necessario avviare delle nuove istanze EC2.

2. Creare un sistema di bilanciamento del carico nella VPC utilizzando la procedura seguente.

   a. Definire un sistema di bilanciamento del carico

      Nella sezione Basic Configuration (Configurazione di base), selezionare la VPC dove è anche possibile creare le istanze EC2 su cui montare il file system.

      Nella sezione Seleziona sottoreti, seleziona tutte le sottoreti disponibili. Per ulteriori dettagli, consultare lo script `cloud-config` nella sezione successiva.

   b. Assegnare i gruppi di sicurezza

      Creare un nuovo gruppo di sicurezza per il sistema di bilanciamento del carico per consentire l'accesso HTTP alla porta 80 da qualunque origine, come illustrato qui di seguito:

      - Type (Tipo): HTTP
      - Protocol (Protocollo): TCP
      - Port Range (Intervallo porte: 80
      - Origine: Qualsiasi (0.0.0.0/0)

      > **Note**
      >
      > Quando tutto funziona, è anche possibile aggiornare la regola in ingresso del gruppo di sicurezza delle istanze EC2 per consentire la ricezione del solo traffico HTTP originato dal sistema di bilanciamento del carico.

   c. Configurare un controllo dello stato

      Impostare il valore Ping Path a `/efs-mount-point/test.html`. `efs-mount-point` è la sottocartella sulla quale è stato montato il file system. In questa procedura è possibile aggiungere la pagina `test.html` in un secondo momento.

> **Note**
>
> Non aggiungere nessuna istanza EC2. Successivamente, è necessario creare un gruppo auto scaling all'interno del quale avviare l'istanza EC2 e specificare questo sistema di bilanciamento del carico.

Per informazioni sulla creazione di un sistema di bilanciamento del carico, consulta Nozioni di base con Elastic Load Balancer nella Guida per l'utente di Elastic Load Balancing Balancer.

Creare un gruppo auto scaling con due istanze EC2. In primo luogo, è necessario creare una configurazione di avvio che descriva le istanze. Quindi, creare un gruppo auto scaling specificando la configurazione di avvio. I passaggi seguenti forniscono informazioni sulla configurazione che viene specificato per creare un gruppo Auto Scaling dalla console Amazon EC2.

1. Nel riquadro di navigazione sinistro, sotto Launch Configurations (Configurazioni di avvio), scegliere AUTO SCALING.
2. Scegliere Create Auto Scaling group (Crea gruppo auto scaling) per avviare la procedura guidata.
3. Scegli Create launch configuration (Crea configurazione di avvio).
4. Da Quick Start, seleziona la versione più recente dell'AMI Amazon Linux 2. È la stessa AMI utilizzata in Fase 2: Creazione delle risorse EC2 e avvio dell'istanza EC2 dell'esercitazione sulle nozioni di base.
5. Nella sezione Advanced (Avanzate), eseguire le seguenti operazioni:

   - Come IP Address Type (Tipo indirizzo IP), scegliere Assign a public IP address to every instance (Assegna un indirizzo IP pubblico a ogni istanza).
   - Copiare/incollare i seguenti script nella casella User data (Dati utente).

     È necessario aggiornare lo script fornendo i valori per la regione *`file-system-id`*e *`aws-region`* (se avete seguito l'esercizio Getting Started, avete creato il file system nella regione us-west-2).

     Nello script, tenere presente quanto segue:

     - Lo script installa il client NFS e il server Web Apache.

- Il comando echo inserisce la voce seguente nel file `/etc/fstab` indicando il nome sul DNS del file system e la sottocartella sulla quale montarlo. Questa voce garantisce che il file system venga montato dopo ogni riavvio del sistema. Si noti che il nome sul DNS del file system viene costruito in modo dinamico. Per ulteriori informazioni, consulta Montaggio su Amazon EC2 con un nome DNS.

  ```
  file-system-ID.efs.aws-region.amazonaws.com:/ /var/www/html/efs-mount-point
   nfs4   defaults
  ```

- Crea una`efs-mount-point` sottodirectory e monta il file system su di essa.
- Crea una`test.html` pagina in modo che ELB health check possa trovare il file (durante la creazione di un load balancer avete specificato questo file come punto di ping).

Per ulteriori informazioni sugli script relativi ai dati utente, consulta Aggiungere dati utente nella Guida per l'utente di Amazon EC2 per le istanze Linux.

```
#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. In Assign a security group (Assegna un gruppo di sicurezza), scegliere Select an existing security group (Seleziona un gruppo di sicurezza esistente) e quindi scegliere il gruppo di sicurezza creato per l'istanza EC2.
7. Ora, configurazione dei dettagli del gruppo Auto Scaling utilizzando le informazioni seguenti.

   a. Per Group size (Dimensione gruppo), scegliere **`Start with 2 instances`**. Saranno così create due istanze EC2.

   b. Selezionare la VPC dall'elenco Network (Rete).

c. Selezionare una sottorete nella stessa zona di disponibilità utilizzato nella specifica dell'ID della destinazione di montaggio nello script User Data alla creazione della configurazione di avvio durante la fase precedente.

d. Nella sezione Dettagli avanzati

i. In Load Balancing, scegliere Receive traffic from Elastic Load Balancer(s) (Ricevi traffico da Elastic Load Balancer), quindi selezionare il sistema di bilanciamento del carico creato per questa esercitazione.

ii. In Health Check Type (Tipo di controllo di stato), scegliere ELB.

8. Segui le istruzioni per creare un gruppo Auto Scaling nella sezione Configurazione di un'applicazione scalata e con bilanciamento del carico nella Guida per l'utente di Amazon EC2 Auto Scaling. Utilizzare le informazioni nelle tabelle precedenti, ove applicabile.

9. Una volta completata la creazione del gruppo auto scaling, si disporrà di due istanze EC2 con `nfs-utils` e il server Web Apache installato. In ogni istanza, verifica di avere la`/var/www/html/efs-mount-point` sottodirectory su cui è montato il file system Amazon EFS. Per ulteriori informazioni sulla Connect all'istanza Linux, consulta Connessione all'istanza Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.

> **Note**
>
> Se scegli l'AMI Amazon Linux 2016.03.0 Amazon Linux all'avvio dell'istanza Amazon EC2, non dovrai installarlan`fs-utils` perché è già inclusa nell'AMI per impostazione predefinita.

10. Creazione di una pagina di esempio (index.html).

a. Cambiare la cartella.

```
$ cd /var/www/html/efs-mount-point
```

b. Creare una sottocartella `sampledir` e modificarne la proprietà. E modificare la cartella in modo da poter creare dei file nella sottocartella `sampledir`. Se sono state seguire le indicazioni fornite in precedenza File che servono file a singola istanza EC2, la cartella `sampledir` è già stata creata, perciò è possibile ignorare questo passaggio.

```
$  sudo mkdir sampledir
$  sudo chown  ec2-user sampledir
$  sudo chmod -R o+r sampledir
```

```
$  cd sampledir
```

c. Creare un file `index.html` di esempio.

```
$ echo "<html><h1>Hello from Amazon EFS</h1></html>" > index.html
```

11. A questo punto è possibile eseguire il test della configurazione. Utilizzo del nome pubblico sul DNS del sistema di bilanciamento del carico, accesso alla pagina index.html.

```
http://load balancer public DNS Name/efs-mount-point/sampledir/index.html
```

Il sistema di bilanciamento del carico invia una richiesta a una delle istanze EC2 su cui è in esecuzione il server Web Apache. Quindi, il server Web serve il file archiviato nel file system Amazon EFS.

## Scenario: creazione di sottocartelle con possibilità di scrittura per gli utenti e configurazione del montaggio automatico al riavvio

Dopo aver creato un file system Amazon EFS e averlo montato localmente sull'istanza EC2, viene esposta una directory vuota chiamata *file system root*. Un caso di utilizzo comune è creare una sottocartella "scrivibile" all'interno di questa radice del file system per ogni utente creato sull'istanza di EC2 e montarla sulla cartella principale dell'utente. Tutti i file e le sottodirectory che l'utente crea nella propria home directory vengono quindi creati nel file system Amazon EFS.

In questo scenario, si crea prima di tutto un utente "mike" sull'istanza EC2. Quindi si monta una sottodirectory Amazon EFS nella home directory dell'utente mike. Lo scenario spiega inoltre come configurare il montaggio automatico delle sottocartelle al riavvio del sistema.

Supponiamo che tu abbia un file system Amazon EFS creato e montato su una directory locale della tua istanza EC2. Chiamiamolo *EFSroot*

> **Note**
>
> Puoi seguire l'Nozioni di baseesercizio per creare e montare un file system Amazon EFS su un'istanza EC2.

Nei passaggi seguenti, si crea un utente (mike), si crea una sottodirectory per l'utente (*EFSRoot*/mike), si rende l'utente mike il proprietario della sottodirectory, concedendogli le autorizzazioni complete e infine si monta la sottodirectory Amazon EFS nella home directory dell'utente (/home/mike).

1. Creazione dell'utente mike:

   - Accesso all'istanza EC2. Utilizzando i privilegi di root (in questo caso, utilizzando il comando sudo), creare l'utente mike e assegnargli una password.

     ```
     $ sudo useradd -c "Mike Smith" mike
     $ sudo passwd mike
     ```

     Questa operazione crea anche una cartella principale /home/mike per l'utente.

2. Creare una sottocartella in *EFSroot* per l'utente mike:

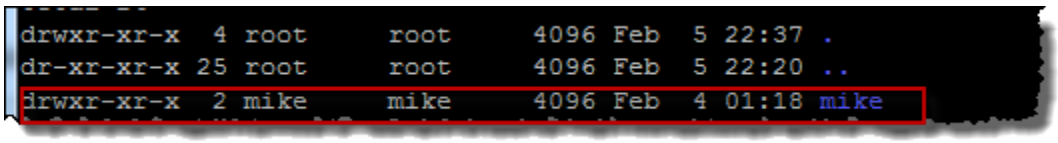
   a. Creare una sottocartella mike sotto *EFSroot*.

      ```
      $  sudo mkdir /EFSroot/mike
      ```

      È necessario sostituire *EFSroot* con il nome della cartella locale.

   b. L'utente root e il gruppo root sono proprietari della sottocartella /mike (è possibile verificarlo utilizzando il comando ls -l). Per abilitare tutte le autorizzazioni per l'utente mike in questa sottocartella, assegnare a mike la proprietà della cartella.

      ```
      $ sudo chown mike:mike /EFSroot/mike
      ```

3. Utilizzare il comando mount per montare la sottocartella *EFSroot*/mike nella cartella principale di mike.

   ```
   $  sudo mount -t nfs -o
    nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-DNS:/mike  /home/mike
   ```

L'indirizzo *Mount-target-DNS* identifica la radice del file system Amazon EFS remoto.

Ora la home directory dell'utente mike è una sottodirectory, scrivibile da mike, nel file system Amazon EFS. Se si smonta questa destinazione di montaggio, l'utente non è in grado di accedere alla propria cartella EFS senza il rimontaggio, che richiede le autorizzazioni di root.

### Rimontaggio automatico al riavvio

Per rimontare automaticamente il file system dopo un riavvio del sistema, è possibile utilizzare il file `fstab`. Per ulteriori informazioni, consulta Montaggio automatico del file system Amazon EFS.

## Procedura dettagliata: creare e montare un file system in locale con una VPN AWS Direct Connect

In questo scenario si utilizza la AWS Management Console per creare e montare un file system su un client locale. Lo fai utilizzando una AWS Direct Connect connessione o una connessione su un AWS Virtual Private Network (). AWS VPN

> **Note**
>
> L'utilizzo di Amazon EFS con client basati su Microsoft Windows non è supportato.

Argomenti

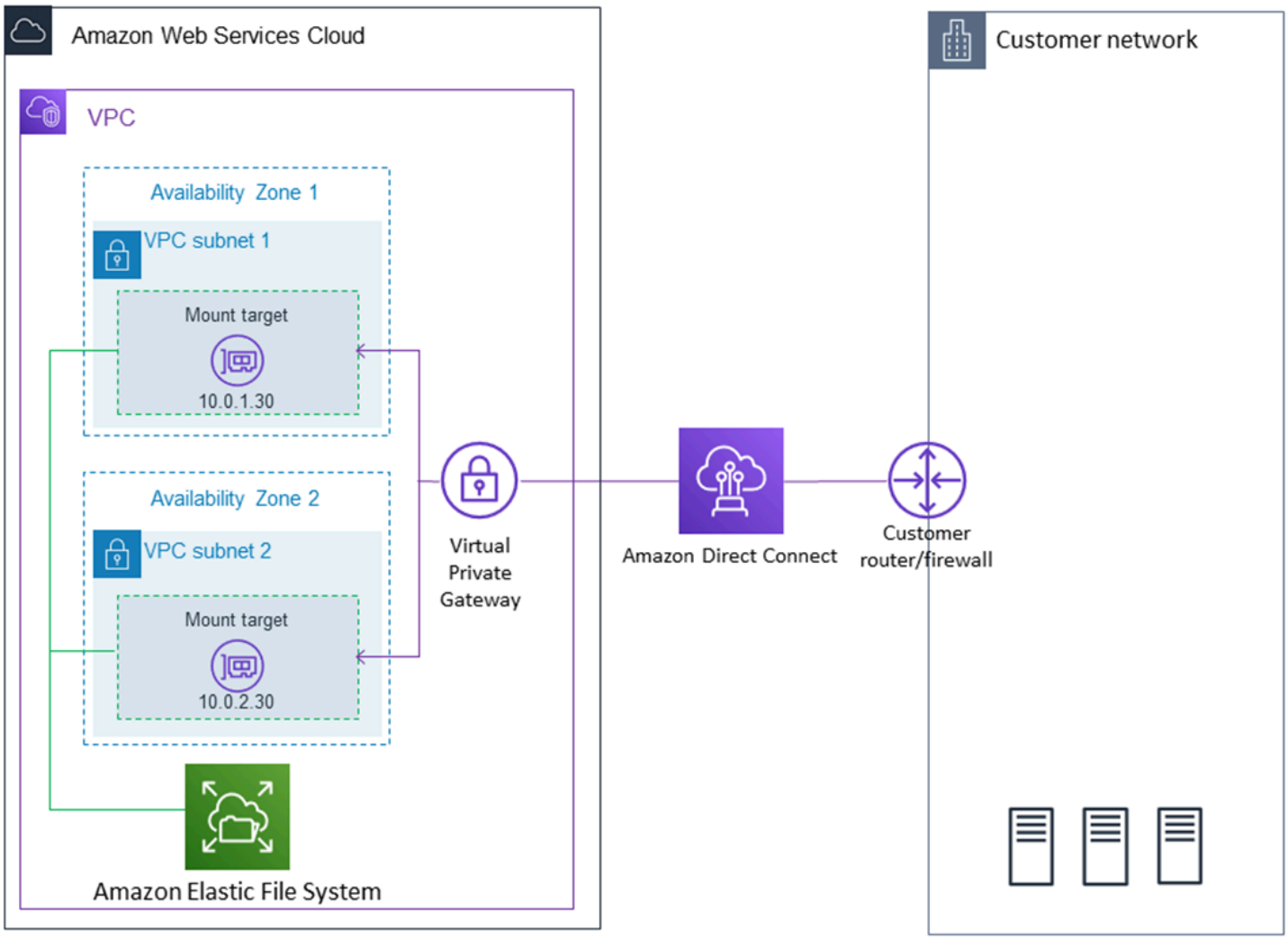
- Prima di iniziare
- Fase 1: crea le tue risorse Amazon Elastic File System
- Passaggio 2: installa il client NFS
- Fase 3: installa il file system Amazon EFS sul tuo client locale
- Fase 4: Pulisci le risorse e proteggi il tuo AWS account
- Facoltativo: crittografia dei dati in transito

In questo scenario, supponiamo che si disponga già di una connessione AWS Direct Connect o VPN. Se non si dispone di tale connessione, è possibile avviare subito il processo di connessione e tornare su questo scenario quando la connessione è stabilita. Per ulteriori informazioni suAWS

Direct Connect, consulta la Guida per l'AWS Direct Connectutente. Per ulteriori informazioni sulla configurazione di una connessione VPN, consulta Connessioni VPN nella Amazon VPC User Guide.

Quando disponi di una connessione AWS Direct Connect o VPN, crei un file system Amazon EFS e una destinazione di montaggio nel tuo Amazon VPC. Dopodiché, scarichi e installi gli amazon-efs-utils strumenti. Quindi, è possibile testare il file system dal client locale. Infine, la fase di pulizia alla fine dello scenario fornisce informazioni che consentono di rimuovere queste risorse.

La procedura dettagliata crea tutte queste risorse nella regione degli Stati Uniti occidentali (Oregon) (). `us-west-2` Qualunque cosa Regione AWS tu usi, assicurati di usarlo in modo coerente. Tutte le tue risorse, il tuo VPC, il tuo target di montaggio e il tuo file system Amazon EFS, devono essere nella Regione AWS stessa posizione, come mostrato nel diagramma seguente.



> **Note**
>
> In alcuni casi, è possibile che l'applicazione locale debba conoscere la disponibilità del file system EFS. In questi casi, l'applicazione deve essere in grado di puntare a un diverso indirizzo IP di montaggio se il primo punto di montaggio diventa temporaneamente non disponibile. In questo scenario, è consigliabile disporre di due client locali collegati ai file system attraverso diverse zone di disponibilità per una maggiore disponibilità.

## Prima di iniziare

Puoi utilizzare le tue credenziali root Account AWS per accedere alla console e provare questo esercizio. Tuttavia, le best practice AWS Identity and Access Management (IAM) consigliano di non utilizzare le credenziali root del proprio. Account AWS Al contrario, è necessario creare un utente amministratore nell'account e utilizzare tali credenziali per gestire le risorse nel proprio account. Per ulteriori informazioni, consulta Configurazione.

È possibile usare una VPC di default o una VPC personalizzata creata all'interno dell'account. Per questo scenario, va bene la configurazione di default della VPC. Tuttavia, se si utilizza una VPC personalizzata, verificare quanto segue:

- Il gateway Internet è connesso alla VPC. Per ulteriori informazioni, consultare la sezione relativa ai gateway Internet nella Guida per l'utente di Amazon VPC.
- La tabella di routing della VPC include una regola per l'invio di tutto il traffico Internet-verso il gateway Internet.

## Fase 1: crea le tue risorse Amazon Elastic File System

In questa fase, crei il tuo file system Amazon EFS e monti le destinazioni.

Per creare il tuo file system Amazon EFS

1. Apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Scegliere Create File System (Crea file system).
3. Selezionare la VPC di default dall'elenco delle VPC.
4. Selezionare le caselle di controllo per tutte le zone di disponibilità. Assicurarsi che tutte abbiano selezionati le sottoreti di default, gli indirizzi IP automatici e i gruppi di sicurezza di default.

Queste sono le destinazioni di montaggio. Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

5. Selezionare Next Step (Fase successiva).
6. Denominare il file system, mantenere General Purpose (Utilizzo generico) selezionato come modalità prestazionale di default e scegliere Next Step (Fase successiva).
7. Scegliere Create File System (Crea file system).
8. Scegliere il file system dall'elenco e annotare il valore del Security group (Gruppo di sicurezza). che servirà per la fase successiva.

Il file system creato dispone di destinazioni di montaggio. A ogni destinazione di montaggio è associato un gruppo di sicurezza. Il gruppo di sicurezza funge da firewall virtuale che controlla il traffico di rete. Se non hai fornito un gruppo di sicurezza durante la creazione di un target di montaggio, Amazon EFS associa il gruppo di sicurezza predefinito del VPC ad esso. Se le procedure precedenti sono state seguite correttamente, le destinazioni di montaggio utilizzano il gruppo di sicurezza di default.

A questo punto, è possibile aggiungere una regola al gruppo di sicurezza della destinazione di montaggio affinché il traffico in entrata possa raggiungere la porta NFS (Network File System) (2049). Per aggiungere la regola al gruppo di sicurezza della destinazione di montaggio nella VPC è possibile utilizzare la AWS Management Console.

Per permettere al traffico in entrata di raggiungere la porta NFS

1. Accedi a AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Sotto NETWORK & SECURITY (RETE & SICUREZZA), scegliere Security Groups (Gruppi di sicurezza).
3. Scegliere il gruppo di sicurezza associato al file system. Tale valore dovrebbe essere stato annotato al termine di Fase 1: crea le tue risorse Amazon Elastic File System.
4. Nel riquadro a schede visualizzato sotto l'elenco dei gruppi di sicurezza, scegliere la scheda Inbound (In ingresso).
5. Scegliere Modifica.
6. Scegliere Add Rule (Aggiungi regola)e scegliere una regola del tipo seguente:

   - Tipo – NFS
   - Origine – Qualsiasi

È consigliabile utilizzare come origine Qualsiasi solo nella fase di test. È possibile creare un set di origine personalizzato per l'indirizzo IP del client locale, oppure utilizzare la console dal client stesso e scegliere My IP (Il mio IP).

> **Note**
>
> Non è necessario aggiungere una regola in uscita, perché la regola di default consente l'uscita di tutto il traffico. Se non è presente per default questa regola sul traffico in uscita, aggiungere una regola in uscita per permettere l'apertura di una connessione TCP verso la porta NFS, identificando come destinazione il gruppo di sicurezza della destinazione di montaggio.

## Passaggio 2: installa il client NFS

In questa fase si installa il client NFS.

Per installare il client NFS sul server locale

> **Note**
>
> Se occorre crittografare in transito dei dati, utilizzare l'assistente di montaggio Amazon EFS, `amazon-efs-utils`, al posto del client NFS. Per informazioni sull'installazione amazon-efs-utils, consulta la sezione Opzionale: crittografia dei dati in transito.

1. Accedere al terminale del client locale.
2. Installa NFS.

   Se si utilizza Red Hat Linux, installare NFS con il comando seguente.

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

   Se si utilizza Ubuntu, installare NFS con il comando seguente.

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

# Fase 3: installa il file system Amazon EFS sul tuo client locale

Per creare una directory di montaggio

1. Utilizzare il comando seguente per creare una cartella da usare come punto di montaggio.

   Example

   ```
   mkdir ~/efs
   ```

2. Scegliere l'indirizzo IP della destinazione di montaggio nella zona di disponibilità. È possibile misurare la latenza dal client Linux locale. Per farlo, utilizzare uno strumento per terminale come `ping` per testare l'indirizzo IP delle istanze EC2 in diverse zone di disponibilità per trovare quella che presenta la latenza minima.

- Eseguire il comando di montaggio per montare il file system utilizzando l'indirizzo IP della destinazione di montaggio.

  ```
  $ sudo mount -t nfs -o
   nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-IP:/   ~/efs
  ```

Ora che hai montato il tuo file system Amazon EFS, puoi testarlo con la seguente procedura.

Per testare la connessione del file system Amazon EFS

1. Spostarsi nella nuova cartella appena creata con il seguente comando.

   ```
   $ cd ~/efs
   ```

2. Creare una sottocartella e modificare il proprietario di tale sottocartella nell'utente dell'istanza EC2. Quindi spostarsi in tale nuova cartella tramite i seguenti comandi.

   ```
   $ sudo mkdir getting-started
   $ sudo chown ec2-user getting-started
   $ cd getting-started
   ```

3. Creare un file di testo con il comando seguente.

```
$ touch test-file.txt
```

4. Elencare il contenuto della cartella con il comando seguente.

```
$ ls -al
```

Come risultato, viene creato il seguente file.

```
-rw-rw-r-- 1 username username 0 Nov 15 15:32 test-file.txt
```

È inoltre possibile impostare il montaggio automatico del file system aggiungendo una voce al file `/etc/fstab`. Per ulteriori informazioni, consulta Montaggio automatico del file system Amazon EFS.

> **Warning**
>
> In caso di montaggio automatico del file system, utilizzare l'opzione `_netdev`, usata per identificare i file system di rete. Se `_netdev` è mancante, l'istanza EC2 potrebbe smettere di rispondere. Questo risultato è dovuto al fatto che i file system di rete devono essere inizializzati dopo che l'istanza di calcolo ha avviato la sua interfaccia di rete. Per ulteriori informazioni, consulta Il montaggio automatico non funziona e l'istanza non risponde.

## Fase 4: Pulisci le risorse e proteggi il tuo AWS account

Dopo aver completato questa procedura dettagliata, o se non desideri approfondire le procedure dettagliate, segui questi passaggi per ripulire le tue risorse e proteggere il tuo account. AWS

Per ripulire le risorse e proteggere le tue Account AWS

1. Smonta il file system Amazon EFS con il seguente comando.

```
$ sudo umount ~/efs
```

2. Apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
3. Scegli il file system Amazon EFS che desideri eliminare dall'elenco dei file system.
4. In Azioni, seleziona Elimina file system.

5. Nella finestra di dialogo Elimina definitivamente il file system, digita l'ID del file system Amazon EFS che desideri eliminare, quindi scegli Elimina file system.
6. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
7. Fai clic su Gruppi di sicurezza nel pannello di navigazione.
8. Selezionare il nome del gruppo di sicurezza a cui è stata aggiunta la regola per questo scenario.

   > **Warning**
   >
   > Non eliminare il gruppo di sicurezza predefinito della VPC.

9. Nel menu Actions (Operazioni), selezionare Edit inbound rules (Modifica regole in entrata).
10. Scegliere la X alla fine della regola in entrata aggiunta e scegliere Save (Salva).

## Facoltativo: crittografia dei dati in transito

Per crittografare i dati in transito, utilizza l'helper di montaggio di Amazon EFS anziché il client NFS. amazon-efs-utils

Il amazon-efs-utils pacchetto è una raccolta open source di strumenti Amazon EFS. La amazon-efs-utils raccolta include un supporto di montaggio e strumenti che semplificano la crittografia dei dati in transito per Amazon EFS. Per ulteriori informazioni su questo pacchetto, consultare Utilizzo degli amazon-efs-utils strumenti. Questo pacchetto è disponibile come download gratuito da GitHub, che puoi ottenere clonando l'archivio del pacchetto.

Da clonare da amazon-efs-utils GitHub

1. Accedere al terminale del client locale.
2. Dal terminale, clona lo amazon-efs-utils strumento da una cartella GitHub a tua scelta, con il seguente comando.

   ```
   git clone https://github.com/aws/efs-utils
   ```

Ora che si dispone del pacchetto, è possibile installarlo. Questa installazione viene gestita in modo diverso a seconda della distribuzione Linux del client locale. Sono supportate le seguenti distribuzioni:

- Amazon Linux 2

- Amazon Linux
- Red Hat Enterprise Linux (e derivati come CentOS) versione 7 e successive
- Ubuntu 16.04 LTS e versioni più recenti

Da compilare e installare amazon-efs-utils come pacchetto RPM

1. Apri un terminale sul tuo client e vai alla directory da cui è stato clonato amazon-efs-utils il pacchetto. GitHub
2. Compilare il pacchetto con il seguente comando.

```
make rpm
```

> **Note**
>
> Se non è già stato fatto, installare il pacchetto rpm-builder con il comando seguente.
>
> ```
> sudo yum -y install rpm-build
> ```

3. Installare il pacchetto con il seguente comando.

```
sudo yum -y install build/amazon-efs-utils*rpm
```

Da compilare e installare amazon-efs-utils come pacchetto deb

1. Apri un terminale sul tuo client e vai alla directory da cui è stato clonato amazon-efs-utils il pacchetto. GitHub
2. Compilare il pacchetto con il seguente comando.

```
./build-deb.sh
```

3. Installare il pacchetto con il seguente comando.

```
sudo apt-get install build/amazon-efs-utils*deb
```

Dopo aver installato il pacchetto, configuralo amazon-efs-utils per l'utilizzo Regione AWS con AWS Direct Connect o VPN.

Da configurare amazon-efs-utils per l'uso nel tuo Regione AWS

1. Utilizzando un editor di testo di scelta, aprire `/etc/amazon/efs/efs-utils.conf` per la modifica.
2. Individuare la riga "`dns_name_format = {fs_id}.efs.{region}.amazonaws.com`".
3. Modifica *`{region}`* con l'ID della tua AWS regione, ad esempio`us-west-2`.

Per montare il file system EFS sul client locale, aprire un terminale sul client Linux locale. Per montare il sistema, sono necessari l'ID del file system, l'indirizzo IP di destinazione di montaggio per una delle destinazioni di montaggio e quello del file systemRegione AWS. Se vengono create più destinazioni di montaggio per il file system, è possibile sceglierne una qualsiasi.

Quando si dispone di tali informazioni, è possibile montare il file system in tre passaggi:

Per creare una directory di montaggio

1. Utilizzare il comando seguente per creare una cartella da usare come punto di montaggio.

   Example

   ```
   mkdir ~/efs
   ```

2. Scegliere l'indirizzo IP della destinazione di montaggio nella zona di disponibilità. È possibile misurare la latenza dal client Linux locale. Per farlo, utilizzare uno strumento per terminale come `ping` per testare l'indirizzo IP delle istanze EC2 in diverse zone di disponibilità per trovare quella che presenta la latenza minima.

Per aggiornare **`/etc/hosts`**

- Aggiungere una voce al file `/etc/hosts` locale con l'ID del file system e l'indirizzo IP della destinazione di montaggio nel formato seguente.

  ```
  mount-target-IP-Address file-system-ID.efs.region.amazonaws.com
  ```

Example

```
192.0.2.0 fs-12345678.efs.us-west-2.amazonaws.com
```

Per creare una directory di montaggio

1. Utilizzare il comando seguente per creare una cartella da usare come punto di montaggio.

   Example

   ```
   mkdir ~/efs
   ```

2. Eseguire il comando di montaggio per montare il file system.

   Example

   ```
   sudo mount -t efs fs-12345678 ~/efs
   ```

   Se si desidera utilizzare la crittografia dei dati in transito, il comando di montaggio assomiglierà al seguente.

   Example

   ```
   sudo mount -t efs -o tls fs-12345678 ~/efs
   ```

# Scenario: Montaggio di un file system da un VPC diverso

In questa procedura dettagliata, configuri un'istanza Amazon EC2 per montare un file system Amazon EFS che si trova in un cloud privato virtuale (VPC) diverso. È possibile eseguire questa operazione utilizzando l'helper di montaggio EFS. Il supporto di montaggio fa parte del set di strumenti `amazon-efs-utils`. Per ulteriori informazioni su `amazon-efs-utils`, consulta Utilizzo degli amazon-efs-utils strumenti.

Il VPC del client e il VPC del file system EFS devono essere connessi utilizzando una connessione di peering VPC o un gateway di transito VPC. Quando utilizzi una connessione peering VPC o un gateway di transito per connettere i VPC, le istanze Amazon EC2 che si trovano in un VPC possono accedere ai file system EFS in un altro VPC, anche se i VPC appartengono a account diversi.

> **Note**
>
> L'uso di Amazon EFS con client basati su Microsoft Windows non è supportato.

Argomenti



## Prima di iniziare

In questo scenario, supponiamo che si disponga già di quanto riportato di seguito:

- Il set di strumenti `amazon-efs-utils` viene installato nell'istanza EC2 prima di utilizzare questa procedura. Per istruzioni sull'installazione di `amazon-efs-utils`, vedere Utilizzo degli amazon-efs-utils strumenti.
- Una delle seguenti:
  - Una connessione peering VPC tra il VPC in cui si trova il file system EFS e il VPC in cui si trova l'istanza EC2. Una connessione di peering VPC è una connessione di rete tra due VPC. Questo tipo di connessione consente di instradare il traffico tra di essi utilizzando indirizzi IPv4 (Internet Protocol version 4) o IPv6 (Internet Protocol version 6) privati. Puoi utilizzare il peering VPC per connettere i VPC all'interno dello stessoRegione AWS o traRegione AWS s. Per ulteriori informazioni, consulta Creating and Accepting a VPC peering Connection nella Amazon VPC Peering Guide.
  - Un Transit Gateway che connette il VPC in cui si trova il file system EFS e il VPC in cui si trova l'istanza EC2. Un Transit Gateway è un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti locali. Per ulteriori informazioni, consulta Getting Started with Transit Gateways nella Guida ai gateway di transito di Amazon VPC.

# Passaggio 1: Determinare l'ID della zona di disponibilità della destinazione di montaggio EFS

Per garantire un'elevata disponibilità del file system, si consiglia di utilizzare sempre un indirizzo IP di destinazione del montaggio EFS che si trovi nella stessa zona di disponibilità del client NFS. Se state montando un file system EFS che si trova in un altro account, assicuratevi che il client NFS e la destinazione di montaggio EFS siano nello stesso ID della zona di disponibilità. Questo requisito si applica perché i nomi delle zone di disponibilità possono differire da un account all'altro.

Per determinare l'ID della zona di disponibilità dell'istanza EC2

1. Connettiti all'istanza EC2:

   - Per connettersi all'istanza da un computer che esegue macOS o Linux, specificare il file .pem per il comando SSH. Per fare ciò, utilizzare l'opzione `-i` e il percorso della chiave privata.
   - Per connettere l'istanza da un computer che esegue Windows, puoi usare uno MindTerm o PuTTY. Per utilizzare PuTTY, installarlo e convertire il file .pem in un file .ppk.

   Per ulteriori informazioni, consulta Amazon EC2 argomenti i:

   - Connessione all'istanza Linux tramite SSH
   - Connessione all'istanza Linux da Windows tramite PuTTY
2. Determina l'ID della zona di disponibilità in cui si trova l'istanza EC2 utilizzando il comando`describe-availability-zones` CLI come segue.

```
[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"
        }
    ]
}
```

   L'ID della zona di disponibilità viene restituito nella`ZoneId` proprietà,`use2-az2`.

# Passaggio 2: Determinare l'indirizzo IP di destinazione di montaggio

Ora che conosci l'ID della zona di disponibilità dell'istanza EC2, puoi ora recuperare l'indirizzo IP del target di montaggio che si trova nello stesso ID della zona di disponibilità.

Per determinare l'indirizzo IP di destinazione del montaggio nello stesso ID della zona di disponibilità

- Recuperare l'indirizzo IP di destinazione del montaggio per il file system nell'ID AZ `use2-az2` utilizzando il comando `describe-mount-targets` CLI, come segue.

```
$ 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"
        }
    ]
}
```

La destinazione di montaggio nell'ID della zona diuse2-az2 disponibilità ha un indirizzo IP 10.0.2.153.

## Passaggio 3: Aggiungere una voce host per la destinazione di montaggio

È ora possibile inserire una voce nel file `/etc/hosts` nell'istanza EC2 che associa l'indirizzo IP di destinazione del montaggio al nome host del file system EFS.

Come aggiungere una voce host per la destinazione di montaggio

1. Aggiungere una riga per l'indirizzo IP di destinazione del montaggio al file `/etc/hosts` dell'istanza EC2. La voce utilizza il formato m*ount-target-IP-Address file-system-ID*`.efs.`*region*`.amazonaws.com`. Utilizzare il seguente comando per aggiungere la riga al file.

   ```
   echo "10.0.2.153 fs-01234567.efs.us-east-2.amazonaws.com" | sudo tee -a /etc/hosts
   ```

2. Assicurati che i gruppi di sicurezza VPC per l'istanza EC2 e il target di montaggio dispongano di regole che consentano l'accesso al sistema EFS, se necessario. Per ulteriori informazioni, consulta Utilizzo di gruppi di sicurezza VPC per istanze Amazon EC2 e destinazioni di montaggio.

## Passaggio 4: Montare il file system utilizzando EFS Mount Helper

Per montare il file system EFS, creare prima una directory di montaggio sull'istanza EC2. Quindi, utilizzando l'helper di montaggio EFS, è possibile montare il file system con l'autorizzazione IAM o un punto di accesso EFS. Per ulteriori informazioni, consultare Utilizzo di IAM per controllare l'accesso ai dati del file system e Utilizzo dei punti di accesso Amazon EFS.

Per creare una directory di montaggio

- Creare una directory per il montaggio del file system utilizzando il seguente comando.

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

Per montare il file system utilizzando l'autorizzazione IAM

- Utilizzare il seguente comando per montare il file system utilizzando l'autorizzazione IAM.

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

Per montare il file system utilizzando un punto di accesso EFS

- Utilizzare il comando seguente per montare il file system utilizzando un punto di accesso EFS.

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

Ora che hai montato il tuo file system Amazon EFS, puoi testarlo con la seguente procedura.

Per connettere file system Amazon EFS

1. Spostarsi nella nuova cartella appena creata con il seguente comando.

```
$ cd ~/mnt/efs
```

2. Creare una sottocartella e modificare il proprietario di tale sottocartella nell'utente dell'istanza EC2. Quindi spostarsi in tale nuova cartella tramite i seguenti comandi.

```
$ sudo mkdir getting-started
$ sudo chown ec2-user getting-started
$ cd getting-started
```

3. Creare un file di testo con il comando seguente.

```
$ touch test-file.txt
```

4. Elencare il contenuto della cartella con il comando seguente.

```
$ ls -al
```

Come risultato, viene creato il seguente file.

```
-rw-rw-r-- 1 username username 0 Nov 15 15:32 test-file.txt
```

È inoltre possibile impostare il montaggio automatico del file system aggiungendo una voce al file `/etc/fstab`. Per ulteriori informazioni, consulta Utilizzo di `/etc/fstab` con EFS mount helper per rimontare automaticamente i file system EFS.

> **Warning**
>
> In caso di montaggio automatico del file system, utilizzare l'opzione `_netdev`, usata per identificare i file system di rete. Se `_netdev` è mancante, l'istanza EC2 potrebbe smettere di rispondere. Questo risultato è dovuto al fatto che i file system di rete devono essere inizializzati dopo che l'istanza di calcolo ha avviato la sua interfaccia di rete. Per ulteriori informazioni, consulta Il montaggio automatico non funziona e l'istanza non risponde.

## Passaggio 5: ripulisci le risorse e proteggi il tuoAWS account

Dopo aver completato questa procedura dettagliata o se non si desidera esplorare le procedure dettagliate, assicurarsi di eseguire le seguenti operazioni. Questi ripuliscono le tue risorse e proteggono le tueAccount AWS.

Per ripulire le risorse e proteggere leAccount AWS

1. Smonta file system Amazon EFS con il ordine i.

   ```
   $ sudo umount ~/efs
   ```

2. Apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
3. Scegli il file system Amazon EFS che desideri eliminare dall'elenco dei file system.
4. In Azioni, seleziona Elimina file system.
5. Nella finestra di dialogo Elimina definitivamente il file system, digita l'ID del file system per il file system Amazon EFS che desideri eliminare, quindi scegli Elimina file system.
6. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
7. Fai clic su Gruppi di sicurezza nel pannello di navigazione.
8. Selezionare il nome del gruppo di sicurezza a cui è stata aggiunta la regola per questo scenario.

   > **Warning**
   >
   > Non eliminare il gruppo di sicurezza predefinito della VPC.

9. Nel menu Actions (Operazioni), selezionare Edit inbound rules (Modifica regole in entrata).
10. Scegliere la X alla fine della regola in entrata aggiunta e scegliere Save (Salva).

# Procedura passo per passo: Applicazione della crittografia dei dati memorizzati su disco su un file system Amazon EFS

Qui di seguito, è possibile trovare ulteriori dettagli su come applicare la crittografia dei dati memorizzati su disco utilizzando Amazon CloudWatch eAWS CloudTrail. Questa procedura dettagliata si basa sulAWSwhite paperCrittografia dei dati inattivi con i file system Amazon EFS crittografati.

> **Note**
>
> Il metodo per applicare la creazione di file system Amazon EFS crittografati a riposo descritto in questa procedura dettagliata è obsoleto. Il metodo preferito per implementare la creazione di file system crittografati a riposo è quello di utilizzare`elasticfilesystem:Encrypted`Chiavi di condizione inAWS Identity and Access Managementpolicy basate su identità. Per ulteriori informazioni, consultare Esempio: applicazione della creazione di file system crittografati. È possibile utilizzare questa procedura dettagliata per creare allarmi CloudWatch per verificare che le policy IAM impediscono la creazione di file system non crittografati.

## Abilitazione della crittografia dei dati memorizzati su disco

Un'azienda potrebbe richiedere la crittografia dei dati memorizzati su disco di tutti i dati che soddisfano una determinata classificazione o che sono associati a una determinata applicazione, carico di lavoro o ambiente. È possibile implementare le policy per la crittografia dei dati memorizzati su disco sui file system Amazon EFS utilizzando dei meccanici di controllo a riposo. Questi controlli rilevano la creazione di un file system e verificano che la crittografia dei dati memorizzati su disco sia abilitata.

Se per un file system non viene rilevata la crittografia dei dati memorizzati su disco, è possibile rispondere in diversi modi. Tali risposte vanno dall'eliminazione del file system e delle destinazioni di montaggio fino alla semplice notifica ad un amministratore.

Se si desidera eliminare un file system senza crittografia dei dati memorizzati su disco mantenendo però i dati, è necessario prima creare un nuovo file system con la crittografia dei dati memorizzati su disco abilitata. Quindi, copiare i dati sul nuovo file system con la crittografia dei dati memorizzati su disco abilitata. Al termine della copia, è possibile eliminare il file system senza crittografia dei dati memorizzati su disco.

## Rilevamento di file system non crittografati a riposo

Puoi creare un allarme CloudWatch per monitorare i log di CloudTrail`CreateFileSystem`Evento . È quindi possibile attivare l'allarme per notificare a un amministratore se il file system è stato creato senza crittografia dei dati memorizzati su disco.

## Creazione di un filtro parametri

Per creare un allarme CloudWatch da attivare quando viene creato un file system Amazon EFS non crittografato, utilizzare la procedura seguente.

Prima di iniziare, è necessario disporre di un osservatore precedentemente creato che invii i log di CloudTrail verso un gruppo di log di CloudWatch Logs. Per ulteriori informazioni, consultaInvio di eventi a CloudWatch LogsnellaAWS CloudTrailGuida per l'utente di.

Per creare un filtro parametrico

1. Apri la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione scegli Logs (Log).
3. Nell'elenco dei gruppi di log, scegli il gruppo di log creato per gli eventi di log di CloudTrail.
4. Scegliere Create Metric Filter (Crea filtro parametro).
5. Nella pagina Define Logs Metric Filter (Definisci il filtro parametrico sui log), scegliere Filter Pattern (Schema del filtro) e quindi inserire quanto segue:

   ```
   { ($.eventName = CreateFileSystem) && ($.responseElements.encrypted IS FALSE) }
   ```

6. Scegli Assign Metric (Assegna parametro).
7. Per Filter Name (Nome filtro), digitare **`UnencryptedFileSystemCreated`**.
8. Per Metric Namespace (Spazio dei nomi parametro), digita **`CloudTrailMetrics`**.
9. Per Metric Name (Nome parametro) digita **`UnencryptedFileSystemCreatedEventCount`**.
10. Scegliere Show advanced metric settings (Mostra impostazioni parametro avanzate).

11. Per Metric Value (Valore parametro), digitare **1**.
12. Scegli Create Filter (Crea filtro).

## Creazione di un allarme

Dopo aver creato il filtro parametro, seguire questa procedura per creare un allarme.

Per creare un allarme

1. Alla voce Filters (Filtri) nella pagina Log_Group_Name (Nome gruppo di log), dopo il nome del filtro UnencryptedFileSystemCreated, scegliere Create Alarm (Crea allarme).
2. Nella pagina Create Alarm (Crea allarme), impostare i seguenti parametri:
   - Per Nome, digitare **`Unencrypted File System Created`**
   - Alla voce Whenever (Ogni volta che), procedere nel seguente modo:
     - Impostare is (è) a *`> = 1`*
     - Imposta for: (per:) a *1* periodo/i consecutivo/i.
   - Alla voce Treat missing data as (Considera dati mancanti come), scegliere good (not breaching threshold) (buoni - non superano la soglia).
   - Alla voce Actions (Operazioni), procedere nel seguente modo:
     - In Whenever this alarm (Ogniqualvolta questo allarme), seleziona State is ALARM (Lo stato è ALLARME).
     - Alla voce Send notification to (Invia notifica a) scegliere NotifyMe (Notificami), scegliere New list (Nuovo elenco) e quindi digitare un nome di argomento univoco per questo elenco.
     - Alla voce Email list (Elenco email), digitare l'indirizzo email a cui devono essere inviate le notifiche. Sarà inviata un'email a questo indirizzo per confermare la creazione dell'allarme.
   - Alla voce Alarm Preview (Anteprima allarme), procedere nel seguente modo:
     - Alla voce Period (Periodo), scegliere 1 Minute (1 minuto).
     - Alla voce Statistic (Statistica), scegliere Standard e Sum (Somma).
3. Scegliere Create Alarm (Crea allarme).

## Testare l'allarme per la creazione di file system senza crittografia

È possibile testare l'allarme mediante la creazione di un file system senza crittografia dei dati memorizzati su disco, come descritto di seguito.

Per testare l'allarme mediante la creazione di un file system senza crittografia dei dati memorizzati su disco

1. Eseguire l'accesso allaAWS Management Consolee apri la console Amazon EFS all'indirizzohttps://console.aws.amazon.com/efs/.
2. ScegliereCreare un file systemper visualizzareCreare un file systemfinestra di dialogo.
3. Per creare un file system non crittografato a riposo, sceglierePersonalizzaper visualizzareImpostazioni del file system(Certificato creato).
4. PerGeneraleimpostazioni, immettere quanto segue.
   a. (Facoltativo) Immettere unNomeper il sistema di file.
   b. KeepGestione del ciclo di vita,modalità prestazionali, eModalità di throughputimpostati sui valori predefiniti.
   c. DisattivaCrittografiaper compensazioneAbilitare la crittografia dei dati inattivi.
5. ScegliereSuccessivoper continuare ad arrivare allaAccess alla retepassaggio nel processo di configurazione.
6. Scegliere il valore predefinitoVirtual Private Cloud (VPC).
7. PerObiettivi di montaggio, scegli il valore predefinitoGruppi di sicurezzaper ogni destinazione di montaggio.
8. ScegliereSuccessivoper visualizzareCriteri del file system(Certificato creato).
9. ScegliereSuccessivoper continuare ad arrivare allaRivedi e crea(Certificato creato).
10. Esamina il file system e scegliCreateper creare il file system e tornare alFile system(Certificato creato).

Il percorso registra`CreateFileSysteme` distribuisce l'evento al gruppo di log di CloudWatch Logs. L'evento genera l'allarme metrico e CloudWatch Logs invia una notifica relativa alla modifica.

# Procedura dettagliata: abilita il root squashing utilizzando l'autorizzazione IAM per i client NFS

In questa procedura dettagliata, configuri Amazon EFS per impedire l'accesso root al tuo file system Amazon EFS per tutti iAWS principali ad eccezione di una singola workstation di gestione. A tale scopo, è necessario configurare l'autorizzazioneAWS Identity and Access Management (IAM) per i

client Network File System (NFS). Per ulteriori informazioni sull'autorizzazione IAM per i client NFS in EFS, vedere Utilizzo di IAM per controllare l'accesso ai dati del file system.

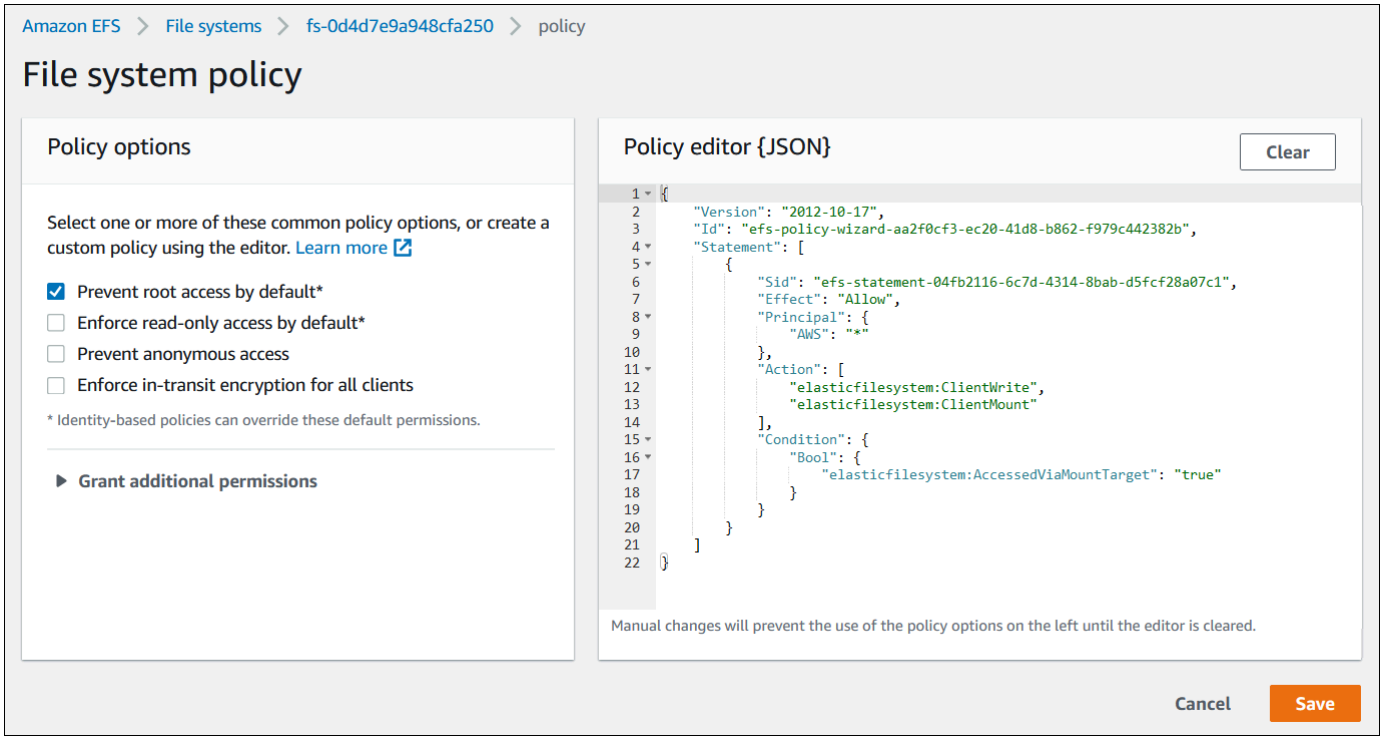
Per fare ciò è necessaria la configurazione di due politiche di autorizzazione IAM, come segue:

- Creare una policy del file system EFS che consente esplicitamente l'accesso in lettura e scrittura al file system e rifiuta implicitamente l'accesso root.
- Assegna un'identità IAM alla workstation di gestione Amazon EC2 che richiede l'accesso root al file system utilizzando un profilo di istanza Amazon EC2. Per ulteriori informazioni sui profili di istanza Amazon EC2, consulta Utilizzo dei profili di istanza nella Guida per l'AWS Identity and Access Managementutente.
- Assegnare la policy gestita `AmazonElasticFileSystemClientFullAccess` AWS al ruolo IAM della workstation di gestione. Per ulteriori informazioni sulle politicheAWS gestite per EFS, vedereGestione dell'identità e degli accessi per Amazon Elastic File System.

Per abilitare il root squashing root l'autorizzazione IAM per i client NFS, utilizzare le procedure seguenti.

Per impedire l'accesso root al file system

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Scegli Filesystems.
3. Scegliere il file system per cui si desidera abilitare il root squashing nella pagina File systems (File system).
4. Nella pagina dei dettagli del file system, scegli Criteri del file system, quindi scegli Modifica. Viene visualizzata la pagina File system policy (Policy del file system).




5. Scegli Impedisci l'accesso root per impostazione predefinita* in Opzioni politiche. L'oggetto JSON della policy viene visualizzato nell'editor delle policy.
6. Scegliere Save (Salva) per salvare la policy del file system.

I client non anonimi possono ottenere l'accesso root al file system tramite una policy basata su identità. Quando si collega la policy`AmazonElasticFileSystemClientFullAccess` gestita al ruolo della workstation, IAM concede l'accesso root alla workstation in base alla sua politica di identità.

Per abilitare l'accesso root dalla workstation di gestione

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Creazione di un ruolo per Amazon EC2 chiamato`EFS-client-root-access`. IAM crea un profilo di istanza con lo stesso nome del ruolo EC2 che hai creato.
3. Assegnare la policy AWS gestita `AmazonElasticFileSystemClientFullAccess` al ruolo EC2 creato. Il contenuto di questa policy è mostrato di seguito.

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

```
            "Effect": "Allow",
            "Action": [
                    "elasticfilesystem:ClientMount",
                    "elasticfilesystem:ClientRootAccess",
                    "elasticfilesystem:ClientWrite",
                    "elasticfilesystem:DescribeMountTargets"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Collegare il profilo di istanza all'istanza EC2 che si sta utilizzando come workstation di gestione, come descritto di seguito. Per ulteriori informazioni, consultare la sezione relativa al collegamento di un ruolo IAM a un'istanza nella Guida per l'utente di Amazon EC2 per le istanze Linux.

   a. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   b. Nel pannello di navigazione, seleziona Instances (Istanze).
   c. Selezionare l'istanza. In Actions (Operazioni), scegliere Instance Settings (Impostazioni istanza), e quindi scegliere Attach/Replace IAM role (Collega/Sostituisci ruolo IAM).
   d. Scegliere il ruolo IAM creato nella prima fase, `EFS-client-root-access`, e scegliere Apply (Applica).

5. Installare l'assistente per il montaggio di EFS sulla workstation di gestione. Per ulteriori informazioni sull'helper di montaggio EFS e sul amazon-efs-utils pacchetto, vedereUtilizzo degli amazon-efs-utils strumenti.

6. Montare il file system EFS sulla workstation di gestione utilizzando il seguente comando con l'opzione di montaggio `iam`.

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

   Puoi configurare l'istanza Amazon EC2 per montare automaticamente il file system con l'autorizzazione IAM. Per ulteriori informazioni su come montare un file system EFS con autorizzazione IAM, consultaMontaggio con autorizzazione IAM.

# Sicurezza in Amazon EFS

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in Amazon Elastic File System. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog AWS Shared Responsibility Model and GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con EFS o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Argomenti

# Crittografia dei dati in Amazon EFS

Amazon EFS supporta due forme di crittografia per i file system, la crittografia dei dati in transito e la crittografia dei dati memorizzati su disco. Alla creazione di un file system Amazon EFS, è possibile abilitare la crittografia dei dati a riposo. Al montaggio del file system è possibile abilitare la crittografia dei dati in transito.

Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

## Quando usare la crittografia

Se la propria azienda è soggetto a policy aziendali o normative che richiedono la crittografia dei dati e dei metadati memorizzati su disco, consigliamo di creare un file system crittografato montando il file system utilizzando la crittografia dei dati in transito.

### Argomenti correlati

Per ulteriori informazioni sulla crittografia con Amazon EFS, consulta questi argomenti correlati:

- Utilizzo delle risorse Amazon EFS
- Gestione dell'accesso ai file system crittografati
- Suggerimenti per le prestazioni Amazon EFS

- Voci dei file di log di Amazon encrypted-at-rest EFS per i file system
- Risoluzione dei problemi di crittografia

## Crittografia dei dati a riposo

Puoi creare file system crittografati utilizzando AWS Management Console AWS CLI, o programmaticamente tramite l'API Amazon EFS o uno degli AWS SDK. Un'azienda potrebbe richiedere la crittografia di tutti i dati che soddisfano una determinata classificazione o sono associati a una determinata applicazione, carico di lavoro o ambiente.

Una volta creato un file system EFS, non è possibile modificarne l'impostazione di crittografia. Ciò significa che non è possibile modificare un file system non crittografato per renderlo crittografato. Invece, è necessario creare un nuovo file system crittografato.

> **Note**
>
> L'infrastruttura di gestione delle AWS chiavi utilizza algoritmi crittografici approvati dal Federal Information Processing Standards (FIPS) 140-2. L'infrastruttura è compatibile con le raccomandazioni National Institute of Standards and Technology (NIST) 800-57.

### Implementazione della creazione di file system Amazon EFS crittografati a riposo

Puoi utilizzare la chiave di condizione `elasticfilesystem:Encrypted` IAM nelle policy basate sull'identità AWS Identity and Access Management (IAM) per controllare se gli utenti possono creare file system Amazon EFS crittografati a riposo. Per ulteriori informazioni su come utilizzare la chiave di condizione, consulta Esempio: applicazione della creazione di file system crittografati.

È inoltre possibile definire policy di controllo dei servizi (SCP) all'interno AWS Organizations per applicare la crittografia Account AWS EFS per tutti i membri dell'organizzazione. Per ulteriori informazioni sulle politiche di controllo del servizio in AWS Organizations, consulta le politiche di controllo dei servizi nella Guida per l'AWS Organizations utente.

### Crittografia di un file system memorizzato su disco tramite l'utilizzo della console

Quando crei un nuovo file system utilizzando la console Amazon EFS, la crittografia a riposo è abilitata per impostazione predefinita. La procedura seguente descrive come abilitare la crittografia per un nuovo file system al momento della sua creazione tramite la console.

> **Note**
>
> La crittografia a riposo non è abilitata per impostazione predefinita quando si crea un nuovo file system utilizzando AWS CLI, l'API e gli SDK. Per ulteriori informazioni, consulta Creazione di un file system mediante AWS CLI.

Per crittografare un nuovo file system dalla console EFS

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Scegli Crea file system per aprire la finestra di dialogo Crea file system.
3. (Facoltativo) Immetti un Nome per il file system.
4. Per Virtual Private Cloud (VPC), scegli il tuo VPC o mantienilo impostato sul tuo VPC predefinito.
5. Scegli Crea per creare un file system che utilizzi le seguenti impostazioni consigliate dal servizio:

   - La crittografia dei dati inattivi è abilitata utilizzando l'impostazione predefinita AWS KMS key per Amazon EFS (`aws/elasticfilesystem`).
   - Backup automatici attivati - Per ulteriori informazioni, consulta Backup dei file system di Amazon EFS.
   - Destinazioni di montaggio - Amazon EFS crea destinazioni di montaggio con le seguenti impostazioni:
     - Si trova in ogni zona di disponibilità in Regione AWS cui viene creato il file system.
     - Si trovano nelle sottoreti predefinite della VPC selezionata.
     - Usa il gruppo di sicurezza predefinito per la VPC. È possibile gestire i gruppi di sicurezza dopo aver creato il file system.

     Per ulteriori informazioni, consulta Gestione dell'accessibilità del file system dalla rete.
   - Per ulteriori informazioni sulle prestazioni a scopi generali, consulta Modalità prestazionali.
   - Per ulteriori informazioni sul Throughput Elastic, consulta Modalità di velocità di trasmissione effettiva.
   - Gestione del ciclo di vita abilitata con una policy di 30 giorni: per ulteriori informazioni, consulta la sezione Gestione dello storage del file system.
6. La pagina File system viene visualizzata con un banner nella parte superiore che mostra lo stato del file system creato. Quando il file system diventa disponibile, nel banner viene visualizzato un collegamento per accedere alla pagina dei dettagli del file system.

Ora hai un nuovo encrypted-at-rest file system.

## Come funziona la crittografia dei dati memorizzati su disco

In un file system crittografato, i dati e i metadati vengono automaticamente crittografati prima di essere scritti sul file system. Analogamente, quando i dati e i metadati vengono letti, sono automaticamente decifrati prima di essere presentati all'applicazione. Questi processi vengono gestiti in modo trasparente da Amazon EFS, perciò non è necessario modificare le applicazioni.

Amazon EFS utilizza un algoritmo di crittografia AES-256 standard del settore per crittografare i dati e i metadati EFS memorizzati su disco. Per ulteriori informazioni, consulta Elementi di base di crittografia nella Guida per sviluppatori di AWS Key Management Service .

In che modo Amazon EFS utilizza AWS KMS

Amazon EFS si integra con AWS Key Management Service (AWS KMS) per la gestione delle chiavi. Amazon EFS utilizza chiavi gestite dal cliente per crittografare il file system nel modo seguente:

- Crittografia dei metadati a riposo: Amazon EFS utilizza per Chiave gestita da AWS Amazon EFS per crittografare e decrittografare i metadati del file system (ovvero nomi di file, nomi di directory e contenuti delle directory). `aws/elasticfilesystem`
- Crittografia dei dati a riposo - L'utente sceglie la chiave gestita dal cliente utilizzata per crittografare e decifrare i file di dati (ovvero i contenuti dei file). È possibile attivare, disattivare o revocare le concessioni su questa chiave gestita dal cliente. Questa chiave gestita dal cliente può essere dei due tipi seguenti:
  - Chiave gestita da AWS per Amazon EFS: questa è la chiave gestita dal cliente predefinita,`aws/elasticfilesystem`. Non viene addebitato alcun costo per creare e archiviare una chiave gestita dal cliente, ma sono previsti costi di utilizzo. Per ulteriori informazioni, consulta Prezzi di AWS Key Management Service.
  - Chiave gestita dal cliente – Questa è la chiave KMS più flessibile da usare, perché è possibile configurare le policy e i permessi per più utenti o servizi. Per ulteriori informazioni sulla creazione di chiavi gestite dal cliente, consulta Creating keys nella AWS Key Management Service Developer Guide.

    Se si utilizza una chiave gestita dal cliente per la crittografia e la decrittografia dei dati dei file, è possibile attivare la rotazione delle chiavi. Quando abiliti la rotazione dei tasti, ruota AWS KMS automaticamente la chiave una volta all'anno. Inoltre, con una chiave gestita dal cliente, è possibile scegliere quando disattivare, riattivare, eliminare o revocare l'accesso alla chiave

gestita dal cliente in qualsiasi momento. Per ulteriori informazioni, consulta Disabilitazione, eliminazione o revoca dell'accesso alla chiave KMS di un file system.

> **Important**
>
> Amazon EFS accetta solo chiavi simmetriche gestite dal cliente. Non puoi usare chiavi asimmetriche gestite dai clienti con Amazon EFS.

La crittografia e la decifratura dei dati memorizzati su disco sono gestite in modo trasparente. Tuttavia, gli ID di AWS account specifici di Amazon EFS vengono visualizzati nei AWS CloudTrail log relativi alle AWS KMS azioni. Per ulteriori informazioni, consulta Voci dei file di log di Amazon encrypted-at-rest EFS per i file system.

Politiche chiave di Amazon EFS per AWS KMS

Le policy delle chiavi sono il modo principale per controllare l'accesso alle chiavi gestite dai clienti. Per ulteriori informazioni sulle policy delle chiavi, consulta Policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .L'elenco seguente descrive tutte le autorizzazioni AWS KMS correlate richieste o altrimenti supportate da Amazon EFS per i file system crittografati a riposo:

- kms:Encrypt - (Facoltativa) Crittografa testo normale in testo criptato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms:Decrypt - (Obbligatoria) Decifra il testo criptato. Il testo cifrato è un testo normale che è stato precedentemente crittografato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: ReEncrypt — (Facoltativo) Crittografa i dati sul lato server con una nuova chiave gestita dal cliente, senza esporre il testo in chiaro dei dati sul lato client. I dati sono prima decifrati e quindi nuovamente crittografati. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: GenerateDataKeyWithoutPlaintext — (Obbligatorio) Restituisce una chiave di crittografia dei dati crittografata con una chiave gestita dal cliente. Questa autorizzazione è inclusa nella politica delle chiavi predefinita in kms: GenerateDataKey *.
- kms: CreateGrant — (Obbligatorio) Aggiunge una concessione a una chiave per specificare chi può utilizzare la chiave e in quali condizioni. I grant sono meccanismi di autorizzazioni alternative alle policy sulle chiavi. Per ulteriori informazioni sulle autorizzazioni, consulta Utilizzo delle autorizzazioni nella Guida per gli sviluppatori di AWS Key Management Service . Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

- kms: DescribeKey — (Obbligatorio) Fornisce informazioni dettagliate sulla chiave gestita dal cliente specificata. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: ListAliases — (Facoltativo) Elenca tutti gli alias chiave dell'account. Quando si utilizza la console per creare un file system crittografato, questa autorizzazione popola l'elenco Seleziona chiave KMS. Consigliamo di usare questa autorizzazione per garantire la migliore esperienza utente. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

### Chiave gestita da AWS per la politica Amazon EFS KMS

La policy KMS JSON per Chiave gestita da AWS Amazon EFS `aws/elasticfilesystem` è la seguente:

```
{
    "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": "*"
        }
    ]
}
```

## Crittografia dei dati in transito

È possibile crittografare i dati in transito usando un file system Amazon EFS, senza la necessità di modificare le proprie applicazioni.

### Crittografia dei dati in transito con TLS

L'abilitazione della crittografia dei dati in transito sul file system Amazon EFS avviene tramite l'abilitazione di Transport Layer Security (TLS) al momento del montaggio del file system utilizzando l'helper di montaggio di Amazon EFS. Per ulteriori informazioni, consulta Monta il file system utilizzando l'helper di montaggio di EFS.

Quando la crittografia dei dati in transito viene dichiarata come opzione di montaggio per il file system Amazon EFS, l'helper di montaggio inizializza un processo client stunnel. Stunnel è un relay di rete multifunzione open source. Il processo client stunnel rimane in ascolto su una porta locale in attesa del traffico in entrata e l'helper di montaggio reindirizza il traffico del client Network File System (NFS) verso questa porta locale. L'helper di montaggio utilizza TLS versione 1.2 per comunicare con il file system.

Per il montaggio del file system Amazon EFS con l'helper di montaggio con la crittografia dei dati in transito abilitata

1. Accedi al terminale dell'istanza utilizzando SSH (Secure Shell) e accedi con il nome utente opportuno. Per ulteriori informazioni sulla procedura, consulta Connessione all'istanza Linux tramite SSH nella Guida per l'utente di Amazon EC2 per le istanze Linux.
2. Eseguire il seguente comando per montare il file system.

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

## Come funziona la crittografia dei dati in transito

Per abilitare la crittografia dei dati in transito, è possibile connettersi ad Amazon EFS utilizzando TLS. Si consiglia di utilizzare l'helper di montaggio EFS per montare il file system perché semplifica il processo di montaggio rispetto al montaggio con NFS `mount`. L'helper di montaggio EFS gestisce il processo utilizzando `stunnel` per TLS. Se non si utilizza l'helper di montaggio, è comunque possibile abilitare la crittografia dei dati in transito. Ad alto livello, i passaggi necessari per farlo sono i seguenti.

Per abilitare la crittografia dei dati in transito senza l'helper di montaggio EFS

1. Scaricare e installare `stunnel` e annotare la porta che sulla quale si pone in ascolto l'applicazione. Per istruzioni su come eseguire questa operazione, consulta Aggiornamento di `stunnel`.
2. Esegui `stunnel` per connetterlo al file system Amazon EFS alla porta 2049 usando TLS.
3. Utilizzando il client NFS, montare `localhost:`*`port`*, dove *`port`* è la porta annotato nel primo passaggio.

Poiché la crittografia dei dati in transito viene configurata su base connessione, a ogni montaggio configurato deve a corrispondere un processo `stunnel` dedicato in esecuzione sull'istanza. Per impostazione predefinita, il processo `stunnel` utilizzato dall'helper di montaggio EFS ascolta sulle porte locali 20049 e 20449, e si connette ad Amazon EFS sulla porta 2049.

> **Note**
>
> Per impostazione predefinita, quando utilizzi l'helper di montaggio di Amazon EFS con TLS, l'helper di montaggio esegue la verifica del certificato associato al nome dell'host. L'helper di montaggio di Amazon EFS utilizza il programma `stunnel` per la sua funzionalità TLS. Alcune versioni di Linux non includono una versione di stunnel che supporta queste funzionalità di TLS per impostazione predefinita. Quando si utilizza una di tali versioni di Linux, il montaggio di un file system Amazon EFS con l'utilizzo di TLS ha esito negativo. Dopo aver installato il amazon-efs-utils pacchetto, per aggiornare la versione di stunnel del sistema, consulta. Aggiornamento di `stunnel`

Per problemi relativi alla crittografia, consultare Risoluzione dei problemi di crittografia.

Quando si utilizza la crittografia dei dati in transito, la configurazione del client NFS viene modificata. Quando si ispezionano i tuoi file system montati, se ne vede uno montato all'indirizzo 127.0.0.1 o `localhost`, come nell'esempio seguente.

```
$ mount | column -t
127.0.0.1:/  on  /home/ec2-user/efs        type  nfs4
 (rw,relatime,vers=4.1,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,port=20127,timeo=6
```

Quando si esegue il montaggio con TLS e l'helper di montaggio di Amazon EFS, si riconfigura il client NFS per affinché esegua il montaggio su una porta locale. L'helper di montaggio EFS avvia un processo client `stunnel` che rimane in ascolto su questa porta locale, e `stunnel` apre una connessione crittografata verso EFS usando TLS. L'helper di montaggio di EFS è responsabile per la configurazione e la manutenzione di questa connessione crittografata e della relativa configurazione.

Per determinare quale ID del file system Amazon EFS corrisponde a quale punto di montaggio locale, è possibile utilizzare il comando seguente. Sostituire *`efs-mount-point`* con il percorso locale in cui è stato montato il file system.

```
grep -E "Successfully mounted.*efs-mount-point" /var/log/amazon/efs/mount.log | tail -1
```

Quando si utilizza l'helper di montaggio per la crittografia dei dati in transito, questo crea anche un processo denominato `amazon-efs-mount-watchdog`. Questo processo garantisce che ogni processo stunnel associato al montaggio sia in esecuzione, e arresta stunnel quando il file system Amazon EFS viene smontato. Se per qualsiasi motivo un processo stunnel si arresta in modo inatteso, il processo watchdog lo riavvia.

# Gestione dell'identità e degli accessi per Amazon Elastic File System

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (accesso effettuato) e autorizzato (dotato di autorizzazioni) per utilizzare le risorse Amazon EFS. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti



## Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in Amazon EFS.

Utente del servizio: se si utilizza il servizio Amazon EFS per svolgere il proprio lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di caratteristiche Amazon EFS utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in Amazon EFS, consulta Risoluzione dei problemi relativi all'identità e all'accesso di Amazon Elastic File System.

Amministratore del servizio: se si è responsabile delle risorse Amazon EFS presso la propria azienda, probabilmente si dispone dell'accesso completo a Amazon EFS. Il tuo compito è determinare le funzionalità e le risorse di Amazon EFS a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon EFS, consulta Funzionamento di Amazon Elastic File System con IAM.

Amministratore IAM: se si è amministratore IAM, potrebbe essere interessante ottenere informazioni su come scrivere policy per gestire l'accesso ad Amazon EFS. Per visualizzare policy basate su

identità Amazon EFS di esempio che possono essere utilizzate in IAM, consulta Esempi di policy basate su identità per Amazon Elastic File System.

## Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. Gli utenti AWS IAM Identity Center (Centro identità IAM), l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Console o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWS nella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

### Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

## Identità federata

Come best practice, richiedi agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede ai Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono agli Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center.

## Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

## Ruoli IAM

Un ruolo IAM è un'identità all'interno di un Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'azione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio

AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

## Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

## Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

## Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWS provenienti da IAM in una policy basata su risorse.

## Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

## Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

### Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

## Funzionamento di Amazon Elastic File System con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon EFS, scopri quali funzionalità IAM sono disponibili per l'uso con Amazon EFS.

Funzionalità IAM utilizzabili con Amazon Elastic File System

| Funzionalità IAM | Supporto di Amazon EFS |
|---|---|
| Policy basate su identità | Sì |
| Policy basate su risorse | Sì |
| Azioni di policy | Sì |
| Risorse relative alle policy | Sì |
| Chiavi di condizione della policy (specifica del servizio) | Sì |
| Liste di controllo degli accessi (ACL) | No |
| ABAC (tag nelle policy) | Parziale |
| Credenziali temporanee | Sì |
| Autorizzazioni del principale | Sì |
| Ruoli di servizio | Sì |
| Ruoli collegati al servizio | Sì |

Per ottenere un quadro generale del funzionamento di Amazon EFS e altri servizi AWS con la maggior parte delle funzionalità di IAM, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

## Policy basate su identità per Amazon EFS

| | |
|---|---|
| Supporta le policy basate su identità | Sì |

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate su identità per Amazon EFS

Per visualizzare esempi di policy basate su identità Amazon EFS, consultare Esempi di policy basate su identità per Amazon Elastic File System.

## Policy basate su risorse all'interno di Amazon EFS

| | |
|---|---|
| Supporta le policy basate su risorse | Sì |

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Per ulteriori informazioni sull'utilizzo di una policy delle risorse per controllare l'accesso ai dati del file system, consulta Utilizzo di IAM per controllare l'accesso ai dati del file system. Per informazioni su come collegare una policy basata su risorse a un file system, consulta Creazione di policy del file system.

Esempi di policy basate su risorse all'interno di Amazon EFS

Per visualizzare esempi di policy basate su risorse Amazon EFS, consulta Esempi di policy basate su identità per Amazon Elastic File System.

## Operazioni delle policy per Amazon EFS

| | |
|---|---|
| Supporta le azioni di policy | Sì |

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di operazioni di Amazon EFS, consulta Operazioni definite da Amazon Elastic File System nella Guida di riferimento per l'autorizzazione al servizio.

Le operazioni delle policy in Amazon EFS utilizzano il seguente prefisso prima dell'operazione:

```
elasticfilesystem
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "elasticfilesystem:action1",
      "elasticfilesystem:action2"
         ]
```

Per visualizzare esempi di policy basate su identità Amazon EFS, consultare Esempi di policy basate su identità per Amazon Elastic File System.

## Risorse delle policy per Amazon EFS

| | |
|---|---|
| Supporta le risorse di policy | Sì |

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco di tipi di risorse di Amazon EFS e degli ARN, consulta Risorse definite da Amazon Elastic File System in Riferimento all'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da Amazon Elastic File System.

Per visualizzare esempi di policy basate su identità Amazon EFS, consulta Esempi di policy basate su identità per Amazon Elastic File System.

## Chiavi di condizione delle policy per Amazon EFS

| | |
|---|---|
| Supporta le chiavi di condizione delle policy specifiche del servizio | Sì |

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Per visualizzare un elenco di chiavi di condizione Amazon EFS, consulta nella Chiavi di condizione per Amazon Elastic File System nel Riferimento per l'autorizzazione al servizio. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta Operazioni definite da Amazon Elastic File System.

Per visualizzare esempi di policy basate su identità Amazon EFS, consulta Esempi di policy basate su identità per Amazon Elastic File System.

## ACL in Amazon EFS

| | |
|---|---|
| Supporta le ACL | No |

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

## ABAC con Amazon EFS

| | |
|---|---|
| Supporta ABAC (tag nelle policy) | Parziale |

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono denominati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

## Utilizzo delle credenziali temporanee con Amazon EFS

| | |
|---|---|
| Supporta le credenziali temporanee | Sì |

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWS che funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi ad AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

## Autorizzazioni delle entità principali tra servizi per Amazon EFS

| | |
|---|---|
| Supporta sessioni di accesso diretto (FAS) | Sì |

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

## Ruoli di servizio per Amazon EFS

| | |
|---|---|
| Supporta i ruoli di servizio | Sì |

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per

ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di Amazon EFS. Modifica i ruoli del servizio solo quando Amazon EFS fornisce le indicazioni per farlo.

### Ruoli collegati ai servizi per Amazon EFS

| | |
|---|---|
| Supporta i ruoli collegati ai servizi | Sì |

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per maggiori dettagli su come creare e gestire i ruoli collegati ai servizi Amazon EFS, consulta Utilizzo di ruoli collegati ai servizi per Amazon EFS.

## Esempi di policy basate su identità per Amazon Elastic File System

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse Amazon EFS. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. Per concedere agli utenti l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti da Amazon EFS, incluso il formato degli ARN per ogni tipo di risorsa, consulta Operazioni, risorse e chiavi di condizione per Amazon Elastic File System nella Guida di riferimento per l'autorizzazione del servizio.

Argomenti



## Best practice per le policy

Le policy basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon EFS all'interno dell'account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla

sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.

- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

## Utilizzo della console Amazon EFS

Per accedere alla console Amazon Elastic File System, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse Amazon EFS nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere le autorizzazioni minime della console agli utenti che effettuano chiamate solo alla AWS CLI o all'API AWS. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano continuare a utilizzare la console Amazon EFS, collega anche la policy `AmazonElasticFileSystemReadOnlyAccess` AWS gestita da Amazon EFS alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Puoi visualizzare le policy `AmazonElasticFileSystemReadOnlyAccess` dei servizi gestiti di Amazon EFS e altre in Policy gestite da AWS per Amazon EFS.

## Esempio: consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLIo l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Esempio: applicazione della creazione di file system crittografati

Nell'esempio seguente viene illustrato una policy basata sull'identità che autorizza i principali a creare solo file system crittografati.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "elasticfilesystem:CreateFileSystem",
```

```
            "Condition": {
                "Bool": {
                    "elasticfilesystem:Encrypted": "true"
                }
            },
            "Resource": "*"
        }
    ]
}
```

Se questa policy viene assegnata a un utente che tenta di creare un file system non crittografato, la richiesta ha esito negativo. L'utente visualizza un messaggio simile al seguente, indipendentemente dal fatto che stia utilizzando API o SDK AWS Management Console, AWS CLI o AWS:

```
User: arn:aws:iam::111122223333:user/username is not authorized to
      perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

## Esempio: applicazione della creazione di file system decrittografati

Nell'esempio seguente viene illustrato una policy basata sull'identità che autorizza i principali a creare solo file system decrittografati.

```
{
      "Statement": [
        {
            "Effect": "Allow",
            "Action": "elasticfilesystem:CreateFileSystem",
            "Condition": {
                "Bool": {
                    "elasticfilesystem:Encrypted": "false"
                }
            },
            "Resource": "*"
        }
    ]
}
```

Se questa policy viene assegnata a un utente che tenta di creare un file system crittografato, la richiesta ha esito negativo. L'utente visualizza un messaggio simile al seguente, indipendentemente dal fatto che stia utilizzando API o SDK AWS Management Console, AWS CLI o AWS:

```
User: arn:aws:iam::111122223333:user/username is not authorized to
      perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

Puoi anche imporre la creazione di file system Amazon EFS crittografati o non crittografati creando una policy di controllo del servizio AWS Organizations (SCP). Per ulteriori informazioni sulle policy di controllo dei servizi in AWS Organizations, consulta Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.

## Esempi di policy basate su identità per Amazon Elastic File System

In questa sezione sono disponibili policy del file system di esempio che concedono o rifiutano le autorizzazioni per diverse operazioni Amazon EFS. Le policy del file system EFS hanno un limite di 20.000 caratteri. Per informazioni sugli elementi di una policy basata sulle risorse, consulta Policy basate su risorse all'interno di Amazon EFS.

> **Important**
>
> Se si concede l'autorizzazione a un singolo utente o ruolo IAM in un criterio del file system, non eliminare o ricreare tale utente o ruolo mentre il criterio è ancora attivo sul file system. In questo caso, tale utente o ruolo viene effettivamente bloccato fuori dal file system e non sarà in grado di accedervi. Per ulteriori informazioni, vedere Specifica di un utente/gruppo/ruolo nel manuale utente IAM.

Per ulteriori informazioni sulla creazione di una policy di file system, consulta Creazione di policy del file system.

Argomenti

- Esempio: concedere l'accesso in lettura e scrittura a un ruolo AWS specifico
- Esempio 2: concedere accesso in sola lettura
- Esempio 3: concedere l'accesso a un punto di accesso EFS

### Esempio: concedere l'accesso in lettura e scrittura a un ruolo AWS specifico

In questo esempio, la policy del file system EFS dispone delle seguenti caratteristiche:

- L'effetto è `Allow`.
- L'entità principale è impostata su Testing_Role in Account AWS.
- L'operazione è impostata su `ClientMount` (lettura) e `ClientWrite`.
- La condizione per la concessione delle autorizzazioni è impostata su `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"
                }
            }
        }
    ]
}
```

## Esempio 2: concedere accesso in sola lettura

La seguente policy del file system concede solo autorizzazioni`ClientMount`, o di sola lettura, al ruolo 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"
        }
    ]
}
```

Per informazioni su come impostare ulteriori policy del file system, incluso rifiutare l'accesso root a tutti i principali IAM, ad eccezione di una workstation di gestione specifica, consulta Procedura dettagliata: abilita il root squashing utilizzando l'autorizzazione IAM per i client NFS.

## Esempio 3: concedere l'accesso a un punto di accesso EFS

Utilizzare una policy di accesso EFS per fornire a un client NFS una visualizzazione specifica dell'applicazione in set di dati condivisi basati su file in un file system EFS. Concedere le autorizzazioni del punto di accesso sul file system utilizzando una policy del file system.

Questo esempio di policy di file utilizza un elemento condizione per concedere l'accesso al file system a un punto di accesso specifico identificato dal relativo ARN completo.

Per ulteriori informazioni sui punti di accesso EFS, consulta Utilizzo dei punti di accesso 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" }
```

```
            }
        }
    ]
}
```

## Policy gestite da AWS per Amazon EFS

Una policy gestita da AWSè una policy autonoma creata e amministrata da AWS. Le policy gestite da AWSsono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWSpotrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWSaggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWSaggiorni una policy gestita da AWSquando viene lanciato un nuovo Servizio AWSo nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

### AWSpolitica gestita: AmazonElasticFileSystemFullAccess

È possibile allegare la policy `AmazonElasticFileSystemFullAccess`alle identità IAM.

Questa policy concede autorizzazioni amministrative che consentono l'accesso completo ad Amazon EFS e l'accesso ai servizi AWS correlati tramite AWS Management Console.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `elasticfilesystem`: consente alle entità principali di eseguire tutte le operazioni nella console di Amazon EFS. Consente inoltre alle entità principali di creare (`elasticfilesystem:Backup`) e ripristinare (`elasticfilesystem:Restore`) backup utilizzando AWS Backup.
- `cloudwatch`— Consente ai responsabili di descrivere i parametri e gli allarmi del CloudWatch file system di Amazon per una metrica nella console Amazon EFS.

- `ec2`— Consente ai responsabili di creare, eliminare e descrivere interfacce di rete, descrivere e modificare gli attributi dell'interfaccia di rete, descrivere zone di disponibilità, gruppi di sicurezza, sottoreti, cloud privati virtuali (VPC) e attributi VPC associati a un file system Amazon EFS nella console Amazon EFS.
- `kms`— Consente ai responsabili di elencare gli alias per le chiavi AWS Key Management Service (AWS KMS) e di descrivere le chiavi KMS nella console Amazon EFS.
- `iam`— Concede l'autorizzazione a creare un ruolo collegato al servizio che consente ad Amazon EFS di gestire risorse AWS per conto dell'utente.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

## AWSpolitica gestita: AmazonElasticFileSystemReadOnlyAccess

È possibile allegare la policy `AmazonElasticFileSystemReadOnlyAccess`alle identità IAM.

Questa policy garantisce inoltre l'accesso ad Amazon EFS tramite AWS Management Console.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `elasticfilesystem`— Consente ai responsabili di descrivere gli attributi dei file system Amazon EFS, incluse le preferenze degli account, le policy di backup e file system, la configurazione del ciclo di vita, i target di montaggio e i relativi gruppi di sicurezza, tag e punti di accesso nella console Amazon EFS.
- `cloudwatch`— Consente ai responsabili di recuperare i CloudWatch parametri e descrivere gli allarmi relativi ai parametri nella console Amazon EFS.
- `ec2`— Consente ai mandanti di visualizzare le zone di disponibilità, le interfacce di rete e i relativi attributi, i gruppi di sicurezza, le sottoreti, i VPC e i relativi attributi nella console Amazon EFS.
- `kms`— Consente alle entità principali di elencare gli alias per le chiavi AWS KMS nella console 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": "*"
        }
    ]
}
```

## AWSpolitica AmazonElasticFileSystemClientReadWrite gestita: accesso

Puoi collegare la policy `AmazonElasticFileSystemClientReadWriteAccess` anche alle tue entità IAM.

Questa policy concede ai client l'accesso di lettura e scrittura a un file system Amazon EFS. Questa policy consente ai client NFS di montare, leggere e scrivere su file system Amazon EFS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:DescribeMountTargets"
            ],
            "Resource": "*"
        }
    ]
}
```

## Aggiornamenti di Amazon EFS sulle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per Amazon EFS da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti di Amazon EFS.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Aggiornamento a una policy esistente | Politica: AmazonElasticFileSystemFullAccess<br><br>Amazon EFS ha aggiunto una nuova autorizzazione per consentire ai principali di disabilitare e abilitare la protezione su un file system. Le autorizzazioni sono necessarie per consentire ad Amazon EFS di effettuare la replica su un file system esistente. | 27 novembre 2023 |
| Aggiornamento a una policy esistente | Politica: AmazonElasticFileSystemServiceRolePolicy<br><br>Amazon EFS ha aggiunto nuove autorizzazioni per consentire ai responsabili di creare, descrivere ed eliminare repliche Amazon EFS e creare file system Amazon EFS. Le autorizzazioni sono necessarie per consentire ad Amazon EFS di gestire le configurazioni di replica dei file system per conto dell'utente. | 25 gennaio 2022 |
| Aggiornamento a una policy esistente | Politica: AmazonElasticFileSystemReadOnlyAccess<br><br>Amazon EFS ha aggiunto una nuova autorizzazione per consentire ai principali di descrivere le repliche di Amazon EFS. Le autorizzazioni sono necessarie per consentire agli utenti di visualizzare le configurazioni di replica dei file system. | 25 gennaio 2022 |
| Aggiornamento a una policy esistente | Politica: AmazonElasticFileSystemFullAccess<br><br>Amazon EFS ha aggiunto nuove autorizzazioni per consentire ai committenti di creare, descrivere ed eliminare le repliche di Amazon EFS. Le autorizza | 25 gennaio 2022 |

| Modifica | Descrizione | Data |
| --- | --- | --- |
| | zioni sono necessarie per consentire agli utenti di gestire le configurazioni di replica dei file system. | |
| Monitoraggio delle informazioni iniziato | Politica: AmazonElasticFileSystemClientReadWriteaccesso<br><br>Concede privilegi di lettura e scrittura sui file system Amazon EFS ai client NFS. | 3 gennaio 2022 |
| Monitoraggio delle informazioni iniziato | Politica: AmazonElasticFileSystemServiceRolePolicy<br><br>Autorizzazioni del ruolo collegato ai servizi per Amazon EFS. | 8 ottobre 2021 |
| Aggiornamento a una policy esistente | Politica: AmazonElasticFileSystemFullAccess<br><br>Amazon EFS ha aggiunto nuove autorizzazioni per consentire ai responsabili di modificare e descriver e le preferenze dell'account Amazon EFS. Le autorizzazioni sono necessarie per consentire agli utenti di visualizzare e configurare le impostazioni delle preferenze dell'account nella console Amazon EFS. | 7 maggio 2021 |
| Aggiornamento a una policy esistente | Politica: AmazonElasticFileSystemReadOnlyAccess<br><br>Amazon EFS ha aggiunto nuove autorizzazioni per consentire alle entità principali di descrivere le preferenze dell'account Amazon EFS. Le autorizza zioni sono necessarie per consentire agli utenti di visualizzare le impostazioni delle preferenze dell'account nella console Amazon EFS. | 7 maggio 2021 |
| Amazon EFS ha cominciato a tenere traccia delle modifiche | Amazon EFS ha iniziato a tenere traccia delle modifiche per le sue policy gestite da AWS. | 7 maggio 2021 |

# Utilizzo dei tag con Amazon EFS

È possibile utilizzare tag per controllare l'accesso alle risorse Amazon EFAC per implementare il controllo di accesso basato sugli attribute-based access control. Per ulteriori informazioni, consultare:

- Aggiunta di tag alle risorse Amazon ECS
- Controllo degli accessi in base ai tag delle risorse
- AWS? nella Guida per l'utente IAM

> **Note**
>
> La replica Amazon EFAC non supporta l'utilizzo di tag per il controllo degli accessi basato su attribute-based access control.

Per applicare i tag alle risorse Amazon EFS durante la creazione, gli utenti devono disporre di determinate autorizzazioniAWS Identity and Access Management (IAM).

## Concessione delle autorizzazioni per taggare le risorse durante la creazione

Le seguenti operazioni API Amazon EFS ti consentono di specificare tag quando crei le risorse.

- `CreateAccessPoint`
- `CreateFileSystem`

Per consentire agli utenti di applicare tag alle risorse durante la creazione, essi devono disporre delle autorizzazioni per utilizzare l'operazione che crea le risorse, come`elasticfilesystem:CreateAccessPoint` o`elasticfilesystem:CreateFileSystem`. Se i tag vengono specificati nell'azione di creazione delle risorse,AWS esegue autorizzazioni aggiuntive per l'`elasticfilesystem:TagResource`azione per verificare se gli utenti dispongono delle autorizzazioni per creare tag. Pertanto, gli utenti devono disporre anche delle autorizzazioni esplicite per utilizzare l'operazione `elasticfilesystem:TagResource`.

Nella definizione della policy IAM per l'operazione `elasticfilesystem:TagResource`, utilizzare l'elemento `Condition` con la chiave di condizione `elasticfilesystem:CreateAction` per assegnare autorizzazioni di tagging all'operazione che crea la risorsa.

Example policy: consente l'aggiunta di tag ai file system solo al momento della creazione

La seguente policy di esempio consente agli utenti di creare file system e contrassegnare tag ai file system e contrassegnare con tag i file system. Gli utenti non sono autorizzati ad applicare tag alle risorse esistenti (non possono chiamare l'operazione `elasticfilesystem:TagResource` direttamente).

```
{
  "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"
          }
       }
    }
  ]
}
```

## Utilizzo dei tag per controllare l'accesso alle risorse Amazon EFS

Per controllare l'accesso alle risorse e alle azioni di Amazon EFS, puoi utilizzare le policy IAM basate sui tag. Puoi fornire questo controllo in due modi:

- Puoi controllare l'accesso alle risorse Amazon EFS in base ai tag delle risorse.
- È possibile controllare quali tag possono essere passati in una condizione di richiesta IAM.

Per informazioni su come utilizzare i tag per controllare l'accesso alleAWS risorse, consulta Controllare l'accesso tramite tag nella Guida per l'utente IAM.

## Controllo degli accessi in base ai tag delle risorse

Per controllare quali azioni un utente o un ruolo può eseguire su una risorsa Amazon EFS, puoi utilizzare i tag sulla risorsa. Ad esempio, potresti voler consentire o negare operazioni API specifiche su una risorsa del file system in base alla coppia chiave-valore del tag sulla risorsa.

Example policy: crea un file system solo quando viene utilizzato un tag specifico

La seguente politica di esempio consente all'utente di creare un file system solo quando lo tagga con una coppia chiave-valore di tag specifica, in questo esempio`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 politica: eliminare i file system con tag specifici

La seguente policy di esempio consente all'utente di cancellare solo i file system con tag`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"
                }
```

```
            }
        }
    ]
}
```

## Utilizzo di ruoli collegati ai servizi per Amazon EFS

Amazon Elastic File System utilizza un ruolo collegato al servizioAWS Identity and Access Management (IAM). Il ruolo collegato ai servizi Amazon EFS è un tipo di ruolo IAM univoco collegato direttamente ad Amazon EFS. Il ruolo collegato ai servizi Amazon EFS include le autorizzazioni richieste dal servizio per effettuare chiamate agli altri per tuoServizi AWS conto.

Un ruolo collegato ai servizi semplifica la configurazione di Amazon EFS perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Amazon EFS definisce le autorizzazioni del ruolo collegato ai servizi e solo Amazon EFS potrà assumere tale ruolo. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Puoi eliminare il ruolo collegato ai servizi Amazon EFS solo dopo avere eliminato i file system Amazon EFS. Questa procedura protegge le risorse di Amazon EFS perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Il ruolo collegato ai servizi abilita tutte le chiamate API in modo che siano visibili tramite AWS CloudTrail. Questa procedura semplifica i requisiti di monitoraggio e controllo perché consente di tenere traccia di tutte le operazioni che Amazon EFS esegue per tuo conto. Per ulteriori informazioni, consulta Voci di registro per i ruoli collegati al servizio EFS.

### Autorizzazioni del ruolo collegato ai servizi per Amazon EFS

Amazon EFS utilizza il ruolo collegato al servizio denominato`AWSServiceRoleForAmazonElasticFileSystem` per consentire ad Amazon EFS di chiamare e gestireAWS le risorse per conto dei tuoi file system EFS.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForAmazonElasticFileSystem considera attendibili i seguenti servizi:

- `elasticfilesystem.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Amazon EFS di completare le operazioni incluse nella definizione della policy JSON:

```
{
    "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**
>
> È necessario configurare manualmente le autorizzazioni IAM per laAWS KMS creazione di un nuovo file system Amazon EFS crittografato a riposo. Per ulteriori informazioni, consulta Crittografia dei dati a riposo.

## Creazione di un ruolo collegato ai servizi per Amazon EFS

Per consentire a un'entità IAM (ad esempio un utente, un gruppo o un ruolo) di creare un ruolo collegato ai servizi. Per fare ciò, aggiungi l'`iam:CreateServiceLinkedRole`autorizzazione a un'entità IAM, come visualizzato nell'esempio seguente.

```
{
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": [
                "elasticfilesystem.amazonaws.com"
            ]
        }
    }
}
```

Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei obiettivi di montaggio o una configurazione di replica per il file system EFS nelAWS Management ConsoleAWS CLI, o nell'AWSAPI di, Amazon EFS crea il ruolo collegato ai servizi per l'utente.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei obiettivi di montaggio o una configurazione di replica per il file EFS, Amazon EFS crea di nuovo il ruolo collegato ai servizi per l'utente.

## Modifica di un ruolo collegato ai servizi per Amazon EFS

Amazon EFS non consente di modificare il ruolo`AWSServiceRoleForAmazonElasticFileSystem` collegato ai servizi. Dopo aver creato

un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

## Eliminazione di un ruolo collegato ai servizi per Amazon EFS

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio Amazon EFS utilizza tale ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse Amazon EFS utilizzate daAWSServiceRoleForAmazonElasticFileSystem

Completa i seguenti passaggi per eliminare le risorse Amazon EFS utilizzate daAWSServiceRoleForAmazonElasticFileSystem. Per la procedura dettagliata, vedereFase 4: Eliminazione delle risorse e protezione dell'account AWS.

1. Nell'istanza Amazon EC2, smonta il file system Amazon EFS.
2. Elimina il file system Amazon EFS.
3. Eliminare il gruppo di sicurezza personalizzato per il file system.

> **Warning**
>
> Se hai utilizzato il gruppo di sicurezza predefinito per il tuo VPC, non eliminare tale gruppo di sicurezza.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi AWSServiceRoleForAmazonElasticFileSystem. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

# Risoluzione dei problemi relativi all'identità e all'accesso di Amazon Elastic File System

Utilizza le informazioni seguenti per eseguire la diagnosi e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Amazon EFS e IAM.

Argomenti



## Non dispongo dell'autorizzazione per eseguire un'operazione in Amazon EFS

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `elasticfilesystem:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 elasticfilesystem:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `elasticfilesystem:`*`GetWidget`*.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire l'operazione `iam:PassRole`, per poter passare un ruolo ad Amazon EFS dovrai aggiornare le policy.

Alcuni Servizi AWSconsentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente esempio di errore si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in Amazon EFS. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Desidero consentire alle persone esterne al mio Account AWS di accedere alle mie risorse Amazon EFS

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon EFS supporta queste caratteristiche, consulta Funzionamento di Amazon Elastic File System con IAM.
- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

# Utilizzo di IAM per controllare l'accesso ai dati del file system

È possibile utilizzare policy di identità e policy delle risorse IAM per controllare l'accesso del client NFS alle risorse Amazon EFS in un modo che sia scalabile e ottimizzato per gli ambienti cloud. Utilizzando IAM, è possibile consentire ai client di eseguire operazioni specifiche su un file system, incluso l'accesso di sola lettura, scrittura e root. Un'autorizzazione «consenti» per un'azione o in una policy di identità IAM o in una policy di risorse del file system consente l'accesso a tale azione. L'autorizzazione non deve essere concessa sia in una policy di identità sia in una policy delle risorse.

I client NFS possono identificarsi utilizzando un ruolo IAM durante la connessione a un file system EFS. Quando un client si connette a un file system, Amazon EFS valuta la policy delle risorse IAM del file system (policy del file system) insieme alle eventuali policy basate su identità IAM per determinare le autorizzazioni di accesso al file system appropriate da concedere.

Quando si utilizza l'autorizzazione IAM per i client NFS, le connessioni client e le decisioni di autorizzazione IAM vengono registrate in AWS CloudTrail. Per ulteriori informazioni su come registrare le chiamate API di Amazon EFS con CloudTrail, consultaRegistrazione delle chiamate API Amazon EFS con AWS CloudTrail.

> **Important**
>
> È necessario utilizzare l'helper di montaggio EFS per montare i file system Amazon EFS al fine di utilizzare l'autorizzazione IAM per controllare l'accesso da parte dei client. Per ulteriori informazioni, consulta Montaggio con autorizzazione IAM.

## Policy del file system EFS predefinita

La Policy EFS predefinita del file system EFS non utilizza IAM per l'autenticazione e consente l'accesso completo a qualsiasi client anonimo in grado di connettersi al file system utilizzando una destinazione di montaggio. La policy predefinita è effettiva ogni volta che non esiste una policy di file system configurata dall'utente, anche a livello di creazione del file system. Ogni volta che la policy del file system predefinita è in essere, un'operazione API `DescribeFileSystemPolicy` restituisce una risposta `PolicyNotFound`.

## Operazioni EFS per client

È possibile specificare le seguenti operazioni per i client in un file system utilizzando una policy del file system.

| Azione | Descrizione |
| --- | --- |
| `elasticfilesystem:ClientMount` | Fornisce un accesso in sola lettura a un file system. |
| `elasticfilesystem:ClientWrite` | Fornisce le autorizzazioni di scrittura su un file system. |
| `elasticfilesystem:ClientRootAccess` | Fornisce la possibilità di utilizzare l'utente root quando si accede a un file system. |

## Chiavi di condizione EFS per client

Per esprimere le condizioni è necessario utilizzare chiavi di condizione predefinite. Amazon EFS dispone delle seguenti chiavi di condizione predefinite per i client NFS. Qualsiasi altra chiave di condizione non viene applicata quando si utilizzano i controlli IAM per proteggere l'accesso ai file system EFS.

| Chiave di condizione EFS | Descrizione | Operatore |
| --- | --- | --- |
| `aws:SecureTransport` | Utilizzare questa chiave per richiedere ai client NFS di utilizzare TLS durante la connessione a un file system EFS. | Booleano |
| `aws:SourceIp` | Indirizzo IP privato del client che accede a un file system EFS. | Stringa |
| `elasticfilesystem:AccessPointArn` | ARN del punto di accesso EFS a cui il client si connette. | Stringa |
| `elasticfilesystem:AccessedViaMountTarget` | Utilizza questa chiave per impedire l'accesso a un file system EFS da parte di client | Booleano |

| Chiave di condizione EFS | Descrizione | Operatore |
| --- | --- | --- |
| | che non utilizzano destinazioni di montaggio del file system. | |

## Esempi di policy del file system

Per visualizzare esempi di policy dei file system di Amazon EFS, consulta Esempi di policy basate su identità per Amazon Elastic File System.

# Controllo dell'accesso di rete ai file system Amazon EFS per i client NFS

È possibile controllare l'accesso da client NFS ai file system Amazon EFS utilizzando policy di sicurezza e del file system EFS del livello di rete. È possibile utilizzare i meccanismi di sicurezza del livello di rete disponibili con Amazon EC2, ad esempio le regole del gruppo di sicurezza VPC e le liste di controllo degli accessi di rete. Puoi anche utilizzare AWS IAM per controllare l'accesso NFS con una policy del file system EFS e policy basate sull'identità.

Argomenti

- Utilizzo di gruppi di sicurezza VPC per istanze Amazon EC2 e destinazioni di montaggio
- Porte di origine per lavorare con EFS
- Considerazioni relative alla sicurezza per l'accesso di rete
- Utilizzo degli endpoint VPC di interfaccia in Amazon EFS

## Utilizzo di gruppi di sicurezza VPC per istanze Amazon EC2 e destinazioni di montaggio

Quando si utilizza Amazon EFS, è necessario specificare i gruppi di sicurezza Amazon EC2 per le istanze EC2 e i gruppi di sicurezza per le destinazioni di montaggio EFS associate al file system. Un gruppo di sicurezza funge da firewall e le regole aggiunte definiscono il flusso di traffico. Nell'esercitazione sulle nozioni di base, è stato creato un gruppo di sicurezza quando è stata avviata l'istanza di EC2. Ne è quindi stato associato un altro alla destinazione di montaggio EFS (ossia il gruppo di sicurezza di default della VPC). Questo approccio funziona per l'esercitazione sulle

nozioni di base. Tuttavia, per un sistema di produzione, è necessario configurare i gruppi di sicurezza riducendo al minimo le autorizzazioni all'uso di EFS.

È possibile autorizzare l'accesso in entrata e in uscita verso il file system EFS. Per farlo, è sufficiente aggiungere regole che consentono all'istanza di EC2 di connettersi al file system Amazon EFS tramite la destinazione di montaggio utilizzando la porta NFS (Network File System). Seguire i seguenti passi per creare e aggiornare i gruppi di sicurezza.

Per creare gruppi di sicurezza per istanze EC2 e destinazioni di montaggio

1. Creare due gruppi di sicurezza nella VPC.

   Per istruzioni, consulta la procedura "Per creare un gruppo di sicurezza" nella sezione Creazione di un gruppo di sicurezza nella Guida per l'utente di Amazon VPC.
2. Apri la console di gestione Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/ e verifica le regole predefinite per questi gruppi di sicurezza. Entrambi i gruppi di sicurezza dovrebbero avere solo una regola in uscita che consente l'uscita del traffico.

Per aggiornare gli accessi necessari dei gruppi di sicurezza

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Aggiungere una regola al gruppo di sicurezza di EC2 per consentire l'accesso in entrata utilizzando SSH (Secure Shell) da qualsiasi host. Facoltativamente, è possibile limitare l'indirizzo Source (Origine).

   Non è necessario aggiungere una regola in uscita, perché la regola di default consente l'uscita di tutto il traffico. In caso contrario, è necessario aggiungere una regola in uscita per aprire la connessione TCP sulla porta NFS, identificando come destinazione il gruppo di sicurezza della destinazione di montaggio.

   Per istruzioni, consulta Aggiunta ed eliminazione delle regole nella Guida per l'utente di Amazon VPC.
3. Aggiungi regole in entrata e in uscita per la destinazione di montaggio.

   - Aggiungi una regola per il gruppo di sicurezza della destinazione di montaggio per consentire l'accesso in entrata dal gruppo di sicurezza di EC2. Identifica il gruppo di sicurezza EC2 come origine.

- Aggiungi una regola in uscita per aprire la connessione TCP su tutte le porte NFS. Identifica il gruppo di sicurezza EC2 come origine.

  Per istruzioni, consulta Aggiunta ed eliminazione delle regole nella Guida per l'utente di Amazon VPC.

4. Verificare che entrambi i gruppi di sicurezza autorizzino l'accesso in entrata e in uscita.

Per ulteriori informazioni sui gruppi di sicurezza, consulta Gruppi di sicurezza per EC2-VPC nella Guida per l'utente di Amazon EC2 per istanze Linux.

## Porte di origine per lavorare con EFS

Per supportare un'ampia gamma di client NFS, Amazon EFS consente connessioni da qualsiasi porta di origine. Se si richiede che solo gli utenti privilegiati possano accedere ad Amazon EFS, consigliamo di utilizzare le seguenti regole di firewall per il client. Connettiti al file system tramite SSH ed esegui questo comando:

```
iptables -I OUTPUT 1 -m owner --uid-owner 1-4294967294 -m tcp -p tcp --dport 2049 -j
 DROP
```

Questo comando inserisce una nuova regola all'inizio della catena di OUTPUT (`-I OUTPUT 1`). La regola impedisce a qualsiasi processo non privilegiato e non-kernel (`-m owner --uid-owner 1-4294967294`) di aprire una connessione alla porta NFS (`-m tcp -p tcp –dport 2049`).

## Considerazioni relative alla sicurezza per l'accesso di rete

Un client NFS versione 4.1 (NFSv4.1) può montare un file system solo se è in grado di aprire una connessione di rete alla porta NFS (porta TCP 2049) di una delle destinazioni di montaggio del file system. Analogamente, un client NFSv4.1 client può far valere un ID utente e di gruppo per l'accesso a un file system solo se è in grado di instaurare tale connessione di rete.

La possibilità di attivare questa connessione di rete è disciplinata da una combinazione dei seguenti elementi:

- Isolamento di rete fornito dalla VPC delle destinazioni di montaggio - Le destinazioni di montaggio del file system non possono avere indirizzi IP pubblici associati ad esse. Le uniche destinazioni su cui è possibile montare i file system sono le seguenti:

  - Istanze Amazon EC2 nella stessa Amazon VPC locale
  - Istanze EC2 nelle VPC connesse
  - Server locali connessi a un Amazon VPC AWS Direct Connect tramite e AWS Virtual Private Network una (VPN)
- Liste di controllo degli accessi di rete (ACL) per le sottoreti della VPC del client e delle destinazioni di montaggio, per l'accesso dall'esterno alle sottoreti delle destinazioni di montaggio - Per montare un file system, il client deve essere in grado di effettuare una connessione TCP alla porta NFS di una destinazione di montaggio e di ricevere il traffico di ritorno.
- Regole dei gruppi di sicurezza VPC del client e delle destinazioni di montaggio per tutti gli accessi – Per montare un file system su un'istanza EC2, devono essere attive le seguenti regole dei gruppi di sicurezza:
  - Il file system deve disporre di una destinazione di montaggio la cui interfaccia di rete dispone di un gruppo di sicurezza con una regola che consente le connessioni in entrata sulla porta NFS dall'istanza. È possibile abilitare le connessioni in entrata sulla base dell'indirizzo IP (intervallo CIDR) o del gruppo di sicurezza. L'origine delle regole del gruppo di sicurezza per le regole in ingresso sulla porta NFS dell'interfaccia di rete della destinazione di montaggio è un elemento chiave del controllo degli accessi al file system. Le regole per il traffico in entrata diverse da quella sulla porta NFS e tutte le regole in uscita, non vengono utilizzate dalle interfacce di rete per le destinazioni di montaggio del file system.
  - L'istanza che esegue il montaggio del file system deve disporre di un'interfaccia di rete con una regola del gruppo di sicurezza che consente le connessioni in uscita verso la porta NFS su una delle destinazioni di montaggio del file system. È possibile abilitare le connessioni in uscita sulla base dell'indirizzo IP (intervallo CIDR) o del gruppo di sicurezza.

Per ulteriori informazioni, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

## Utilizzo degli endpoint VPC di interfaccia in Amazon EFS

Per stabilire una connessione privata tra il cloud privato virtuale (VPC) e l'API Amazon EFS, puoi creare un endpoint VPC dell'interfaccia. L'endpoint offre una connettività sicura all'API Amazon EFS senza richiedere un Internet gateway, un'istanza NAT o una connessione di rete privata virtuale (VPN). Per ulteriori informazioni, consulta Endpoint VPC di interfaccia nella Guida per l'utente di Amazon VPC.

Gli endpoint VPC dell'interfaccia si basano sulla tecnologiaAWSPrivateLink, una tecnologia che abilita la comunicazione privata traAWS i servizi che utilizzano indirizzi IP privati. Per

utilizzarloAWSPrivateLink, crea un endpoint VPC di interfaccia per Amazon EFS nel tuo VPC utilizzando la console, l'API o l'interfaccia a riga di comando di Amazon VPC. In questo modo si crea un'elastic network interface nella sottorete con un indirizzo IP privato che serve le richieste API Amazon EFS. È inoltre possibile accedere a un endpoint VPC da ambienti locali o da altri VPC utilizzando AWS VPN, AWS Direct Connect o il peering di VPC. Per ulteriori informazioni, consulta Accessing Services ThroughAWSPrivateLink nella Amazon VPC User Guide.

## Creazione di un endpoint di interfaccia per Amazon EFS

Per creare un endpoint VPC dell'interfaccia per Amazon EFS, utilizza uno dei seguenti:

- **`com.amazonaws.`*`region`*`.elasticfilesystem`**— Crea un endpoint per le operazioni delle API Amazon EFS.
- **`com.amazonaws.`*`region`*`.elasticfilesystem-fips`**— Creazione un endpoint per l'API Amazon EFS conforme agli standard FIPS (Federal Information Processing Standard) 140-2.

Per un elenco completo degli endpoint Amazon EFS, consulta Amazon Elastic File System nel Riferimenti generali di Amazon Web Services.

Per ulteriori informazioni su come creare un endpoint di interfaccia, consulta Creating an Interface Endpoint nella Amazon VPC User Guide.

## Creazione di una policy di endpoint VPC per Amazon EFS

Per controllare l'accesso all'API Amazon EFS, puoi collegare una policyAWS Identity and Access Management (IAM) all'endpoint VPC. La policy specifica quanto segue:

- Il principale che può eseguire operazioni.
- Le operazioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, consultare Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Nell'esempio seguente viene illustrato una policy di endpoint VPC che nega a chiunque l'autorizzazione per creare un sistema di file EFS tramite l'endpoint. Inoltre, la policy di esempio concede a chiunque l'autorizzazione per eseguire tutte le altre operazioni.

```
{
```

```
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "elasticfilesystem:CreateFileSystem",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
```

Per ulteriori informazioni, consulta Utilizzo delle policy dell'endpoint VPC nella Guida per l'utente di Amazon VPC.

# Utilizzo di utenti, gruppi e autorizzazioni a livello di Network File System (NFS)

Argomenti

- Autorizzazioni di file e directory
- Casi d'uso di esempio del file system Amazon EFS e autorizzazioni
- Autorizzazioni per ID utente e gruppo su file e directory all'interno di un file system
- No Root Squashing
- Caching delle autorizzazioni
- Modifica della proprietà degli oggetti del file system
- Punti di accesso EFS

Alla creazione di un file system, per impostazione predefinita, solo l'utente root (UID 0) dispone delle autorizzazioni di lettura, scrittura ed esecuzione. Affinché gli altri utenti possano modificare il file system, l'utente root deve esplicitamente concedere loro l'accesso. È possibile utilizzare i punti di accesso per automatizzare la creazione di directory da cui un utente non root può scrivere. Per ulteriori informazioni, consulta Utilizzo dei punti di accesso Amazon EFS.

Gli oggetti del file system Amazon EFS hanno una modalità di tipo Unix associata ad essi. Questo valore di modalità definisce le autorizzazioni per l'esecuzione di azioni su quell'oggetto. Gli utenti che hanno familiarità con i sistemi tipo UNIX possono comprendere facilmente come Amazon EFS si comporta rispetto a queste autorizzazioni.

Inoltre, sui sistemi in stile Unix, utenti e i gruppi sono mappati a identificatori numerici, che sono impiegati da Amazon EFS per rappresentare la proprietà dei file. Per Amazon EFS, gli oggetti del file system (ovvero file, directory e così via) sono di proprietà di un singolo proprietario e di un singolo gruppo. Amazon EFS utilizza questi ID numerici per controllare le autorizzazioni quando un utente cerca di accedere a un oggetto del file system.

> **Note**
>
> Il protocollo NFS supporta un massimo di 16 ID di gruppo (GID) per utente e tutti i GID aggiuntivi vengono troncati dalle richieste dei client NFS. Per ulteriori informazioni, consulta Accesso negato ai file consentiti sul file system NFS.

Di seguito sono disponibili esempi di autorizzazioni e una discussione sulle considerazioni sulle autorizzazioni NFS per Amazon EFS.

## Autorizzazioni di file e directory

I file e le directory in un file system EFS supportano le autorizzazioni di lettura, scrittura ed esecuzione di tipo Unix standard in base all'ID utente e all'ID gruppo rivendicati dal client NFSv4.1 che ha eseguito il montaggio, a meno che non sia sostituito dal punto di accesso EFS.  Per ulteriori informazioni, consulta Utilizzo di utenti, gruppi e autorizzazioni a livello di Network File System (NFS).

> **Note**
>
> Per impostazione predefinita, questo livello di controllo degli accessi dipende dall'affidabilità del client NFSv4.1 nella sua rivendicazione dell'ID utente e gruppo. Puoi utilizzare policy basate su risorse AWS Identity and Access Management (IAM) e policy di identità per autorizzare i client NFS e fornire autorizzazioni di sola lettura, scrittura e accesso root. È possibile utilizzare i punti di accesso EFS per sovrascrivere le informazioni sull'identità di gruppo e utente del sistema operativo fornite dal client NFS. Per ulteriori informazioni, consultare Utilizzo di IAM per controllare l'accesso ai dati del file system e Creazione ed eliminazione dei punti di accesso.

Come esempio di autorizzazioni di lettura, scrittura ed esecuzione su i file e cartelle, Alice può avere le autorizzazioni di lettura e scrittura su tutti i file che desidera nella sua cartella personale su un file system, `/alice`. Tuttavia, in questo esempio, ad Alice non è consentita la lettura o la scrittura su qualsiasi file nella cartella personale di Mark sullo stesso file system, `/mark`. Sia ad Alice che a Mark è consentito leggere ma non scrivere i file nella cartella condivisa `/share`.

## Casi d'uso di esempio del file system Amazon EFS e autorizzazioni

Dopo aver creato un file system Amazon EFS e le destinazioni di montaggio del file system in VPC, è possibile montare il file system remoto in locale sull'istanza Amazon EC2. Il comando `mount` può montare qualsiasi cartella presente nel file system. Tuttavia, quando si crea il file system, è disponibile solo una cartella principale all'indirizzo `/`. L'utente root e il gruppo root sono proprietari della directory montata.

Il seguente comando `mount` monta la cartella principale di un file system Amazon EFS, identificato dal nome DNS del file system, sulla directory locale `/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
```

Le autorizzazioni iniziali attribuiscono:

- autorizzazioni di `read-write-execute` per il proprietario root
- autorizzazioni di `read-execute` per il gruppo root
- autorizzazioni di `read-execute` per gli altri utenti

Solo l'utente root può modificare questa directory. L'utente root può anche concedere le autorizzazioni di scrittura su questa directory ad altri utenti, ad esempio:

- Creare sottocartelle con possibilità di scrittura per gli utenti. Per istruzioni, vedere. step-by-step Scenario: creazione di sottocartelle con possibilità di scrittura per gli utenti e configurazione del montaggio automatico al riavvio
- Consentire agli utenti di scrivere sulla cartella root del file system Amazon EFS. Un utente con privilegi di root può concedere ad altri utenti l'accesso al file system.
  - Per modificare la proprietà del file system Amazon EFS intestandola a un utente e gruppo non-root, utilizzare la seguente procedura:

```
$ sudo chown user:group /EFSroot
```

- Per modificare le autorizzazioni del file system per renderlo un po' più permissivo, utilizzare il seguente comando:

  ```
  $ sudo chmod 777 /EFSroot
  ```

  Questo comando concede read-write-execute i privilegi a tutti gli utenti su tutte le istanze EC2 su cui è montato il file system.

## Autorizzazioni per ID utente e gruppo su file e directory all'interno di un file system

I file e le directory in un file system Amazon EFS supportano le autorizzazioni in lettura, scrittura ed esecuzione standard di tipo Unix in base all'ID utente e agli ID gruppo. Quando un client NFS monta un file system EFS senza utilizzare un punto di accesso, l'ID utente e l'ID gruppo forniti dal client sono attendibili. I punti di accesso EFS possono essere anche utilizzati per eseguire l'override dell'ID utente e degli ID gruppo utilizzati dal client NFS. Quando un utente cerca di accedere a file e cartelle, Amazon EFS controlla il suo ID utente e ID gruppo per verificare che l'utente abbia l'autorizzazione per accedere agli oggetti. Amazon EFS utilizza inoltre tali ID per impostare il valori di proprietario e gruppo del proprietario per i nuovi file e le nuove cartelle creati dall'utente. Amazon EFS non esamina i nomi dell'utente o del gruppo, utilizza esclusivamente gli identificatori numerici.

> **Note**
>
> Quando crei un utente su un'istanza EC2, puoi assegnare all'utente qualunque ID utente (user ID, UID) e ID gruppo (group ID, GID) numerico. Sui sistemi Linux, gli ID utente numerici sono impostati nel file `/etc/passwd`. Gli ID numerici dei gruppo si trovano nel file `/etc/group`. Questi file definiscono il mapping tra nomi e ID. Al di fuori dell'istanza EC2, Amazon EFS non esegue alcuna autenticazione di questi ID, incluso l'ID 0 appartenente all'utente root.

Se un utente accede a un file system Amazon EFS da due diverse istanze EC2, si può osservare un comportamento diverso a seconda se l'UID per l'utente è lo stesso o diverso, nel seguente modo:

- Se gli ID utente sono gli stessi su entrambe le istanze EC2, Amazon EFS li considera come indicativi dello stesso utente, indipendentemente dall'istanza EC2 utilizzata. L'esperienza utente relativamente all'accesso al file system è lo stesso da entrambe le istanze EC2.
- Se gli ID utente non sono gli stessi, Amazon EFS considera gli utenti come diversi. L'esperienza utente non è la stessa quando si accede al file system Amazon EFS da due istanze EC2 diverse.
- Se due utenti diversi su diverse istanze EC2 condividono un ID, Amazon EFS li considera come se fossero lo stesso utente.

Una gestione coerente delle mappature di ID degli utenti sulle diverse istanze EC2 dovrebbe essere presa in seria considerazione. Gli utenti possono controllare il loro ID numerico utilizzando il comando `id`.

```
$ id

uid=502(joe) gid=502(joe) groups=502(joe)
```

### Disattivare l'ID Mapper

Le utility NFS incluse nel sistema operativo includono un daemon chiamato ID Mapper che gestisce la mappatura tra i nomi e gli ID degli utenti. Su Amazon Linux, il daemon viene chiamato `rpc.idmapd` e su Ubuntu viene chiamato `idmapd`. Tale daemon traduce gli ID di utenti e gruppi in nomi e viceversa. Tuttavia, Amazon EFS opera solo con gli ID numerici. È consigliabile disattivare il processo sulle istanze EC2. Su Amazon Linux, di solito l'ID mapper è disabilitato; se lo è, non va abilitato. Per disattivare l'ID mapper, utilizzare i comandi riportati di seguito.

```
$  service rpcidmapd status
$  sudo service rpcidmapd stop
```

## No Root Squashing

Per impostazione predefinita, il root squashing è disabilitato sui file system EFS. Amazon EFS si comporta come un server NFS Linux con `no_root_squash`. Se un ID utente o di gruppo è 0, Amazon EFS considera tale utente come `root` e ignora le verifiche delle autorizzazioni (consentendo l'accesso e la modifica a tutti gli oggetti del file system). Il root squashing può essere abilitato su una connessione client quando la politica delle identità o delle risorse AWS Identity and Access Management (AWS IAM) non consente l'accesso all'azione. `ClientRootAccess` Quando il root

squashing è abilitato, l'utente root viene trasformato in un utente con autorizzazioni limitate sul server NFS.

Per ulteriori informazioni, consultare Utilizzo di IAM per controllare l'accesso ai dati del file system e Procedura dettagliata: abilita il root squashing utilizzando l'autorizzazione IAM per i client NFS.

### Caching delle autorizzazioni

Amazon EFS memorizza nella cache le autorizzazioni sui file per un piccolo intervallo di tempo. Di conseguenza, ci potrebbe essere una breve finestra temporale in cui un utente che aveva accesso a un oggetto del file system, ma il cui accesso è stato revocato di recente, può ancora accedere a quell'oggetto.

### Modifica della proprietà degli oggetti del file system

Amazon EFS applica l'attributo POSIX `chown_restricted`. Questo significa solo l'utente root può modificare il proprietario di un oggetto del file system. Il root dell'utente proprietario può modificare il gruppo proprietario di un oggetto del file system. Tuttavia, a meno che l'utente non sia un utente root, il gruppo può essere modificato solo in un gruppo di cui sia membro l'utente proprietario.

### Punti di accesso EFS

Un punto di accesso applica un utente del sistema operativo, gruppo e percorso del file system a qualsiasi richiesta di file system effettuata utilizzando il punto di accesso. L'utente e il gruppo per sistema operativo del punto di accesso sostituiscono le eventuali informazioni di identità fornite dal client NFS. Il percorso file system viene esposto al client come la directory radice del punto di accesso. Con questo approccio ogni applicazione utilizza sempre l'identità del sistema operativo corretta e la directory corretta durante l'accesso a set di dati basati su file condivisi. Le applicazioni che utilizzano il punto di accesso possono accedere ai dati solo nella propria directory e sotto a questa. Per ulteriori informazioni sui punti di accesso, consulta la sezione Utilizzo dei punti di accesso Amazon EFS.

## Utilizzo dei punti di accesso Amazon EFS

I punti di accesso Amazon EFS sono punti di accesso specifici dell'applicazione in un file system EFS che semplificano la gestione dell'accesso dell'applicazione ai set di dati condivisi. I punti di accesso possono applicare un'identità utente, inclusi i gruppi dell'utente POSIX, per tutte le richieste al file system effettuate tramite il punto di accesso. I punti di accesso possono inoltre applicare una

directory radice diversa per il file system in modo che i client possano accedere solo ai dati nella directory specificata o nelle sue sottodirectory.

È possibile utilizzare politicheAWS Identity and Access Management (IAM) per imporre che applicazioni specifiche utilizzino un punto di accesso specifico. Combinando le policy IAM con i punti di accesso, puoi fornire facilmente accesso sicuro a set di dati specifici per le applicazioni.

> **Note**
>
> È necessario creare almeno un target di montaggio sul file system EFS per utilizzare i punti di accesso.

Per ulteriori informazioni sulla creazione di un punto di accesso, consultare Creazione ed eliminazione dei punti di accesso.

Argomenti

- Creazione di un access point
- Montaggio di un file system utilizzando un punto di accesso
- Far rispettare l'identità di un utente utilizzando un punto di accesso
- Applicazione di una directory principale con un punto di accesso
- Utilizzo dei punti di accesso nelle policy IAM

## Creazione di un access point

Puoi creare punti di accesso per un file system Amazon EFS esistente utilizzando l'AWS Management ConsoleAPI,AWS Command Line Interface (AWS CLI) e EFS. Un file system Amazon EFS può avere un massimo massimo di essi access point point. Non è possibile modificare un punto di accesso esistente dopo averlo creato.

Per step-by-step le procedure per creare un punto di accesso, vedereCreazione ed eliminazione dei punti di accesso.

## Montaggio di un file system utilizzando un punto di accesso

Utilizza l'assistente per il montaggio di EFS durante il montaggio di un file system mediante un punto di accesso. Nel comando di montaggio, includere l'ID del file system, l'ID del punto di accesso e l'opzione di montaggio `tls`, mostrata nell'esempio seguente.

```
$ mount -t efs -o tls,iam,accesspoint=fsap-abcdef0123456789a fs-
abc0123def456789a: /localmountpoint
```

Per ulteriori informazioni sul montaggio di file system mediante un punto di accesso, consulta Montaggio con punti di accesso EFS.

## Far rispettare l'identità di un utente utilizzando un punto di accesso

Puoi utilizzare un punto di accesso per applicare le informazioni relative a utente e gruppo per tutte le richieste di file system effettuate tramite il punto di accesso. Per abilitare questa caratteristica, è necessario specificare l'identità del sistema operativo da applicare durante la creazione del punto di accesso.

Come parte di questo, fornire quanto segue:

- ID utente: l'ID utente POSIX numerico per l'utente.
- ID gruppo: l'ID numerico del gruppo POSIX per l'utente.
- ID di gruppo secondari: un elenco opzionale di ID di gruppo secondari.

Quando l'applicazione degli utenti è abilitata, Amazon EFS sostituisce gli ID utente e di gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni del file system. L'imposizione utente ha anche i seguenti effetti:

- Il proprietario e il gruppo per i nuovi file e directory vengono impostati sull'ID utente e sull'ID gruppo del punto di accesso.
- EFS considera l'ID utente, l'ID gruppo e gli ID gruppi secondari del punto di accesso durante la valutazione delle autorizzazioni del file system. EFS ignora gli ID del client NFS.

> **Important**
>
> L'applicazione di un'identità utente è soggetta all'autorizzazione IAM `ClientRootAccess`. Ad esempio, in alcuni casi è possibile configurare l'ID utente del punto di accesso, l'ID del gruppo o entrambi in modo che siano impostati su “radice” (ovvero impostando UID, GID o entrambi su 0). In questi casi, è necessario concedere l'autorizzazione `ClientRootAccess` al client NFS.

# Applicazione di una directory principale con un punto di accesso

Puoi utilizzare un punto di accesso per sovrascrivere la directory radice di un file system. Quando applichi una directory radice, il client NFS che utilizza il punto di accesso usa la directory radice configurata sul punto di accesso anziché la directory radice del file system.

Abilita questa caratteristica impostando l'attributo `Path` del punto di accesso durante la creazione di un punto di accesso. L'attributo `Path` è il percorso completo della directory radice del file system per tutte le richieste di file system effettuate attraverso questo punto di accesso. Il percorso completo non può superare i 100 caratteri. Può includere fino a quattro sottodirectory.

Quando specifichi una directory radice su un punto di accesso, questa diventa la directory radice del file system per il client NFS che monta il punto di accesso. Ad esempio, supponiamo che la directory principale del punto di accesso sia `/data`. In questo caso, il montaggio `fs-12345678:/` utilizzando il punto di accesso ha lo stesso effetto del montaggio `fs-12345678:/data` senza utilizzare il punto di accesso.

Quando specifichi una directory root nel punto di accesso, assicurati che le autorizzazioni della directory siano configurate per consentire all'utente del punto di accesso di eseguire il montaggio correttamente il file system. In particolare, assicurati che il bit di esecuzione sia impostato per l'utente o il gruppo del punto di accesso o per tutti. Ad esempio, il valore di autorizzazione della directory 755 consente all'utente proprietario della directory di elencare i file, creare file ed eseguire il montaggio e a tutti gli altri utenti di elencare i file ed eseguire il montaggio.

## Creazione della directory principale per un punto di accesso

Se nel file system non esiste un percorso di directory principale per un punto di accesso, Amazon EFS crea automaticamente tale directory radice con la proprietà e le autorizzazioni specificate. Amazon EFS non creerà la directory principale se non si specificano la proprietà e le autorizzazioni della directory al momento della creazione. Con questo approccio è possibile effettuare il provisioning dell'accesso al file system per un utente o un'applicazione specifici senza montare il file system da un host Linux. Per creare una directory principale, è necessario configurare la proprietà e l'autorizzazione della directory principale utilizzando i seguenti attributi durante la creazione di un punto di accesso:

- `OwnerUid`— L'ID utente POSIX numerico da utilizzare come proprietario della directory principale.
- `OwnerGiD`— L'ID numerico del gruppo POSIX da utilizzare come gruppo proprietario della directory principale.

- Autorizzazioni: la modalità Unix della directory. Una configurazione comune è 755. Assicurati che il bit di esecuzione sia impostato per l'utente del punto di accesso in modo che sia in grado di eseguire il montaggio. Questa configurazione dà al proprietario della directory il permesso di inserire, elencare e scrivere nuovi file nella directory. Dà a tutti gli altri utenti il permesso di inserire ed elencare i file. Per ulteriori informazioni sull'utilizzo delle modalità file e directory Unix, consulta Utilizzo di utenti, gruppi e autorizzazioni a livello di Network File System (NFS).

Amazon EFS crea una directory principale del OwnUid punto di accesso solo se vengono specificati una directory. Se non fornisci queste informazioni, Amazon EFS non crea la directory principale. Se la directory principale non esiste, i tentativi di montaggio utilizzando il punto di accesso avranno esito negativo.

Quando si installa un file system con un punto di accesso, la directory principale del punto di accesso viene creata se la directory non esiste già, a condizione che la directory principale OwnerUid e le autorizzazioni siano state specificate al momento della creazione del punto di accesso. Se la directory principale del punto di accesso esiste già prima del montaggio, le autorizzazioni esistenti non vengono sovrascritte dal punto di accesso. Se elimini la directory radice, questa verrà ricreata da EFS la prossima volta che il file system viene montato utilizzando il punto di accesso.

> **Note**
>
> Se non specifichi la proprietà e autorizzazioni per la directory principale del punto di accesso point, Amazon EFS non creerà la directory principale. Tutti i tentativi di montaggio del punto di accesso avranno esito negativo.

## Modello di sicurezza per le directory principali dei punti di accesso

Quando è attiva l'override della directory principale, Amazon EFS si comporta come un server NFS Linux con l'`no_subtree_check`opzione abilitata.

Nel protocollo NFS, i server generano handle di file utilizzati dai client come riferimenti univoci quando si accede ai file. EFS genera in modo sicuro gli handle di file che sono imprevedibili e specifici di un file system EFS. Quando è in essere un override della directory radice, EFS non rivela gli handle di file per i file esterni alla directory radice specificata. Tuttavia, in alcuni casi un utente potrebbe ottenere un handle per un file esterno al proprio punto di accesso utilizzando un out-of-band meccanismo. Ad esempio, potrebbero farlo se hanno accesso a un secondo punto di accesso. Se lo fanno, possono eseguire operazioni di lettura e scrittura sul file.

La proprietà del file e le autorizzazioni di accesso vengono sempre applicate, per accedere ai file all'interno e all'esterno della directory radice del punto di accesso di un utente.

## Utilizzo dei punti di accesso nelle policy IAM

Puoi utilizzare una policy IAM per stabilire che un client NFS specifico, identificato dal suo ruolo IAM, può accedere solo a un punto di accesso specifico. A tale scopo, è possibile utilizzare la chiave di condizione `elasticfilesystem:AccessPointArn` IAM. `AccessPointArn` è l'Amazon Resource Name (ARN) del punto di accesso con cui è montato il file system.

Di seguito è riportato un esempio di un criterio di file system che consente al ruolo IAM `app1` di accedere al file system utilizzando il punto di accesso `fsap-01234567`. La policy consente inoltre a `app2` di utilizzare il file system utilizzando il punto di accesso `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"
                }
            }
        }
    ]
}
```

# Blocco dell'accesso pubblico

La funzionalità di blocco dell'accesso pubblico di Amazon EFS offre impostazioni per semplificare la gestione dell'accesso pubblico ai file system Amazon EFS. Per impostazione predefinita, i nuovi file system Amazon EFS non consentono l'accesso pubblico. Tuttavia, è possibile modificare le policy del file system per consentire l'accesso pubblico.

Argomenti

- Blocco dell'accesso pubblico conAWS Transfer Family
- Significato di "pubblico"

## Blocco dell'accesso pubblico conAWS Transfer Family

Quando usi Amazon EFS conAWS Transfer Family, le richieste di accesso al file system ricevute da un server Transfer Family di proprietà di un account diverso da quello del file system vengono bloccate se il file system consente l'accesso pubblico. Amazon EFS valuta le politiche IAM del file system e, se la politica è pubblica, blocca la richiesta. Per permettereAWS Transfer Familyaccesso al file system, aggiorna il criterio del file system in modo che non sia considerato pubblico.

> **Note**
>
> L'utilizzo di Transfer Family con Amazon EFS è disabilitato per impostazione predefinita perAccount AWSs che dispongono di file system EFS con criteri che consentono l'accesso pubblico creati prima del 6 gennaio 2021. Per abilitare l'utilizzo di Transfer Family per accedere al file system, contattareAWSSupport.

# Significato di "pubblico"

Quando si valuta se un file system consente l'accesso pubblico, Amazon EFS presuppone che la politica del file system sia pubblica. Quindi valuta la policy del file system per determinare se si qualifica come non pubblica. Per essere considerata non pubblica, la policy del file system deve concedere l'accesso solo a valori fissi (valori che non contengono jolly) di uno o più degli elementi seguenti:

- Un set di Classless Inter-Domain Routing (CIDR) tramite `aws:SourceIp`. Per ulteriori informazioni sui CIDR, consulta RFC 4632 nel sito Web RFC Editor.
- Un recordAWSl'entità principale, l'utente, il ruolo o l'entità principale del servizio (ad esempio,`aws:PrincipalOrgID`)
- `aws:SourceArn`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:SourceOwner`
- `aws:SourceAccount`
- `elasticfilesystem:AccessedViaMountTarget`
- `aws:userid, outside the pattern "AROLEID:*"`

In queste regole le policy di esempio seguenti sono considerate pubbliche.

```
{
    "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"
            ]
```

```
        }
    ]
}
```

È possibile rendere questo criterio del file system non pubblico utilizzando la chiave di condizione EFS`elasticfilesystem:AccessedViaMountTarget`impostata su true. É possibile utilizzare`elasticfilesystem:AccessedViaMountTarget`per consentire le azioni EFS specificate ai client che accedono al file system EFS utilizzando una destinazione di montaggio del file system. La seguente politica non pubblica utilizza il`elasticfilesystem:AccessedViaMountTarget`key di condizione impostata su 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"
                }
            }
        }
    ]
}
```

Per ulteriori informazioni sulle chiavi di condizione Amazon EFS, consultaChiavi di condizione EFS per client. Per ulteriori informazioni sulla creazione di policy del file system, consultareCreazione di policy del file system.

# Convalida della conformità per Amazon Elastic File System

Per sapere se il Servizio AWSè coperto da programmi di conformità specifici, consulta i Servizi AWScoperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La responsabilità di conformità durante l'utilizzo dei Servizi AWSè determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWSmette a disposizione le seguenti risorse:

- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWSincentrati sulla sicurezza e sulla conformità.
- Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services: questo whitepaper descrive come le aziende possono utilizzare AWSper creare applicazioni conformi alla normativa HIPAA.

  > **Note**
  >
  > Non tutti i Servizi AWSsono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- AWSGuide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Configvaluta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWSfornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse

AWSe verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

- AWS Audit Manager: questo Servizio AWSaiuta a verificare continuamente l'utilizzo di AWSper semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

# Resilienza in Amazon Elastic File System

L'infrastruttura globale dei servizi AWS è progettata attorno a regioni Regioni AWS e zone di disponibilità. Le regioni di Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e a velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

I file system Amazon EFS sono resilienti a uno o più errori della zona di disponibilità all'interno di unRegione AWS. Le destinazioni di montaggio stesse sono progettate per offrire elevata disponibilità. Durante la progettazione di disponibilità elevata e il failover ad altre zone di disponibilità (AZ), tenere presente che mentre gli indirizzi IP e il DNS per le destinazioni di montaggio in ogni AZ sono statici, sono componenti ridondanti supportati da più risorse. Per ulteriori informazioni, consultare Utilizzo di Amazon EFS con Amazon EC2 .

Per ulteriori informazioni sulle regioni Regione AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

# Isolamento di rete di Amazon Elastic File System

In quanto servizio gestito, Amazon Elastic File System è protetto dalla sicurezza della rete globale AWS. Per informazioni sui servizi di sicurezza AWSe su come AWSprotegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWSutilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWSWell-Architected Framework.

Utilizza le chiamate API pubblicate di AWS per accedere a Amazon EFS attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Queste API possono essere invocate da qualsiasi posizione di rete, ma Amazon EFS non supporta le policy di accesso basate sulle risorse, che possono includere limitazioni basate sull'indirizzo IP di origine. È inoltre possibile utilizzare le policy di Amazon EFS per controllare l'accesso da endpoint Amazon Virtual Private Cloud (Amazon VPC) o VPC specifici. Di fatto, ciò isola l'accesso di rete a una determinata risorsa Amazon EFS solo dal VPC specifico nella rete AWS.

# Quote e limiti di Amazon EFS

Di seguito vengono fornite informazioni sulle quote relative all'utilizzo di Amazon EFS.

Argomenti



## Quote per Amazon EFS che è possibile incrementare

Service Quotas è un AWS servizio che consente di gestire le quote o i limiti da un'unica posizione. Nella console Service Quotas, puoi visualizzare tutti i valori limite di Amazon EFS e richiedere un aumento della quota per il numero di file system EFS in Regione AWS.

Inoltre, puoi richiedere un aumento delle quote Amazon EFS seguenti contattando l'assistenza AWS . Per ulteriori informazioni, vedi Richiesta di aumento delle quote. Il team di assistenza Amazon EFS esamina ogni richiesta individualmente.

- Numero di file system per ogni account cliente.
- Throughput elastico per file system per tutti i client connessi in un Regione AWS.
- Throughput assegnato per file system per tutti i client connessi in un. Regione AWS

La tabella seguente elenca le quote per ogni risorsa modificabile.

Numero di file system per account cliente

| Risorsa | Quota predefinita |
| --- | --- |
| Numero di file system per ogni account cliente in un Regione AWS | 1.000 |

Throughput elastico totale predefinito per file system per tutti i client connessi in ciascuno Regione AWS

| Regione AWS | Velocità di trasmissione effettiva massima in lettura | Velocità di trasmissione effettiva massima in scrittura (throughput misurato) |
|---|---|---|
| Stati Uniti orientali (Ohio)<br>Regione Stati Uniti orientali (Virginia settentrionale)<br>Stati Uniti occidentali (Oregon)<br>Regione Asia Pacifico (Tokyo)<br>Europa (Irlanda) | 20 gibibyte al secondo () GiBps | 5 GiBps |
| Tutti gli altri Regioni AWS | 3 GiBps | 1 GiBps |

Throughput totale predefinito per file system per tutti i client connessi in ciascuno di essi Regione AWS

| Regione AWS | Velocità di trasmissione effettiva massima in lettura | Velocità di trasmissione effettiva massima in scrittura (throughput misurato) |
|---|---|---|
| Stati Uniti orientali (Ohio)<br>Regione Stati Uniti orientali (Virginia settentrionale)<br>Stati Uniti occidentali (Oregon)<br>Europa (Irlanda) | 10 GiBps | 3,33 GiBps |
| Tutti gli altri Regioni AWS | 3 GiBps | 1 GiBps |

## Richiesta di aumento delle quote

Per richiedere un aumento di queste quote AWS Support, procedi nel seguente modo. Il team Amazon EFS esamina ogni richiesta di incremento della quota.

Per richiedere un aumento della quota tramite AWS Support

1. Apri la pagina AWS Support Support Center ed effettua l'accesso, se necessario. Quindi, scegli Crea caso.
2. In Crea caso seleziona Aumento dei limiti del servizio.
3. Per Tipo di limite scegli il tipo di limite da aumentare. Compila i campi necessari nel modulo, quindi scegli il metodo di contatto preferito.

# Quote di risorse di Amazon EFS che non puoi modificare

Le quote per diverse risorse Amazon EFS che non possono essere modificate includono:

- Quote per risorse generali, come il numero di punti di accesso o connessioni per ogni file system.
- Superamento dei limiti di produttività in ciascuno di essi. Regione AWS

Le tabelle seguenti elencano le quote di risorse generali e i limiti di throughput di Bursting che non possono essere modificati.

Quote di risorse generali che non possono essere modificate

| Risorsa | Quota |
|---|---|
| Numero di punti di accesso per ogni file system | 1.000 |
| Numero di connessioni per ogni file system | 25.000 |
| Numero di destinazioni di montaggio per ogni file system in una zona di disponibilità | 1 |
| Numero di target di montaggio per ogni cloud privato virtuale (VPC) | 400 |

| Risorsa | Quota |
| --- | --- |
| Numero di gruppi di sicurezza per ogni destinazione di montaggio | 5 |
| Numero di tag per ogni file system | 50 |
| Numero di VPC per ogni file system | 1 |

> **Note**
>
> I client possono anche connettersi a target di montaggio che si trovano in un account o VPC diverso da quello del file system. Per ulteriori informazioni, consulta Montaggio di file system EFS da un altro Account AWS o da un VPC.

Throughput totale di bursting per file system per tutti i client connessi in ciascuno di essi Regione AWS

| Regione AWS | Velocità di trasmissione effettiva massima in lettura | Velocità di trasmissione effettiva massima in scrittura |
| --- | --- | --- |
| Stati Uniti orientali (Ohio)<br>Regione Stati Uniti orientali (Virginia settentrionale)<br>Stati Uniti occidentali (Oregon)<br>Asia Pacifico (Sydney)<br>Europa (Irlanda) | 5 GiBps | 3 GiBps |
| Tutti gli altri Regioni AWS | 3 GiBps | 1 GiBps |

## Limiti per i client NFS

Sono stabiliti i seguenti limiti per i client NFS, presupponendo l'utilizzo di un client Linux NFSv4.1:

- Il throughput massimo che è possibile raggiungere per ogni client NFS è di 500 mebibyte al secondo (). MiBps Il throughput del client NFS è calcolato come il numero totale di byte inviati e ricevuti, con una dimensione minima della richiesta NFS di 4 KB (dopo aver applicato un tasso di misurazione di 1/3 per le richieste di lettura).
- Fino a 65.536 utenti attivi per ogni client possono avere file aperti contemporaneamente.
- Sull'istanza vengono aperti fino a 65.536 file contemporaneamente. Elencare i contenuti delle directory non è considerato nel conteggio dei file aperti.
- Ogni montaggio univoco sul client può acquisire fino a un totale di 65.536 blocchi per connessione.
- Quando ci si connette ad Amazon EFS, i client NFS on-premise o in un'altra Regione AWS possono osservare un throughput inferiore rispetto a quando si connettono a EFS dalla stessa Regione AWS. Questo effetto è dovuto all'aumento della latenza di rete. È richiesta una latenza di rete di 1 ms al massimo per ottenere il throughput ottimale per client. Utilizza il servizio di migrazione DataSync dei dati durante la migrazione di set di dati di grandi dimensioni dai server NFS locali a EFS.
- Il protocollo NFS supporta un massimo di 16 ID di gruppo (GID) per utente e tutti i GID aggiuntivi vengono troncati dalle richieste dei client NFS. Per ulteriori informazioni, consulta Accesso negato ai file consentiti sul file system NFS.
- L'utilizzo di Amazon EFS con Microsoft Windows non è supportato.

# Quote per i file system Amazon EFS

Le quote seguenti sono specifiche per i file system Amazon EFS.

| Risorsa | Quota |
|---|---|
| Lunghezza del nome del file, in byte | 255 |
| Lunghezza del collegamento simbolico in byte | 4.080 |
| Numero di collegamenti fissi per un file | 177 |
| Dimensione di un singolo file | 52.673.613.135.872 byte (47,9 TiB) |
| Numero di livelli per la profondità della cartella | 1.000 |

| Risorsa | Quota |
| --- | --- |
| Numero di blocchi su un singolo file tra tutte le istanze e gli utenti | 512 |
| Limite di caratteri per ogni policy del file system | 20.000 |
| *Numero di operazioni sui file al secondo per la modalità a scopi generali | 250.000 |

*Per ulteriori informazioni sul numero di operazioni sui file al secondo per la modalità a scopi generali, consulta Riepilogo delle prestazioni.

# Funzionalità NFSv4.0 e 4.1 non supportate

Sebbene Amazon EFS non supporti NFSv2 o NFSv3, supporta sia NFSv4.1 che NFSv4.0, ad eccezione delle seguenti funzionalità:

- pNFS
- Client delegation o callback di qualsiasi tipo
  - L'operazione OPEN restituisce sempre `OPEN_DELEGATE_NONE` come tipo di delega.
  - L'operazione OPEN restituisce `NFSERR_NOTSUPP` per i tipi di richiesta `CLAIM_DELEGATE_CUR` e `CLAIM_DELEGATE_PREV`.
- Blocco obbligatorio

  Tutti i blocchi in Amazon EFS sono di tipo advisory, il che significa che le operazioni di READ e WRITE non verificano la presenza di blocchi in conflitto prima che l'operazione sia eseguita.
- Deny share

  NFS supporta il concetto di rifiuto della condivisione. deny share viene utilizzato principalmente dai client Windows per permettere agli utenti di impedire ad altri utenti di accedere a un determinato file che è stato aperto. Amazon EFS non supporta questa funzionalità e restituisce l'errore NFS `NFS4ERR_NOTSUPP` per qualsiasi comando OPEN che specifica per deny share un valore diverso da `OPEN4_SHARE_DENY_NONE`. I client NFS Linux non utilizzano nessun valore diverso da `OPEN4_SHARE_DENY_NONE`.
- Liste di controllo degli accessi (ACL)

- Amazon EFS non aggiorna l'attributo `time_access` in occasione delle letture del file. Amazon EFS aggiorna `time_access` in occasione dei seguenti eventi:
  - Quando si crea un file (viene creato un inode)
  - Quando un client NFS invia una specifica richiesta `setattr`
  - In occasione di una scrittura sull'inode causata, ad esempio, da una modifica delle dimensioni del file o da modifiche dei metadati
  - In occasione di qualsiasi aggiornamento degli attributi dell'inode
- Spazi dei nomi
- Cache di risposta persistente
- Sicurezza basata su Kerberos
- Conservazione dei dati NFSv4.1
- SetUID su cartelle
- Tipi di file non supportati utilizzando l'operazione CREATE: Dispositivi a blocchi (NF4BLK), dispositivi a caratteri (NF4CHR), attribute directory (NF4ATTRDIR) e named attribute (NF4NAMEDATTR).
- Attributi non supportati: 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 e FATTR4_ACL.

  Un tentativo di impostare tali attributi ha come conseguenza l'invio al client di un errore `NFS4ERR_ATTRNOTSUPP`.

## Ulteriori considerazioni

In aggiunta, tieni presente quanto segue:

- Per un elenco di Regioni AWS dove puoi creare file system Amazon EFS, consulta la Riferimenti generali di AWS.
- Amazon EFS non supporta l'opzione `nconnect` di montaggio.
- È possibile montare un file system Amazon EFS da server di data center on-premise utilizzando AWS Direct Connect e VPN. Per ulteriori informazioni, consulta Montaggio con client on-premise.

# Risoluzione dei problemi di Amazon EFS

Sono disponibili informazioni sulle difficoltà legate alla risoluzione dei problemi relativi ad Amazon Elastic File System (Amazon EFS).

Argomenti



## Risoluzione dei problemi Amazon EFS: problemi generici

Utilizza queste informazioni per risolvere problemi generici con Amazon EFS. Per informazioni sulle prestazioni, consultare Prestazioni Amazon EFS.

In generale, se si verificano problemi difficili da risolvere con Amazon EFS, assicurati di utilizzare un kernel Linux recente. Se si sta utilizzando una distribuzione Linux enterprise, consigliamo di attenersi alle seguenti indicazioni:

- Amazon Linux 2 con kernel 4.3 o successivo
- Amazon Linux 2015.09 o versioni successive
- RHEL 7.3 o versioni successive
- Tutte le versioni di Ubuntu 16.04
- Ubuntu 14.04 con kernel 3.13.0-83 o versioni successive
- SLES 12 Sp2 o versioni successive

Se si sta usando un'altra distribuzione o un kernel personalizzato, consigliamo un kernel versione 4.3 o più recente.

> **Note**
>
> RHEL 6.9 potrebbe non essere una scelta ottimale per determinati carichi di lavoro a causa di Prestazioni scadenti durante l'apertura di svariati file in parallelo.

Argomenti



## Impossibile creare un file system EFS

Una richiesta di creazione di un file system EFS ha esito negativo e viene visualizzato il seguente messaggio:

```
User: arn:aws:iam::111122223333:user/username is not authorized to
perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

Operazione da eseguire

Controlla la tua policy AWS Identity and Access Management (IAM) per confermare di essere autorizzato a creare file system EFS con le condizioni di risorse specificate. Per ulteriori informazioni, consulta Gestione dell'identità e degli accessi per Amazon Elastic File System.

## Accesso negato ai file consentiti sul file system NFS

Quando un utente a cui sono assegnati più di 16 ID di gruppo di accesso (GID) tenta di eseguire un'operazione su un file system NFS, gli potrebbe essere negato l'accesso ai file consentiti sul file system. Questo problema si verifica perché il protocollo NFS supporta un massimo di 16 GID per

utente e tutti i GID aggiuntivi vengono troncati dalla richiesta del client NFS, come definito nella RFC 5531.

Operazione da eseguire

Ristruttura le mappature di utenti e gruppi NFS in modo che a ogni utente non vengano assegnati più di 16 gruppi di accesso (GID).

## Errori durante l'accesso alla console Amazon EFS

Questa sezione descrive gli errori che gli utenti potrebbero riscontrare durante l'accesso alla console di gestione Amazon EFS.

### Errore durante l'autenticazione delle credenziali per **`ec2:DescribeVPCs`**

Il seguente messaggio di errore viene visualizzato quando si accede alla console Amazon EFS:

```
AuthFailure: An error occurred authenticating your credentials for ec2:DescribeVPCs.
```

Questo errore indica che le tue credenziali di accesso non sono state autenticate correttamente con il servizio Amazon EC2. La console Amazon EFS chiama il servizio Amazon EC2 per tuo conto durante la creazione di file system EFS nel VPC che scegli.

Operazione da eseguire

Assicurati che l'ora in cui il client accede alla console Amazon EFS sia impostata correttamente.

## Blocco di istanza Amazon EC2

Un'istanza può bloccarsi perché è stata eliminata una destinazione di montaggio di un file system senza prima smontare quest'ultimo.

Operazione da eseguire

Prima di eliminare una destinazione di montaggio di un file system, smontare il file system. Per ulteriori informazioni sullo smontaggio di un file system Amazon EFS, consulta Smontaggio dei file system.

## Blocco di un'applicazione che esegue la scrittura di grandi quantità di dati

Un'applicazione che scrive una grande quantità di dati su Amazon EFS si blocca e provoca il riavvio dell'istanza.

Operazione da eseguire

Se un'applicazione richiede un tempo troppo lungo per scrivere tutti i suoi dati su Amazon EFS, Linux potrebbe riavviarsi perché sembra che il processo non risponda. Due parametri di configurazione del kernel definiscono questo comportamento, `kernel.hung_task_panic` e `kernel.hung_task_timeout_secs`.

Nell'esempio seguente, lo stato del processo appeso è segnalato dal comando `ps` con `D` prima del riavvio dell'istanza, indicando che il processo di attesa delle operazioni di I/O.

```
$ 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
```

Per prevenire un riavvio, aumentare il periodo di timeout o disabilitare la modalità panic del kernel al rilevamento di un'operazione in attesa. Il comando seguente disabilita la modalità panic del kernel in caso di operazione in attesa sulla maggior parte dei sistemi Linux.

```
$ sudo sysctl -w kernel.hung_task_panic=0
```

## Prestazioni scadenti durante l'apertura di svariati file in parallelo

Le applicazioni che consentono di aprire più file in parallelo non mostrano l'incremento prestazionale previsto della parallelizzazione degli I/O.

Operazione da eseguire

Questo problema si verifica sui client Network File System versione 4 (NFSv4) e sui client RHEL 6 che utilizzano NFSv4.1, in quanto tali client NFS serializzano le operazioni NFS OPEN e CLOSE. Utilizzare il protocollo NFS versione 4.1 e una delle distribuzioni Linux consigliate che non mostrano questo problema.

Se non è possibile utilizzare NFSv4.1, ricordarsi che il client Linux NFSv4.0 serializza le richieste di apertura e chiusura per ID utente e ID di gruppo. Questa serializzazione ha luogo anche quando più processi o più thread inviano molteplici richieste contemporaneamente. Quando tutti gli ID corrispondono, il client invia una sola operazione di apertura o chiusura alla volta al server NFS. Per risolvere questi problemi, è possibile eseguire le seguenti azioni:

- È possibile eseguire ogni processo da un ID utente diverso sulla stessa istanza Amazon EC2.

- È possibile associare lo stesso ID utente a tutte le richieste di apertura e modificare invece l'ID di gruppo.
- È possibile eseguire ogni processo su una diversa istanza Amazon EC2.

## Impostazioni NFS personalizzate che causano ritardi nelle operazioni di scrittura

Si stanno utilizzano impostazioni del client NFS personalizzate e sono necessari fino a tre secondi affinché un'istanza Amazon EC2 veda un'operazione di scrittura eseguita su un file system da un'altra istanza Amazon EC2.

Operazione da eseguire

Se si verifica questo problema, è possibile risolverlo in uno dei seguenti modi:

- Se il client NFS sull'istanza Amazon EC2 che esegue l'operazione di lettura dispone di caching degli attributi attivato, smontare il file system. Quindi rimontare utilizzando l'opzione `noac` per disabilitare il caching degli attributi. Il caching degli attributi su NFSv4.1 è abilitato per impostazione predefinita.

  > **Note**
  >
  > La disabilitazione della cache lato client può ridurre le prestazioni dell'applicazione.

- È inoltre possibile deselezionare il caching degli attributi su richiesta utilizzando un linguaggio di programmazione compatibile con le procedure di NFS. Per eseguire questa operazione, è possibile inviare una richiesta alla procedura di `ACCESS` immediatamente prima di una richiesta di lettura.

  Ad esempio, utilizzando il linguaggio di programmazione Python, è possibile costruire la seguente chiamata.

```
# 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 creazione di backup con Oracle Recovery Manager è lenta

Le creazioni di backup con Oracle Recovery Manager possono essere lente se Oracle Recovery Manager si mette in sospensione per 120 secondi prima dell'avvio di un processo di backup.

Operazione da eseguire

Se si verifica questo problema, disabilitare Oracle Direct NFS, come descritto in Enabling and Disabling Direct NFS Client Control of NFS nell'Oracle Help Center.

> **Note**
>
> Amazon EFS non supporta Oracle Direct NFS.

# Risoluzione degli errori legati alle operazioni sui file

Quando si accede a un file system Amazon EFS, valgono alcuni limiti specifici sui file. Il superamento di tali limiti può causare errori nelle operazioni sui file. Per ulteriori informazioni sui limiti per client e file in Amazon EFS, consulta Limiti per i client NFS. Qui di seguito, è possibile trovare alcuni errori comuni sulle operazioni relative ai file e i limiti associati a ciascun errore.

Argomenti



## Il comando ha esito negativo con l'errore "Quota disco superata"

Amazon EFS non supporta al momento quote disco associate agli utenti. Questo errore può verificarsi se i seguenti limiti sono stati superati:

- Fino a 65.536 utenti attivi possono avere file aperti contemporaneamente. Un account utente che effettua l'accesso più volte viene considerato come unico utente attivo.

- È possibile aprire fino a 65.536 file contemporaneamente per istanza. Elencare i contenuti delle directory non è considerato nel conteggio dei file aperti.
- Ogni montaggio univoco sul client può acquisire fino a un totale di 65.536 blocchi per connessione.

Operazione da eseguire

Se si verifica questo problema, è possibile risolverlo identificando i limiti precedenti che sono stati superati e quindi apportando le modifiche necessarie per rispettare tale limite. Per ulteriori informazioni, consulta Limiti per i client NFS.

## Il comando ha esito negativo con l'errore "Errore di I/O"

Questo errore si verifica in presenza di uno dei problemi seguenti:

- Più di 65.536 account utente attivi per ogni istanza hanno file aperti contemporaneamente.

  Operazione da eseguire

  Se si verifica questo problema, è possibile risolverlo rispettando il limite dei file aperti supportati sulle proprie istanze. Per farlo, ridurre il numero di utenti attivi che mantengono simultaneamente file aperti sul file system Amazon EFS delle proprie istanze.
- La AWS KMS chiave che crittografa il file system è stata eliminata.

  Operazione da eseguire

  Se si verifica questo problema, non è più possibile decrittografare i dati crittografati usando tale chiave, che quindi non possono più essere recuperati.

## Il comando ha esito negativo con l'errore "Nome del file troppo lungo"

Questo errore si verifica quando le dimensioni del nome di un file o di un collegamento simbolico (symlink) è troppo lungo. I nomi di file sono soggetti ai seguenti limiti:

- Ogni nome può essere lungo fino a 255 byte.
- Un collegamento simbolico può arrivare fino a 4080 byte di dimensione.

Operazione da eseguire

Se si verifica questo problema, è possibile risolverlo riducendo le dimensioni del nome del file o del collegamento simbolico affinché rispetti i limiti supportati.

## Il comando ha esito negativo con l'errore "File non trovato"

Questo errore si verifica perché alcune versioni precedenti a 32 bit della suite Oracle E-Business utilizzano interfacce I/O di file a 32 bit, mentre EFS utilizza numeri di inode a 64 bit. Le chiamate di sistema che potrebbero non riuscire includono `stat()` e `readdir()`.

Operazione da eseguire

Se si verifica questo errore, è possibile risolverlo utilizzando l'opzione di avvio nfs.enable_ino64=0 kernel. Questa opzione consente una compressione dei numeri di inode EFS da 64 bit a 32 bit. Le opzioni di avvio del kernel sono gestite in modo diverso dalle diverse distribuzioni Linux. In Amazon Linux, attiva questa opzione aggiungendo `nfs.enable_ino64=0 kernel` alla variabile `GRUB_CMDLINE_LINUX_DEFAULT` in `/etc/default/grub`. Consulta la distribuzione per la documentazione specifica su come attivare le opzioni di avvio del kernel.

## Il comando ha esito negativo con l'errore "Troppi link"

Questo errore si verifica quando ci sono troppi collegamenti fissi a un file. È possibile avere fino a 177 collegamenti fissi in un file.

Operazione da eseguire

Se si verifica questo problema, è possibile risolverlo riducendo il numero di collegamenti fissi a un file affinché rispetti il limite supportato.

## Il comando ha esito negativo con l'errore "File troppo grande"

Questo errore si verifica quando un file è troppo grande. Un singolo file può essere grande fino a 52.673.613.135.872 byte (47,9 TiB).

Operazione da eseguire

Se si verifica questo problema, è possibile risolverlo riducendo la dimensione del file affinché rispetti il limite supportato.

# Risoluzione dei problemi di AMI e kernel

Qui di seguito, è possibile trovare informazioni sulla risoluzione dei problemi relativi a determinate versioni di Amazon Machine Image (AMI) o del kernel quando si utilizza Amazon EFS da un'istanza Amazon EC2.

Argomenti



## Non è possibile eseguire il comando chown

Non è possibile modificare il proprietario di un file o di una cartella utilizzando il comando Linux `chown`.

Versioni di kernel che presentano questo bug

2.6.32

Operazione da eseguire

È possibile evitare questo errore applicando la seguente procedura:

- Se si sta eseguendo `chown` per la singola fase di impostazione necessaria per modificare la proprietà della directory root di EFS, è possibile eseguire il comando `chown` da un'istanza in esecuzione con un kernel più recente. Ad esempio, è possibile usare la versione più recente di Amazon Linux.
- Se `chown` fa parte del flusso di lavoro di produzione, per utilizzare `chown` è necessario aggiornare la versione del kernel.

## Il file system continua a eseguire ripetutamente delle operazioni a causa di un bug del client

Un file system continua a eseguire ripetutamente delle operazioni a causa di un bug del client

Operazione da eseguire

Aggiornare il software del client alla versione più recente.

## Client in deadlock

Un client entra in stato di deadlock.

Versioni di kernel che presentano questo bug

- 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

Operazione da eseguire

Esegui una di queste operazioni:

- Effettuare l'upgrade a una nuova versione del kernel. In caso di CentOS-7, le versioni di kernel Linux 3.10.0-327 o successive contengono la correzione del bug.
- Eseguire il downgrade a una versione di kernel precedente.

## Il recupero dell'elenco dei file di una grande cartella impiega molto tempo

Ciò può verificarsi se la cartella è continuamente soggetta a modifica mentre il client NFS itera sugli elementi della cartella per terminare l'operazione di recupero dell'elenco. Quando il client NFS si accorge che i contenuti della cartella sono stati modificati durante l'iterazione, il client NFS riavvia l'iterazione dall'inizio. Di conseguenza, il comando ls può richiedere molto tempo in caso di cartella di grandi dimensioni con file modificati con una frequenza elevata.

Versioni di kernel che presentano questo bug

Versioni kernel CentOS e RHEL inferiori a 2.6.32-696.el6

Operazione da eseguire

Per risolvere il problema, effettuare l'upgrade a una nuova versione del kernel.

# Risoluzione dei problemi con il montaggio

Qui di seguito, è possibile trovare informazioni sulla risoluzione dei problemi di Amazon EFS legati al montaggio dei file system.

## Montaggio fallito del file system su un'istanza Windows

Il montaggio di un file system su un'istanza Amazon EC2 con Microsoft Windows ha esito negativo.

Operazione da eseguire

Non utilizzare Amazon EFS con istanze EC2 Windows, poiché non è supportato.

## Accesso rifiutato dal server

Un montaggio del file system non va a buon fine con il seguente messaggio:

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

Questo problema si può verificare se il client NFS non dispone dell'autorizzazione per montare il file system.

Operazione da eseguire

Se si sta tentando di montare il file system utilizzando IAM, assicurarsi di utilizzare l'opzione `-o iam` nel comando di montaggio. Questo indica all'helper di montaggio di EFS di passare le credenziali alla destinazione di montaggio EFS. Se ancora non si dispone dell'accesso, controllare la policy del file system e la policy di identità per assicurarsi che non siano presenti clausole DENY applicabili alla connessione e che sia presente almeno una clausola ALLOW che si applica alla connessione. Per ulteriori informazioni, consultare Utilizzo di IAM per controllare l'accesso ai dati del file system e Creazione di policy del file system.

## Il montaggio automatico non funziona e l'istanza non risponde

Questo problema può verificarsi se il file system è stato montato automaticamente su un'istanza e l'opzione `_netdev` non è stata dichiarata. Se `_netdev` è mancante, l'istanza EC2 potrebbe smettere di rispondere. Questo risultato è dovuto al fatto che i file system di rete devono essere inizializzati dopo che l'istanza di calcolo ha avviato la sua interfaccia di rete.

Operazione da eseguire

Se si verifica questo problema, contatta l' AWS assistenza.

## Il montaggio di molteplici file system Amazon EFS in /etc/fstab ha esito negativo

Per le istanze che utilizzano il sistema di inizializzazione systemd con due o più voci Amazon EFS in `/etc/fstab`, potrebbero esservi delle volte in cui alcune o tutte queste voci non vengono montate. In questo caso, l'output di `dmesg` mostra una o più righe simili alle seguenti.

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

Operazione da eseguire

In questo caso, consigliamo di creare un nuovo servizio file per il servizio systemd in `/etc/systemd/system/mount-nfs-sequentially.service`. Il codice da includere nel file dipende dal fatto che tu stia montando manualmente i file system o utilizzando l'helper di montaggio di Amazon EFS.

- Se stai montando manualmente i file system, il comando `ExecStart` deve puntare a Network File System (NFS4). Includi il codice seguente nel file:

```
[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
```

- Se utilizzi l'helper di montaggio di Amazon EFS, il comando `ExecStart` deve puntare a EFS anziché a NFS4 per utilizzare Transport Layer Security (TLS). Includi il codice seguente nel file:

```
[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
```

Dopo aver creato il file, esegui i seguenti due comandi:

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

Quindi riavviare l'istanza Amazon EC2. I file system sono montati a richiesta, in genere entro un secondo.

## Il comando di montaggio ha esito negativo con il messaggio di errore "tipo fs errato"

Il comando ha esito negativo con il seguente messaggio di errore.

```
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.
```

Operazione da eseguire

Se si riceve questo messaggio, installare il pacchetto `nfs-utils` (o `nfs-common` su Ubuntu). Per ulteriori informazioni, consulta Installazione del client NFS.

## Il comando di montaggio ha esito negativo con il messaggio di errore "opzione di montaggio errata"

Il comando ha esito negativo con il seguente messaggio di errore.

```
mount.nfs: an incorrect mount option was specified
```

Operazione da eseguire

Questo messaggio di errore probabilmente significa che la distribuzione Linux non supporta Network File System 4.0 e 4.1 (NFSv4). Per confermare questo caso, è possibile eseguire il comando seguente.

```
$ grep CONFIG_NFS_V4_1 /boot/config*
```

Se il comando precedente restituisce `# CONFIG_NFS_V4_1 is not set`, NFSv4.1 non è supportato dalla propria distribuzione Linux. Per un elenco di Amazon Machine Image (AMI) per Amazon Elastic Compute Cloud (Amazon EC2) che supportano NFSv4.1, consulta Supporto per NFS.

## Montaggio con punti di accesso non riuscito

Il comando mount ha esito negativo durante il montaggio con un punto di accesso, con il seguente messaggio di errore:

```
mount.nfs4: mounting access_point failed, reason given by server: No such file or
 directory
```

Operazione da eseguire

Questo messaggio di errore indica che il percorso EFS specificato non esiste. Assicurati di fornire la proprietà e le autorizzazioni per la directory principale del punto di accesso. EFS non creerà la directory radice utilizzando queste informazioni. Per ulteriori informazioni, consulta Utilizzo dei punti di accesso Amazon EFS.

Se non si specifica alcuna proprietà e autorizzazione della directory principale e la directory principale non esiste già, EFS non creerà la directory principale. Qualsiasi tentativo di montare il file system utilizzando il punto di accesso avrà esito negativo.

## Il montaggio del file system ha esito negativo immediatamente dopo la creazione del file system

Possono volerci fino a 90 secondi dopo la creazione di una destinazione di montaggio affinché il DNS (Domain Name Service) possa propagare completamente i record in una regione Regione AWS.

Operazione da eseguire

Se stai creando e montando file system a livello di programmazione, ad esempio con un AWS CloudFormation modello, ti consigliamo di implementare una condizione di attesa.

## Il montaggio di un file system rimane in attesa e quindi ha esito negativo con un errore di timeout

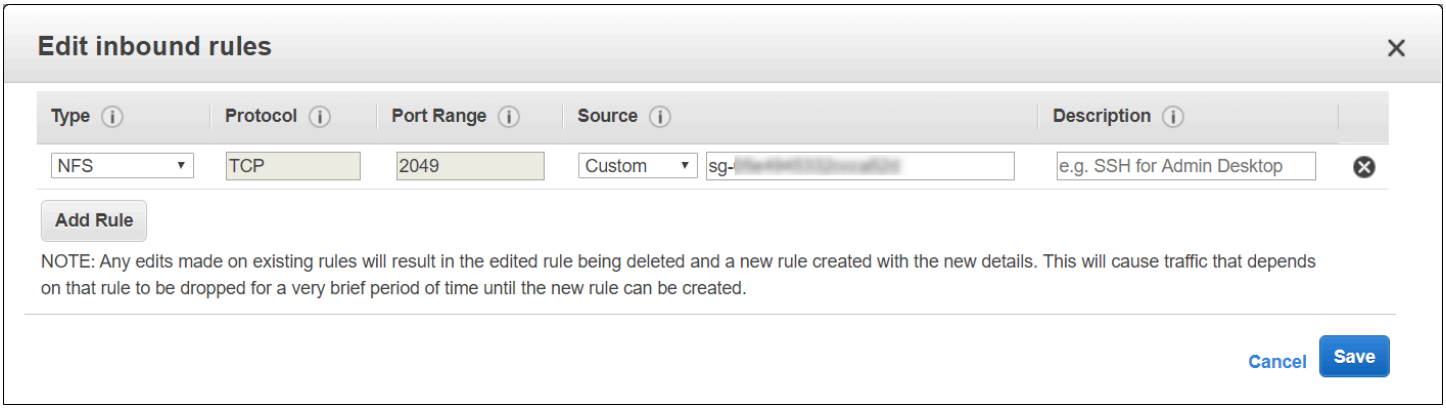
Il comando di montaggio del file system si blocca per uno o due minuti, e quindi ha esito negativo con un errore di timeout. Il codice seguente mostra un esempio.

```
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-ip:/ mnt

[2+ minute wait here]
mount.nfs: Connection timed out
$Â
```

Operazione da eseguire

Questo errore può verificarsi perché il gruppo di sicurezza dell'istanza Amazon EC2 o della destinazione di montaggio non sono configurati correttamente. Assicurarsi che il gruppo di sicurezza della destinazione di montaggio disponga di una regola in entrata che consente l'accesso NFS dal gruppo di sicurezza EC2.




Per ulteriori informazioni, consulta Creazione dei gruppi di sicurezza.

Verificare che l'indirizzo IP della destinazione del montaggio specificato sia valido. Se si specifica un indirizzo IP non corretto e non è presente nient'altro a quell'indirizzo IP che possa rifiutare il montaggio, si potrebbe verificare questo problema.

## Il montaggio di un file system con NFS usando il nome DNS ha esito negativo

I tentativi di montare un file system utilizzando un client NFS (non utilizzando il client `amazon-efs-utils`) utilizzando il nome DNS del file system falliscono, come mostrato nell'esempio seguente:

```
$ 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:/ mnt
mount.nfs: Failed to resolve server file-system-id.efs.aws-region.amazonaws.com:
  Name or service not known.

$
```

Operazione da eseguire

Controlla la tua configurazione VPC. Se si sta usando una VPC personalizzata, accertarsi che le impostazioni DNS siano abilitate. Per ulteriori informazioni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC. Inoltre, i nomi DNS del file system e della destinazione di montaggio non sono risolvibili dall'esterno del VPC dove esistono.

Prima di poter montare un file system utilizzando il relativo nome DNS nel `mount` comando, devi fare quanto segue:

- Verificare la disponibilità di una destinazione di montaggio Amazon EFS nella stessa zona di disponibilità dell'istanza Amazon EC2.
- Assicurarsi che ci sia una destinazione di montaggio nello stesso VPC dell'istanza Amazon EC2. In caso contrario, non è possibile utilizzare la risoluzione dei nomi DNS per le destinazioni di montaggio EFS che si trovano in un altro VPC. Per ulteriori informazioni, consulta Montaggio di file system EFS da un altro Account AWS o da un VPC.
- Collegare l'istanza Amazon EC2 all'interno di Amazon VPC configurata in modo da utilizzare il server DNS fornito da Amazon. Per ulteriori informazioni, consulta Set di opzioni DHCP in Amazon VPC nella Guida per l'utente di Amazon VPC.
- Verificare che l'Amazon VPC dell'istanza Amazon EC2 che si connette abbia degli hostname DNS abilitati. Per ulteriori informazioni, consulta Attributi DNS per VPC nella Guida per l'utente di Amazon VPC.

## Il montaggio del file system ha esito negativo con "nfs not responding" (nfs non risponde)

Il montaggio di un file system Amazon EFS ha esito negativo su un evento di riconnessione TCP (Transmission Control Protocol) con "`nfs: server_name still not responding`".

Operazione da eseguire

Utilizzare l'opzione di montaggio `noresvport` per accertarsi che il client NFS utilizzi una nuova porta di origine TCP quando viene ristabilita una connessione di rete. Ciò contribuisce a garantire la disponibilità continua dopo un evento di ripristino di rete.

## Lo stato del ciclo di vita della destinazione di montaggio è bloccato

Lo stato del ciclo di vita della destinazione di montaggio è bloccato sui valori creating (creazione) o deleting (eliminazione).

Operazione da eseguire

Riprovare le chiamate `CreateMountTarget` o `DeleteMountTarget`.

## Lo stato del ciclo di vita di Mount Target mostra un errore

Lo stato del ciclo di vita del target di montaggio mostra un errore.

Operazione da eseguire

Amazon EFS non può creare i record DNS (Domain Name System) necessari per nuove destinazioni di montaggio del file system se il cloud privato virtuale (VPC) presenta zone ospitate in conflitto. Amazon EFS non può creare nuovi record all'interno di una zona ospitata di proprietà del cliente. Se devi mantenere una zona ospitata con un intervallo `efs.<region>.amazonaws.com` DNS in conflitto, crea la zona ospitata in un VPC separato. Per ulteriori informazioni sulle considerazioni DNS per il VPC, consulta Attributi DNS per VPC.

Per risolvere il problema, elimina l'host `efs.<region>.amazonaws.com` in conflitto da VPC e crea nuovamente la destinazione di montaggio. Per ulteriori informazioni sull'eliminazione di target di montaggio, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

## Il comando di montaggio non risponde

Un montaggio Amazon EFS sembra non rispondere. Ad esempio, comandi come `ls` rimangono in sospeso.

Operazione da eseguire

Questo errore può verificarsi se un'altra applicazione sta scrivendo grandi quantità di dati sul file system. L'accesso ai file sui quali si concentrano le operazioni di scrittura potrebbe essere bloccato fino al completamento dell'operazione. In generale, tutti i comandi o le applicazioni che tentano di accedere ai file oggetto di scrittura potrebbero apparire come bloccati. Ad esempio, il comando `ls` potrebbe bloccarsi quando arriva al file oggetto di scrittura. Questo accade perché alcune distribuzioni di Linux creano un alias per il comando `ls` in modo che recuperi gli attributi dei file, oltre a visualizzare l'elenco dei contenuti della cartella.

Per risolvere il problema, verificare la presenza di un'altra applicazione che sta scrivendo file sulla destinazione di montaggio Amazon EFS e che si trova nello stato `Uninterruptible sleep` (`D`), come nell'esempio seguente:

```
$ 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
```

Dopo aver verificato che questo è il caso, è possibile risolvere il problema rimanendo in attesa del completamento dell'altra operazione di scrittura o implementando una soluzione temporanea. Nell'esempio del comando `ls`, è possibile utilizzare direttamente il comando `/bin/ls`, invece di

un alias. Ciò permette al comando di procedere senza bloccarsi sul file oggetto della scrittura. In generale, se l'applicazione che scrive i dati potesse forzare periodicamente un flush dei dati, ad esempio utilizzando il comando `fsync(2)`, ciò potrebbe migliorare la reattività dei file system per le altre applicazioni. Tuttavia, questo miglioramento potrebbe andare a discapito di prestazioni quando l'applicazione scrive i dati.

## Il client montato viene disconnesso

Un client montato su un file system Amazon EFS può occasionalmente disconnettersi a causa di un numero qualsiasi di cause. I client NFS sono progettati per riconnettersi automaticamente in caso di interruzione per ridurre al minimo l'impatto delle disconnessioni di routine sulle prestazioni e sulla disponibilità delle applicazioni. Nella maggior parte dei casi, i client si riconnettono in modo trasparente in pochi secondi.

Il software client NFS incluso nelle versioni precedenti del kernel Linux (versioni v5.4 e precedenti) include un comportamento che fa sì che i client NFS, dopo la disconnessione, tentino di riconnettersi sulla stessa porta sorgente TCP. Questo comportamento non è conforme al TCP RFC e può impedire a questi client di ristabilire rapidamente le connessioni al server NFS (un file system EFS in questo caso).

Per risolvere questo problema, ti consigliamo vivamente di utilizzare l'helper di montaggio di Amazon EFS per montare i tuoi file system EFS. L'helper di montaggio EFS utilizza impostazioni di montaggio ottimizzate per i file system Amazon EFS. Per ulteriori informazioni sull'uso del client EFS e dell'helper di montaggio, consulta Utilizzo degli amazon-efs-utils strumenti.

Se non è possibile utilizzare l'helper di montaggio EFS, si consiglia vivamente di utilizzare l'opzione di montaggio `noresvport` NFS, che indica ai client NFS di ristabilire le connessioni utilizzando nuove porte sorgente TCP per evitare questo problema. Per ulteriori informazioni, consulta Opzioni di montaggio NFS consigliate.

## Le operazioni su un file system appena montato restituiscono l'errore "handle del file errato"

Le operazioni su un file system appena montato restituiscono un errore `bad file handle`.

Questo errore può verificarsi se un'istanza Amazon EC2 è stata connessa a un file system e a una destinazione di montaggio con un indirizzo IP specificato, e successivamente il file system e la destinazione di montaggio vengono eliminati. Questo problema può verificarsi se si creano un nuovo

file system e una nuova destinazione di montaggio da connettere a tale istanza Amazon EC2 con lo stesso indirizzo IP della destinazione di montaggio.

Operazione da eseguire

È possibile risolvere questo errore smontando il file system e quindi rimontandolo sull'istanza Amazon EC2. Per ulteriori informazioni sullo smontaggio di un file system Amazon EFS, consulta Smontaggio dei file system.

### Esito negativo dello smontaggio di un file system

Se il file system è impegnato, non è possibile smontarlo.

Operazione da eseguire

Il problema può essere risolto nei modi indicati di seguito:

- Usa lazy unmount, umount -l che scollega il file system dalla gerarchia del file system quando viene eseguito, quindi pulisce tutti i riferimenti al file system non appena non è più occupato.
- Attendere il completamento di tutte le operazioni di lettura e scrittura e quindi tentare di nuovo di eseguire il comando umount.
- Forza lo smontaggio usando il comando umount -f.

> **Warning**
>
> La forzatura di un'operazione di smontaggio interrompe tutte le letture e le scritture di dati in corso di elaborazione sul file system. Consulta la pagina umount man per maggiori informazioni e indicazioni sull'uso di questa opzione.

## Risoluzione dei problemi di crittografia

Qui di seguito, è possibile trovare informazioni sulla risoluzione dei problemi di Amazon EFS legati alla cifratura.

- Il montaggio con la crittografia dei dati in transito ha esito negativo
- Il montaggio con la crittografia dei dati in transito è interrotto
- ncrypted-at-rest Il file system E non può essere creato

- File system crittografato inutilizzabile

## Il montaggio con la crittografia dei dati in transito ha esito negativo

Per impostazione predefinita, quando utilizzi l'helper di montaggio di Amazon EFS con Transport Layer Security (TLS), viene eseguita la verifica del nome dell'host. Alcuni sistemi non supportano questa funzionalità, ad esempio Red Hat Enterprise Linux o CentOS. In questi casi, il montaggio di un file system EFS con TLS ha esito negativo.

Operazione da eseguire

È consigliabile che esegua l'aggiornamento della versione del servizio stunnel sul tuo client per assicurarti che sia supportata verifica del nome dell'host. Per ulteriori informazioni, consulta Aggiornamento di `stunnel`.

## Il montaggio con la crittografia dei dati in transito è interrotto

È possibile, anche se improbabile, che la connessione crittografata al proprio file system Amazon EFS possono rimanere bloccata o essere interrotta da eventi lato client.

Operazione da eseguire

Se la connessione al file system Amazon EFS con crittografia dei dati in transito viene interrotta, eseguire i seguenti passaggi:

1. Verificare che il servizio stunnel sia in esecuzione sul client.
2. Confermare che l'applicazione watchdog `amazon-efs-mount-watchdog` sia in esecuzione sul client. È possibile determinare se questa applicazione è in esecuzione con il comando seguente:

   ```
   ps aux | grep [a]mazon-efs-mount-watchdog
   ```

3. Controllare i log di assistenza. Per ulteriori informazioni, consulta Ottenimento dei log per il supporto.
4. Eventualmente, è possibile abilitare i logo di stunnel e controllare anche le informazioni in essi contenute. Per abilitare i log di stunnel, è possibile modificare la configurazione dei registri in `/etc/amazon/efs/efs-utils.conf`. Affinché le modifiche abbiano effetto, tuttavia, è necessario smontare e rimontare il file system con l'helper di montaggio.

> **Important**
>
> L'abilitazione dei log di stunnel potrebbe portare a un consumo di spazio di memorizzazione sul file system non indifferente.

Se le interruzioni persistono, contatta l' AWS assistenza.

## ncrypted-at-rest Il file system E non può essere creato

Hai provato a creare un nuovo encrypted-at-rest file system. Tuttavia, viene visualizzato un messaggio di errore che indica che non AWS KMS è disponibile.

Operazione da eseguire

Questo errore può verificarsi nel raro caso in cui AWS KMS diventi temporaneamente non disponibile nel tuo Regione AWS. In tal caso, attendi AWS KMS il ripristino della piena disponibilità, quindi riprova a creare il file system.

## File system crittografato inutilizzabile

Un file system crittografato restituisce regolarmente errori del server NFS. Questi errori possono verificarsi quando EFS non è in grado di recuperare la chiave master da cui proviene AWS KMS per uno dei seguenti motivi:

- La chiave è stata disabilitata.
- La chiave è stata eliminata.
- Le autorizzazioni concesse a Amazon EFS per l'utilizzo della chiave sono state revocate.
- AWS KMS è temporaneamente non disponibile.

Operazione da eseguire

Innanzitutto, verifica che la AWS KMS chiave sia abilitata. È possibile farlo visualizzando le chiavi nella console. Per ulteriori informazioni, consulta Visualizzazione delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service .

Se la chiave non è abilitato, abilitarla. Per ulteriori informazioni consulta l'articolo relativo all'abilitazione e disabilitazione delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service .

Se la chiave è in attesa di eliminazione, allora questo stato disabilita la chiave. È possibile annullare l'eliminazione e abilitare di nuovo la chiave. Per ulteriori informazioni, consultare Pianificazione e annullamento della cancellazione delle chiavi nella Guida per gli sviluppato di AWS Key Management Service .

Se la chiave è abilitata e il problema persiste o se riscontri un problema durante la riattivazione della chiave, contatta l' AWS assistenza.

# API EFS

L'API Amazon EFS è un protocollo di rete basato su HTTP (RFC 2616). Per ogni chiamata API, si effettua una richiesta HTTP all'endpoint API Amazon EFS specifico della regioneRegione AWS in cui si desidera gestire i file system. L'API fa riferimento ai documenti JSON (RFC 4627) per la definizione dei contenuti delle richieste/risposte HTTP.

L'API Amazon EFS è un modello RPC. In questo modello è presente un insieme fisso di operazioni e la sintassi per ciascuna operazione è nota ai client senza alcuna precedente interazione. Nella sezione seguente, è possibile trovare una descrizione di ciascuna operazione API realizzata tramite una notazione RPC astratta. Ad ognuna è associato un nome operazione che non appare nello scambio in rete. Per ogni operazione, l'argomento specifica la mappatura rispetto agli elementi della richiesta HTTP.

L'operazione specifica di Amazon EFS a cui è associata una determinata richiesta è determinata da una combinazione del metodo della richiesta (GET, PUT, POST o DELETE) e a quale dei vari modelli corrisponde il suo URI di richiesta. Se l'operazione è PUT o POST, Amazon EFS estrae gli argomenti delle chiamate dal segmento del percorso URI della richiesta, dai parametri della query e dall'oggetto JSON nel corpo della richiesta.

> **Note**
>
> Anche se il nome dell'operazione, come ad esempio `CreateFileSystem`, non viene visualizzato nello scambio in rete, i nomi di queste operazioni sono significativi per le policy AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Gestione dell'identità e degli accessi per Amazon Elastic File System.
> Il nome dell'operazione viene utilizzato anche per denominare i comandi negli strumenti della riga di comando e negli elementi delle APIAWS SDK. Ad esempio, è disponibile un comando AWS CLI denominato `create-file-system` mappato all'operazione `CreateFileSystem`.
> Il nome dell'operazione viene visualizzato anche neiAWS CloudTrail registri delle chiamate API Amazon EFS.

## API endpoint

L'endpoint API è il nome sul DNS usato come host nell'URI HTTP per le chiamate API. Questi endpoint API sono specificiRegioni AWS e assumono la forma seguente.

```
elasticfilesystem.aws-region.amazonaws.com
```

Ad esempio, l'endS S S S s s s s s s s S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S

```
elasticfilesystem.us-west-2.amazonaws.com
```

Per un elenco diRegione AWS quelli supportati da Amazon EFS (dove puoi creare e gestire file system), consulta Amazon Elastic File System nel Riferimenti generali di AWS.

L'endpoint API specifico per regione definisce l'ambito delle risorse Amazon EFS accessibili quando si effettua una chiamata API. Ad esempio, quando chiami l'`DescribeFileSystems`operazione utilizzando l'endpoint precedente, ottieni un elenco di file system nella regione degli Stati Uniti occidentali (Oregon) che sono stati creati nel tuo account.

## Versione API

La versione dell'API utilizzata per una chiamata è identificata dal primo segmento di percorso dell'URI della richiesta e il suo formato è una data ISO 8601. Per un esempio, consulta CreateFileSystem.

La documentazione descrive la versione API 2015-02-01.

## Argomenti correlati

Le seguenti sezioni forniscono una descrizione delle operazioni delle API, di come creare una firma per l'autenticazione di una richiesta e di come concedere le autorizzazioni a tali operazioni delle API tramite le policy IAM.

- Gestione dell'identità e degli accessi per Amazon Elastic File System
- Azioni
- Tipi di dati

# Utilizzo della frequenza di richiesta dell'API di interrogazione per Amazon EFS

Le richieste API di Amazon EFS sono limitate per ciascunaAccount AWS area geografica per migliorare le prestazioni del servizio. Tutte le chiamate API Amazon EFS insieme, indipendentemente

dal fatto che provengano da un'applicazioneAWS CLI, dalla console Amazon EFS o dalla console Amazon EFS, non devono superare la velocità massima consentita di richieste API. La velocità massima di richiesta API può variare daRegioni AWS. Le richieste API effettuate sono attribuite al sottostanteAccount AWS.

Se una richiesta API supera il numero massimo di richieste API per la sua categoria, la richiesta restituisce il codice di errore `ThrottlingException`. Per evitare questo errore, assicurarsi che l'applicazione non riprovi ad eseguire richieste API con un'elevata frequenza. È possibile ottenere questo risultato ponendo attenzione all'utilizzo del polling e utilizzando una strategia di backoff esponenziale nella ripetizione dei tentativi.

## Polling

L'applicazione potrebbe aver bisogno di chiamare ripetutamente un'operazione tramite API per verificare la presenza di un aggiornamento nello stato. Prima di avviare il polling, lasciare alla richiesta il tempo necessario per il suo potenziale completamento. Quando si inizia il polling, utilizzare un intervallo di attesa appropriato tra le richieste successive. Per ottimizzare i risultati, utilizzare un intervallo di attesa incrementale.

## Riprovi o elaborazione in batch

L'applicazione potrebbe dover riprovare una richiesta API in caso di esito negativo o elaborare più risorse (ad esempio, tutti i file system Amazon EFS). Per ridurre la frequenza delle richieste API, utilizzare un intervallo di attesa appropriato tra le richieste successive. Per ottimizzare i risultati, utilizzare un intervallo di attesa incrementale o variabile.

## Calcolo di un intervallo di sonno

Quando è necessario eseguire il polling o rieseguire una richiesta API, è consigliato l'uso di un algoritmo di backoff esponenziale per calcolare l'intervallo di tempo di attesa tra le chiamate API. L'idea che sottende al backoff esponenziale è di utilizzare attese progressivamente più lunghe tra i tentativi per le risposte di errore consecutive. Per ulteriori informazioni ed esempi di implementazione di questo algoritmo, vedere Error Retries and Exponential BackoffAWS inRiferimenti generali di Amazon Web Services.

# Azioni

Sono supportate le operazioni seguenti:

- 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 di accesso EFS. Un punto di accesso è una visualizzazione specifica dell'applicazione in un file system EFS che applica un utente e un gruppo del sistema operativo e un percorso del file system a qualsiasi richiesta del file system effettuata tramite il punto di accesso. L'utente e il gruppo per sistema operativo del punto di accesso sostituiscono le informazioni di identità fornite dal client NFS. Il percorso file system viene esposto come la directory root del punto di accesso. Le applicazioni che utilizzano il punto di accesso possono accedere ai dati solo nella propria directory e sotto a questa. Per ulteriori informazioni, vedi Montaggio di un file system utilizzando i punti di accesso EFS.

> **Note**
>
> Se più richieste di creazione di punti di accesso sullo stesso file system vengono inviate in rapida successione e il file system è vicino al limite di 1.000 punti di accesso, è possibile che si verifichi una risposta limitata per queste richieste. Ciò serve a garantire che il file system non superi il limite di punti di accesso dichiarato.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:CreateAccessPoint`.

I punti di accesso possono essere etichettati al momento della creazione. Se i tag vengono specificati nell'azione di creazione delle risorse, IAM esegue autorizzazioni aggiuntive per l'azione `elasticfilesystem:TagResource` per verificare se gli utenti dispongono delle autorizzazioni per creare tag. Pertanto, devi concedere le autorizzazioni esplicite per utilizzare l'operazione `elasticfilesystem:TagResource`. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'assegnazione di tag per le risorse durante la creazione.

## Sintassi della richiesta

```
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"
      }
   ]
}
```

## Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

### ClientToken

Una stringa composta da un massimo di 64 caratteri ASCII che Amazon EFS utilizza per garantire una creazione idempotente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: sì

### FileSystemId

ID del file system EFS a cui si applica il punto di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

PosixUser

L'utente e il gruppo del sistema operativo applicati a tutte le richieste di file system effettuate utilizzando il punto di accesso.

Tipo: oggetto PosixUser

Campo obbligatorio: no

RootDirectory

Specifica la directory del file system EFS da esporre come directory principale ai client NFS utilizzando il punto di accesso per accedere al file system EFS. I client che utilizzano il punto di accesso possono accedere solo alla directory principale e sotto a questa. Se `RootDirectory > Path` specificato non esiste, Amazon EFS crea la directory principale utilizzando le impostazioni `CreationInfo` quando un client si connette a un punto di accesso. Quando si specifica `RootDirectory`, è necessario fornire `Path` e `CreationInfo`.

Amazon EFS crea una directory principale solo se hai fornito CreationInfo: OwnUid, ownGid e le autorizzazioni per la directory. Se non fornisci queste informazioni, Amazon EFS non crea la directory principale. Se la directory principale non esiste, i tentativi di montaggio utilizzando il punto di accesso avranno esito negativo.

Tipo: oggetto RootDirectory

Campo obbligatorio: no

Tags

Crea tag associati al punto di accesso. Ciascun tag è una coppia chiave-valore e ogni chiave deve essere univoca. Per ulteriori informazioni, consulta Assegnazione di tag alle risorse AWS nella Guida di riferimento generale di AWS.

Tipo: matrice di oggetti Tag

Campo obbligatorio: no

## Sintassi della risposta

```
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,
         "OwnerUid": number,
         "Permissions": "string"
      },
      "Path": "string"
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### AccessPointArn

Il nome della risorsa Amazon (ARN) associato al punto di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}$`

AccessPointId

L'ID del punto di accesso, assegnato da Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

ClientToken

La stringa opaca specificata nella richiesta per garantire la creazione idempotent.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

FileSystemId

ID del file system EFS a cui si applica il punto di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(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 di vita del punto di accesso.

Tipo: stringa

Valori validi: `creating | available | updating | deleting | deleted | error`

Name

Il nome del punto di accesso. Questo è il valore del tag `Name`.

Tipo: stringa

OwnerId

Identifica il proprietario (Account AWS) della risorsa del punto di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

PosixUser

Identità POSIX completa, inclusi ID utente, ID gruppo e ID gruppo secondario sul punto di accesso utilizzato per tutte le operazioni di file dai client NFS che utilizzano il punto di accesso.

Tipo: oggetto PosixUser

RootDirectory

La directory nel file system EFS che il punto di accesso espone come directory principale ai client NFS che utilizzano il punto di accesso.

Tipo: oggetto RootDirectory

Tags

I tag associati al punto di accesso, presentati come una serie di oggetti Tag.

Tipo: matrice di oggetti Tag

## Errori

AccessPointAlreadyExists

Restituito se il punto di accesso che state tentando di creare esiste già, con il token di creazione fornito nella richiesta.

Codice di stato HTTP: 409

AccessPointLimitExceeded

Restituito se Account AWS ha già creato il numero massimo di punti di accesso consentiti per file system. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/efs/latest/ug/limits.html#limits-efs-resources-per-account-per-region.

Codice di stato HTTP: 403

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

ThrottlingException

Restituito quando l'azione `CreateAccessPoint` API viene richiamata troppo rapidamente e il numero di punti di accesso sul file system si avvicina al limite di 120.

Codice di stato HTTP: 429

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per V3 JavaScript
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# CreateFileSystem

Crea un nuovo file system vuoto. Nella richiesta, l'operazione richiede un token di creazione che Amazon EFS utilizza per garantire una creazione idempotente (chiamare l'operazione con lo stesso token non ha effetto). Se attualmente non esiste un file system di proprietà dell'account Account AWS chiamante con il token di creazione specificato, l'operazione procede in questo modo:

- Crea un nuovo file system vuoto. Il file system avrà un ID assegnato da Amazon EFS e uno stato iniziale `creating` per il ciclo di vita.
- Restituisce la descrizione del file system creato.

In caso contrario, questa operazione restituisce un errore `FileSystemAlreadyExists` con l'ID del file system esistente.

> **Note**
>
> Per i casi d'uso di base, è possibile utilizzare un UUID generato in modo casuale per il token di creazione.

L'operazione idempotente consente di tentare nuovamente una chiamata `CreateFileSystem` senza rischiare di creare un ulteriore file system. Questo può accadere quando una prima chiamata ha esito negativo senza fornire indicazioni certe sull'effettiva creazione del file system. Un esempio potrebbe essere il verificarsi di un timeout a livello di trasporto o il ripristino della connessione. Se si utilizza lo stesso token di creazione e la chiamata iniziale è riuscita a creare un file system, con l'errore `FileSystemAlreadyExists` il client saprà della sua esistenza.

Per ulteriori informazioni, consulta la sezione relativa alla Creazione di un file system della Guida per l'utente di Amazon EFS.

> **Note**
>
> La chiamata `CreateFileSystem` risponde mentre il ciclo di vita del file system è ancora `creating`. È possibile controllare lo stato di creazione del file system chiamando l'operazione DescribeFileSystems che, tra altri elementi, ne restituirà lo stato.

L'operazione include anche un parametro `PerformanceMode` opzionale che è possibile scegliere per il file system. Consigliamo `generalPurpose` `PerformanceMode` per tutti i file system. La `maxIO` modalità è un tipo di prestazioni della generazione precedente progettata per carichi di lavoro altamente parallelizzati che possono tollerare latenze più elevate rispetto alla modalità. `generalPurpose` `MaxIO`la modalità non è supportata per i file system One Zone o per i file system che utilizzano la velocità effettiva elastica.

Non `PerformanceMode` può essere modificata dopo la creazione del file system. Per ulteriori informazioni, consulta Amazon EFS: modalità prestazionali.

È possibile impostare la modalità di throughput per il file system utilizzando il parametro `ThroughputMode`.

Una volta completamente creato il file system, Amazon EFS ne imposta lo stato del ciclo di vita su `available`. A questo punto è possibile creare una o più target di montaggio per il file system nel VPC. Per ulteriori informazioni, consulta CreateMountTarget. È possibile montare il file system Amazon EFS su un'istanza EC2 nel VPC utilizzando il target di montaggio. Per ulteriori informazioni, consulta Amazon EFS: come funziona.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:CreateFileSystem`.

I file system possono essere etichettati al momento della creazione. Se i tag vengono specificati nell'azione di creazione delle risorse, IAM esegue autorizzazioni aggiuntive per l'azione `elasticfilesystem:TagResource` per verificare se gli utenti dispongono delle autorizzazioni per creare tag. Pertanto, devi concedere le autorizzazioni esplicite per utilizzare l'operazione `elasticfilesystem:TagResource`. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'assegnazione di tag per le risorse durante la creazione.

## Sintassi della richiesta

```
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"
}
```

## Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

### AvailabilityZoneName

Per i file system One Zone, specificare la zona di AWS disponibilità in cui creare il file system. Utilizzare il formato `us-east-1a` per specificare la zona di disponibilità. Per ulteriori informazioni sui file system One Zone, consulta i tipi di file system EFS nella Amazon EFS User Guide.

> **Note**
>
> I file system a zona singola non sono disponibili in tutte le zone di disponibilità in Regioni AWS dove è disponibile Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: no

### Backup

Specifica se i backup automatici sono abilitati sul file system che si sta creando. Imposta il valore su `true` per abilitare i backup automatici. Se stai creando un file system a zona singola, i backup

automatici sono abilitati per impostazione predefinita. Per ulteriori informazioni, consulta Backup automatici nella Guida per l'utente di Amazon EFS.

Il valore predefinito è `false`. Tuttavia, se si specifica `AvailabilityZoneName`, l'impostazione predefinita è `true`.

> **Note**
>
> AWS Backup non è disponibile in ogni Regioni AWS in cui è disponibile Amazon EFS.

Tipo: Booleano

Campo obbligatorio: no

### CreationToken

Stringa contenente un massimo di 64 caratteri ASCII. Amazon EFS utilizza questo sistema per garantire la creazione idempotente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: sì

### Encrypted

Un valore booleano che, se true, crea un file system crittografato. Quando crei un file system crittografato, puoi specificare una chiave AWS Key Management Service esistente (chiave KMS). Se non specifichi una chiave KMS, la chiave KMS predefinita per Amazon EFS, `/aws/elasticfilesystem`, viene utilizzata per proteggere il file system crittografato.

Tipo: Booleano

Campo obbligatorio: no

### KmsKeyId

L'ID della chiave KMS che si desidera utilizzare per proteggere il file system crittografato. Questo parametro è necessario solo se desideri utilizzare una chiave KMS non predefinita. Se

il parametro non è specificato, viene utilizzata la chiave KMS predefinita per Amazon EFS. È possibile specificare un ID chiave KMS utilizzando i seguenti formati:

- ID chiave: un identificatore univoco della chiave, ad esempio `1234abcd-12ab-34cd-56ef-1234567890ab`.
- ARN: un ARN (Amazon Resource Name) per la chiave, ad esempio `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- Alias chiave: un nome di visualizzazione creato in precedenza per una chiave, ad esempio `alias/projectKey1`.
- ARN alias della chiave: un ARN per un alias della chiave, ad esempio `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`.

Se lo usi`KmsKeyId`, devi impostare il CreateFileSystemparametro:Encrypted su true.

> **Important**
>
> EFS accetta solo chiavi KMS simmetriche. Non puoi usare chiavi KMS asimmetriche con i file system Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^([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/_-]+))))$`

Campo obbligatorio: no

PerformanceMode

Le modalità di prestazioni dei file system. Consigliamo la modalità Prestazioni `generalPurpose` per la maggior parte dei file system. I file system che utilizzano la performance `maxIO` sono in grado di ridimensionare le risorse a livelli maggiori di throughput aggregato e di operazioni al secondo, con un compromesso di latenze leggermente più elevate per la maggior parte delle operazioni sui file. La modalità prestazionale non può essere modificata dopo la creazione del file system. La modalità `maxIO` non è supportata sui file system a zona singola.

> **Important**
>
> A causa delle più elevate latenze per operazione con I/O max, consigliamo di utilizzare la modalità prestazionale a scopi generali per tutti i file system.

Il valore predefinito è `generalPurpose`.

Tipo: stringa

Valori validi: `generalPurpose | maxIO`

Campo obbligatorio: no

ProvisionedThroughputInMibps

La velocità effettiva, misurata in mebibyte al secondo (MiBps), che desideri fornire per il file system che stai creando. Obbligatorio se `ThroughputMode` è impostato su `provisioned`. I valori validi sono 1-3414 MiBps, con il limite superiore a seconda della regione. Per aumentare questo limite, contatta AWS Support. Per ulteriori informazioni, consulta Quote di Amazon EFS che è possibile incrementare nella Guida per l'utente di Amazon EFS.

Tipo: double

Intervallo valido: valore minimo di 1.0.

Campo obbligatorio: no

Tags

Utilizza per creare uno o più tag associati al file system. Ogni tag è una coppia chiave-valore definita dall'utente. Denominare il file system quando viene creato, includendo una coppia chiave-valore `"Key":"Name","Value":"{value}"`. Ogni chiave deve essere univoca. Per ulteriori informazioni, consulta Assegnazione di tag alle risorse AWS nella Guida di riferimento generale di AWS.

Tipo: matrice di oggetti Tag

Campo obbligatorio: no

ThroughputMode

Specifica la modalità della velocità di trasmissione effettiva per il file system. La modalità può essere `bursting`, `provisioned` o `elastic`. Se `ThroughputMode`

è impostato su `provisioned`, è necessario impostare anche un valore per `ProvisionedThroughputInMibps`. Dopo avere creato il file system, puoi ridurre la velocità di trasmissione effettiva del file system nella modalità con provisioning o passare a un'altra modalità di velocità di trasmissione effettiva, con determinate limitazioni di tempo. Per ulteriori informazioni, consulta Specifica del throughput nella modalità Provisioned nella Guida per l'utente di Amazon EFS.

Il valore predefinito è `bursting`.

Tipo: stringa

Valori validi: `bursting | provisioned | elastic`

Campo obbligatorio: no

## Sintassi della risposta

```
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"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 201.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### AvailabilityZoneId

L'identificatore univoco e coerente della zona di disponibilità in cui si trova il file system, valido solo per i file system a zona singola. Ad esempio, `use1-az1` è un ID di zona di disponibilità per la regione us-east-1 Regione AWS e identifica la stessa posizione in ogni Account AWS.

Tipo: stringa

### AvailabilityZoneName

Descrive la zona di disponibilità AWS in cui si trova il file system, valida solo per i file system a zona singola. Per ulteriori informazioni, consulta Utilizzo delle classi di archiviazione EFS nella Guida per l'utente di Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

### CreationTime

L'ora di creazione del file system, in secondi (da 1970-01-01T00:00:00Z).

Tipo: Timestamp

CreationToken

Stringa opaca specificata nella richiesta.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Encrypted

Valore booleano che, se "true", indica che il file system è crittografato.

Tipo: Booleano

FileSystemArn

Il nome della risorsa Amazon (ARN) per il file system Amazon EFS in formato `arn:aws:elasticfilesystem:`*`region`*`:`*`account-id`*`:file-system/`*`file-system-id`* . Esempio con dati campione: `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Tipo: stringa

FileSystemId

L'ID del file system, assegnato da Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

FileSystemProtection

Descrive la protezione del file system.

Tipo: oggetto FileSystemProtectionDescription

KmsKeyId

L'ID della AWS KMS key da utilizzare per proteggere il file system crittografato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^([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 di vita del file system.

Tipo: stringa

Valori validi: `creating | available | updating | deleting | deleted | error`

Name

È possibile aggiungere tag a un file system, incluso un tag `Name`. Per ulteriori informazioni, consulta CreateFileSystem. Se il file system ha un tag `Name`, Amazon EFS restituisce il valore in questo campo.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 256.

Modello: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

NumberOfMountTargets

Il numero attuale di target di montaggio del file system. Per ulteriori informazioni, consulta CreateMountTarget.

Tipo: integer

Intervallo valido: valore minimo di 0.

OwnerId

Account AWS che ha creato il file system.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

PerformanceMode

Le modalità di prestazioni dei file system.

Tipo: stringa

Valori validi: `generalPurpose | maxIO`

ProvisionedThroughputInMibps

La quantità di velocità effettiva assegnata, misurata in MiBps, per il file system. Valido per i file system che utilizzano `ThroughputMode` impostato su `provisioned`.

Tipo: double

Intervallo valido: valore minimo di 1.0.

SizeInBytes

L'ultima dimensione misurata nota (in byte) dei dati memorizzati nel file system, nel relativo campo `Value` e l'ora in cui tale dimensione è stata determinata nel campo `Timestamp`. Il valore `Timestamp` è il numero intero di secondi dal 1970-01-01T 00:00:00 Z. Il valore `SizeInBytes` non rappresenta la dimensione di un'istantanea coerente del file system, ma è coerente quando non vi sono operazioni di scrittura sul file system. Ossia, `SizeInBytes` rappresenta la dimensione effettiva solo se il file system non viene modificato per un periodo superiore a un paio d'ore. Altrimenti, il valore non corrisponde alla dimensione esatta che aveva il file system in qualsiasi momento.

Tipo: oggetto FileSystemSize

Tags

I tag associati al file system, presentati come una serie di oggetti `Tag`.

Tipo: matrice di oggetti Tag

ThroughputMode

Visualizza la modalità di throughput per un file system. Per ulteriori informazioni, consulta Modalità di throughput nella Guida per l'utente di Amazon EFS.

Tipo: stringa

Valori validi: `bursting | provisioned | elastic`

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemAlreadyExists

Restituito se il file system che si sta cercando di creare esiste già, con il token di creazione fornito.

Codice di stato HTTP: 409

FileSystemLimitExceeded

Restituito se Account AWS ha già creato il numero massimo di punti di file system consentiti per account.

Codice di stato HTTP: 403

InsufficientThroughputCapacity

Restituito se la capacità non è sufficiente per fornire un throughput aggiuntivo. Questo valore può essere restituito quando si tenta di creare un file system in modalità di throughput assegnato, quando si tenta di aumentare la velocità di trasmissione effettiva assegnata di un file system esistente o quando si tenta di modificare un file system esistente dalla modalità Bursting alla modalità Con provisioning. Riprova più tardi.

Codice di stato HTTP: 503

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

ThroughputLimitExceeded

Restituito se la modalità di throughput o la quantità di throughput assegnata non possono essere modificate perché è stato raggiunto il limite di throughput di 1024 MiB/s.

Codice di stato HTTP: 400

UnsupportedAvailabilityZone

Restituito se la funzionalità Amazon EFS richiesta non è disponibile nella zona di disponibilità specificata.

Codice di stato HTTP: 400

## Esempi

### Creazione di un file system EFS crittografato

L'esempio seguente invia una richiesta POST per creare un file system nella regione `us-west-2` con i backup automatici abilitati. La richiesta specifica `myFileSystem1` come token di creazione per l'idempotenza.

#### Richiesta di esempio

```
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"
      }
   ]
}
```

#### Risposta di esempio

```
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"
}
```

Creazione di un file system EFS crittografato con disponibilità a zona singola

L'esempio seguente invia una richiesta POST per creare un file system nella regione `us-west-2` con i backup automatici abilitati. Il file system disporrà di una sola zona di archiviazione nella zona `us-west-2b` di disponibilità.

Richiesta di esempio

```
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"
      }
   ]
}
```

## Risposta di esempio

```
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"
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per V3 JavaScript
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# CreateMountTarget

Crea un target di montaggio per un file system. È quindi possibile montare il file system su istanze EC2 utilizzando il target di montaggio.

È possibile creare un target di montaggio in ogni zona di disponibilità nella propria VPC. Tutte le istanze EC2 in un VPC all'interno di una determinata zona di disponibilità condividono un singolo target di montaggio per uno specifico file system. Se in una zona di disponibilità vi sono più sottoreti, è possibile creare un target di montaggio in una di tali sottoreti. Non è necessario che le istanze EC2 siano nella stessa sottorete del target di montaggio per accedere ai propri file system.

È possibile creare un solo target di montaggio per un file system a zona singola. È necessario creare tale target di montaggio nella stessa zona di disponibilità in cui si trova il file system. Utilizzate le proprietà `AvailabilityZoneName` e `AvailabiltyZoneId` nell'oggetto DescribeFileSystems di risposta per ottenere queste informazioni. Utilizzate la zona di disponibilità `subnetId` associata alla zona di disponibilità del file system durante la creazione del target di montaggio.

Per ulteriori informazioni, consulta Amazon EFS: come funziona.

Per creare un target di montaggio per un file system, lo stato del ciclo di vita del file system deve essere `available`. Per ulteriori informazioni, consulta DescribeFileSystems.

Nella richiesta, specifica quanto segue:

- L'ID del file system per il quale si sta creando il target di montaggio.
- Un ID di sottorete, che determina quanto segue:
  - VPC in cui Amazon EFS crea il target di montaggio
  - Zona di disponibilità in cui Amazon EFS crea il target di montaggio
  - Intervallo di indirizzi IP da cui Amazon EFS seleziona l'indirizzo IP del target di montaggio (se non specificato nella richiesta)

Dopo aver creato il target di montaggio, Amazon EFS restituisce una risposta che include un `MountTargetId` e un `IpAddress`. L'indirizzo IP è utilizzato nel montaggio del file system in un'istanza EC2. Durante il montaggio del file system è anche possibile utilizzare il nome DNS del target di montaggio. L'istanza EC2 su cui montare il file system attraverso il target di montaggio è in grado di risolvere il nome DNS del target di montaggio per ricavarne l'indirizzo IP. Per ulteriori informazioni, consulta Come funziona: riepilogo dell'implementazione.

Tieni presente che è possibile creare target di montaggio per un file system in un solo VPC e che può esserci un solo target di montaggio per ogni zona di disponibilità. Ciò significa che, se il file system dispone già di una o più target di montaggio create, la sottorete specificata nella richiesta di aggiunta di un'altra target di montaggio deve soddisfare i seguenti requisiti:

- Deve appartenere allo stesso VPC delle sottoreti dei target di montaggio esistenti
- Non deve trovarsi nella stessa zona di disponibilità delle sottoreti dei target di montaggio esistenti

Se la richiesta soddisfa i requisiti, Amazon EFS procede in questo modo:

- Crea un nuovo target di montaggio nella sottorete specificata.
- Crea anche una nuova interfaccia di rete nella sottorete, come segue:
  - Se la richiesta fornisce un `IpAddress`, Amazon EFS assegna tale indirizzo IP all'interfaccia di rete. In caso contrario, Amazon EFS assegna un indirizzo libero nella sottorete (proprio come fa la chiamata `CreateNetworkInterface` di Amazon EC2 quando una richiesta non specifica un indirizzo IP privato principale).
  - Se la richiesta indica `SecurityGroups`, l'interfaccia di rete è associata a tali gruppi di sicurezza. In caso contrario, appartiene al gruppo di sicurezza predefinito per la sottorete del VPC.
  - Assegna la descrizione `Mount target` *`fsmt-id`* `for file system` *`fs-id`* in cui *`fsmt-id`* è l'ID del target di montaggio e *`fs-id`* è il `FileSystemId`.
  - Imposta la proprietà `requesterManaged` dell'interfaccia di rete su `true` e il valore `requesterId` su `EFS`.

  Ogni target di montaggio Amazon EFS dispone di una corrispondente interfaccia di rete EC2 gestita dal richiedente. Una volta creata l'interfaccia di rete, Amazon EFS imposta il campo `NetworkInterfaceId` nella descrizione del target di montaggio sull'ID dell'interfaccia di rete e il campo `IpAddress` sul relativo indirizzo. Se la creazione dell'interfaccia di rete non riesce, l'intera operazione `CreateMountTarget` ha esito negativo.

> **Note**
>
> La chiamata `CreateMountTarget` restituisce solo dopo aver creato l'interfaccia di rete ma, mentre il target di montaggio è ancora in stato `creating`, è possibile controllarne lo stato di

creazione chiamando l'operazione DescribeMountTargets che, tra l'altro, restituirà lo stato del target di montaggio.

È consigliabile creare un target di montaggio in ciascuna delle zone di disponibilità. L'utilizzo di un file system in una zona di disponibilità attraverso un target di montaggio creata in un'altra zona di disponibilità determina costi da tenere in considerazione. Per ulteriori dettagli, consulta Amazon EFS. Inoltre, usando sempre un target di montaggio locale alla zona di disponibilità dell'istanza, è possibile eliminare lo scenario del fallimento parziale. Se la zona di disponibilità in cui viene creata il target di montaggio diventa inutilizzabile, non sarà possibile accedere al file system tramite i target di montaggio.

Questa operazione richiede autorizzazioni per le seguenti operazioni sul file system:

- `elasticfilesystem:CreateMountTarget`

Questa operazione richiede anche autorizzazioni per le seguenti operazioni Amazon EC2:

- `ec2:DescribeSubnets`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`

## Sintassi della richiesta

```
POST /2015-02-01/mount-targets HTTP/1.1
Content-type: application/json

{
   "FileSystemId": "string",
   "IpAddress": "string",
   "SecurityGroups": [ "string" ],
   "SubnetId": "string"
}
```

## Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

### FileSystemId

L'ID del file system per il quale creare il target di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

### IpAddress

Indirizzo IPv4 valido all'interno dell'intervallo di indirizzi della sottorete specificata.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 7. Lunghezza massima di 15.

Modello: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Campo obbligatorio: no

### SecurityGroups

Fino a cinque ID gruppo di sicurezza del VPC, nel formato `sg-xxxxxxxx`. Devono essere per lo stesso VPC della sottorete specificata.

Tipo: matrice di stringhe

Membri della matrice: numero massimo di 100 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 11. Lunghezza massima di 43.

Modello: `^sg-[0-9a-f]{8,40}`

Campo obbligatorio: no

### SubnetId

L'ID della sottorete in cui aggiungere il target di montaggio. Per i file system a zona singola, utilizza la sottorete associata alla zona di disponibilità del file system.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 15. Lunghezza massima di 47.

Modello: `^subnet-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

## Sintassi della risposta

```
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"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### AvailabilityZoneId

L'identificatore univoco e coerente della zona di disponibilità in cui risiede il target di montaggio. Ad esempio, `use1-az1` è un ID AZ per la regione us-east-1 e ha la stessa posizione in ogni Account AWS.

Tipo: stringa

AvailabilityZoneName

Il nome della zona di disponibilità in cui si trova il target di montaggio. I nomi vengono mappati indipendentemente alle zone di disponibilità per ogni Account AWS. Ad esempio, la zona di disponibilità `us-east-1a` di Account AWS potrebbe non avere la stessa posizione fisica di `us-east-1a` per un altro Account AWS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

FileSystemId

L'ID del file system per il quale creare il target di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

IpAddress

Indirizzo presso il quale è possibile montare il file system utilizzando il target di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 7. Lunghezza massima di 15.

Modello: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

LifeCycleState

Stato del ciclo di vita del target di montaggio.

Tipo: stringa

Valori validi: `creating | available | updating | deleting | deleted | error`

MountTargetId

ID del target di montaggio assegnato dal sistema.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 13. Lunghezza massima di 45.

Modello: `^fsmt-[0-9a-f]{8,40}$`

NetworkInterfaceId

L'ID dell'interfaccia di rete creata da Amazon EFS al momento della creazione del target di montaggio.

Tipo: stringa

OwnerId

ID Account AWS proprietario della risorsa.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

SubnetId

L'ID della sottorete del target di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 15. Lunghezza massima di 47.

Modello: `^subnet-[0-9a-f]{8,40}$`

VpcId

L'ID del cloud privato virtuale (VPC) in cui è configurato il target di montaggio.

Tipo: stringa

## Errori

AvailabilityZonesMismatch

Restituito se la zona di disponibilità specificata per un target di montaggio è diversa dalla zona di disponibilità specificata per lo storage a zona singola. Per ulteriori informazioni, consulta Ridondanza dello storage a livello regionale e a zona unica.

Codice di stato HTTP: 400

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

IpAddressInUse

Restituito se la richiesta `IpAddress` ha specificato un elemento già in uso nella sottorete.

Codice di stato HTTP: 409

MountTargetConflict

Restituito se il target di montaggio viola una delle restrizioni specificate in base ai target di montaggio esistenti del file system.

Codice di stato HTTP: 409

NetworkInterfaceLimitExceeded

L'account chiamante ha raggiunto il limite per le interfacce di rete elastiche per lo specifico Regione AWS. Elimina alcune interfacce di rete o richiedi l'aumento della quota dell'account. Per ulteriori informazioni, consulta Quote di Amazon VPC nella Guida per l’utente di Amazon VPC (vedi la voce Interfacce di rete per regione nella tabella Interfacce di rete).

Codice di stato HTTP: 409

NoFreeAddressesInSubnet

Restituito se `IpAddress` non è stato specificato nella richiesta e non vi sono indirizzi IP liberi nella sottorete.

Codice di stato HTTP: 409

SecurityGroupLimitExceeded

Restituito se la dimensione di `SecurityGroups` specificata nella richiesta è maggiore di cinque.

Codice di stato HTTP: 400

SecurityGroupNotFound

Restituito se uno dei gruppi di sicurezza specificati non esiste nel cloud privato virtuale (VPC) della sottorete.

Codice di stato HTTP: 400

SubnetNotFound

Restituito se non è presente alcuna sottorete con l'ID `SubnetId` fornito nella richiesta.

Codice di stato HTTP: 400

UnsupportedAvailabilityZone

Restituito se la funzionalità Amazon EFS richiesta non è disponibile nella zona di disponibilità specificata.

Codice di stato HTTP: 400

## Esempi

Aggiunta di un target di montaggio a un file system

La richiesta che segue crea un target di montaggio per un file system. La richiesta specifica i valori solo per i parametri obbligatori `FileSystemId` e `SubnetId`. La richiesta non fornisce i parametri `IpAddress` e `SecurityGroups` opzionali. Per `IpAddress`, l'operazione utilizza uno degli indirizzi IP disponibili nella sottorete specificata. Inoltre, l'operazione utilizza il gruppo di sicurezza predefinito associato al VPC per `SecurityGroups`.

### Richiesta di esempio

```
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"}
```

### Risposta di esempio

```
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"
}
```

### Aggiunta di un target di montaggio a un file system

La seguente richiesta specifica tutti i parametri della richiesta per creare un target di montaggio.

### Richiesta di esempio

```
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"
   ]
}
```

Risposta di esempio

```
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"
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# CreateReplicationConfiguration

Crea una configurazione di replica che replica un file system EFS esistente in un nuovo file system di sola lettura. Per ulteriori informazioni, consulta Replica Amazon EFS nella Guida per l'utente di Amazon EFS. La configurazione di replica specifica quanto segue:

- File system di origine: il file system EFS che si desidera replicare. Non è possibile utilizzare un file system scelto come file system di destinazione in un'altra configurazione di replica esistente.
- Regione AWS : il file system Regione AWS in cui viene creato il file system di destinazione. La replica Amazon EFS è disponibile in ogni Regioni AWS in cui è disponibile EFS. La regione deve essere abilitata. Per ulteriori informazioni, consulta Gestione di Regioni AWS nella Guida di riferimento generale di AWS.
- Configurazione del file system di destinazione: la configurazione del file system di destinazione in cui verrà replicato il file system di origine. In una configurazione di replica può esistere un solo file system di destinazione.

  I parametri per la configurazione di replica includono:

  - ID del file system: l'ID del file system di destinazione per la replica. Se non viene fornito alcun ID, EFS crea un nuovo file system con le impostazioni predefinite. Per i file system esistenti, la protezione da sovrascrittura della replica del file system deve essere disabilitata. Per ulteriori informazioni, consulta Replica su un file system esistente.
  - Zona di disponibilità: se si desidera che il file system di destinazione utilizzi lo storage a zona unica, è necessario specificare la zona di disponibilità in cui creare il file system. Per ulteriori informazioni, consulta Tipi di file system EFS nella Guida per l'utente di Amazon EFS.
  - Crittografia: tutti i file system di destinazione vengono creati con la crittografia a riposo abilitata. È possibile specificare la chiave AWS Key Management Service (AWS KMS) utilizzata per crittografare il file system di destinazione. Se non specifichi una chiave KMS, viene utilizzata la chiave KMS gestita dai servizi per Amazon EFS.

  > **Note**
  >
  > Dopo aver creato il file system, non è possibile modificare la chiave KMS.

Per i nuovi file system di destinazione, le seguenti proprietà sono impostate di default:

- Modalità Prestazioni: la modalità Prestazioni del file system di destinazione corrisponde a quella del file system di origine, a meno che il file system di destinazione non utilizzi lo storage a zona singola EFS. In tal caso, viene utilizzata la modalità Prestazioni a scopi generali. La modalità Prestazioni non può essere modificata.
- Modalità Throughput: la modalità Throughput del file system di destinazione corrisponde a quella del file system di origine. Dopo aver creato il file system, è possibile modificare la modalità di throughput.

- gestione del ciclo di vita: la gestione del ciclo di vita non è abilitata nel file system di destinazione. Puoi abilitare la gestione del ciclo di vita dopo aver creato il file system di destinazione.
- Backup automatici: i backup giornalieri automatici sono abilitati nel file system di destinazione. Dopo aver creato il file system, è possibile modificare l'impostazione.

Per ulteriori informazioni, consulta Replica Amazon EFS nella Guida per l'utente di Amazon EFS.

## Sintassi della richiesta

```
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"
      }
   ]
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### SourceFileSystemId

Specifica il file system Amazon EFS da replicare. Questo file system non può essere già un file system di origine o di destinazione in un'altra configurazione di replica.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Destinations

Una matrice di oggetti di configurazione di destinazione. È supportato un solo oggetto di configurazione di destinazione.

Tipo: matrice di oggetti DestinationToCreate

Campo obbligatorio: sì

## Sintassi della risposta

```
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"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

Descrive quando è stata creata la configurazione di replica.

Tipo: Timestamp

Destinations

Una matrice di oggetti di destinazione. È supportato un solo oggetto di destinazione.

Tipo: matrice di oggetti Destination

OriginalSourceFileSystemArn

Il nome della risorsa Amazon (ARN) del file system EFS originale nella configurazione di replica.

Tipo: stringa

SourceFileSystemArn

Il nome della risorsa Amazon (ARN) del file system EFS originale nella configurazione di replica.

Tipo: stringa

SourceFileSystemId

ID del file system Amazon EFS di origine che viene replicato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

SourceFileSystemRegion

Il file system EFS di origine Regione AWS in cui si trova.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

ConflictException

Restituito se il file system di origine in una replica è crittografato ma il file system di destinazione non è crittografato.

Codice di stato HTTP: 409

FileSystemLimitExceeded

Restituito se Account AWS ha già creato il numero massimo di punti di file system consentiti per account.

Codice di stato HTTP: 403

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InsufficientThroughputCapacity

Restituito se la capacità non è sufficiente per fornire un throughput aggiuntivo. Questo valore può essere restituito quando si tenta di creare un file system in modalità di throughput assegnato, quando si tenta di aumentare la velocità di trasmissione effettiva assegnata di un file system

esistente o quando si tenta di modificare un file system esistente dalla modalità Bursting alla modalità Con provisioning. Riprova più tardi.

Codice di stato HTTP: 503

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

ReplicationNotFound

Restituito se il file system specificato non dispone di una configurazione di replica.

Codice di stato HTTP: 404

ThroughputLimitExceeded

Restituito se la modalità di throughput o la quantità di throughput assegnata non possono essere modificate perché è stato raggiunto il limite di throughput di 1024 MiB/s.

Codice di stato HTTP: 400

UnsupportedAvailabilityZone

Restituito se la funzionalità Amazon EFS richiesta non è disponibile nella zona di disponibilità specificata.

Codice di stato HTTP: 400

ValidationException

Restituito se il servizio AWS Backup non è disponibile in Regione AWS, dove è stata effettuata la richiesta.

Codice di stato HTTP: 400

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWS JavaScript SDK per V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# CreateTags

> **Note**
>
> OBSOLETO: `CreateTags` è obsoleto e non viene mantenuto. Per creare tag per una risorsa EFS, utilizza l'operazione API TagResource.

Crea o sovrascrive i tag associati a un file system. Ogni tag è una coppia chiave-valore. Se una chiave di tag specificata nella richiesta esiste già nel file system, questa operazione sovrascrive il suo valore con il valore fornito nella richiesta. Se aggiungi il tag `Name` al tuo file system, Amazon EFS lo restituisce nella risposta all'operazione DescribeFileSystems.

Questa operazione richiede l'autorizzazione per l'operazione `elasticfilesystem:CreateTags`.

## Sintassi della richiesta

```
POST /2015-02-01/create-tags/FileSystemId HTTP/1.1
Content-type: application/json

{
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### FileSystemId

L'ID del file system di cui si desidera modificare i tag (String). Questa operazione modifica solo i tag, non il file system.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Tags

Una matrice di oggetti `Tag` da aggiungere. Ogni oggetto `Tag` è una coppia chiave-valore.

Tipo: matrice di oggetti Tag

Campo obbligatorio: sì

## Sintassi della risposta

```
HTTP/1.1 204
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DeleteAccessPoint

Elimina il punto di accesso specificato. Una volta completata l'eliminazione, i nuovi client non possono più connettersi ai punti di accesso. I client connessi al punto di accesso al momento dell'eliminazione continueranno a funzionare fino a quando non interromperanno la connessione.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DeleteAccessPoint`.

## Sintassi della richiesta

```
DELETE /2015-02-01/access-points/AccessPointId HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

AccessPointId

ID del punto di accesso che si desidera eliminare.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 204
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

## Errori

AccessPointNotFound

Restituito se il valore `AccessPointId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DeleteFileSystem

Elimina un file system, annullando definitivamente l'accesso ai suoi contenuti. Al momento della restituzione, il file system non esiste più e non è possibile accedere ai contenuti del file system eliminato.

È necessario eliminare manualmente i target di montaggio allegati a un file system prima di poter eliminare un file system EFS. Questo passaggio viene eseguito quando utilizzi la console AWS per eliminare un file system.

> **Note**
>
> Non è possibile eliminare un file system che fa parte di una configurazione di replica EFS. La configurazione di replica deve prima essere eliminata.

Non è possibile eliminare un file system in uso. Se il file system ha target di montaggio, è necessario prima eliminarli. Per ulteriori informazioni, consultare DescribeMountTargets e DeleteMountTarget.

> **Note**
>
> La chiamata `DeleteFileSystem` risponde mentre lo stato del file system è ancora `deleting`. È possibile verificare lo stato di eliminazione del file system richiamando l'operazione DescribeFileSystems, che restituisce un elenco dei file system presenti nell'account. Se si trasmette l'ID del file system o il token di creazione per il file system eliminato, DescribeFileSystems restituisce un errore `404 FileSystemNotFound`.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DeleteFileSystem`.

## Sintassi della richiesta

```
DELETE /2015-02-01/file-systems/FileSystemId HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

FileSystemId

ID del file system che desideri eliminare.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 204
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemInUse

Restituito se un file system dispone di target di montaggio.

Codice di stato HTTP: 409

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Esempi

### Eliminazione di un file system

L'esempio seguente invia una richiesta DELETE all'endpoint `file-systems` (`elasticfilesystem.us-west-2.amazonaws.com/2015-02-01/file-systems/fs-01234567`) per eliminare un file system il cui ID è `fs-01234567`.

Richiesta di esempio

```
DELETE /2015-02-01/file-systems/fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T233021Z
Authorization: <...>
```

Risposta di esempio

```
HTTP/1.1 204 No Content
x-amzn-RequestId: a2d125b3-7ebd-4d6a-ab3d-5548630bff33
Content-Length: 0
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3

- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DeleteFileSystemPolicy

Elimina `FileSystemPolicy` per il file system specificato. L'impostazione predefinita di `FileSystemPolicy` entra in vigore una volta eliminata la policy esistente. Per ulteriori informazioni sulla policy del file system predefinita, consulta Uso di policy basate su risorse con EFS.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DeleteFileSystemPolicy`.

## Sintassi della richiesta

```
DELETE /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

FileSystemId

Specifica il file system EFS per cui eliminare `FileSystemPolicy`.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 200
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DeleteMountTarget

Elimina il target di montaggio specificato.

L'operazione forza la cancellazione di tutti i montaggi del file system, con possibili conseguenze sulle istanze o sulle applicazioni che utilizzano tali montaggi. Per evitare che le applicazioni vengano interrotte bruscamente, potresti prendere in considerazione lo smontaggio di tutti i supporti del target di montaggio, se possibile. L'operazione elimina anche l'interfaccia di rete associata. Le scritture non eseguite potrebbero andare perse, ma il danneggiamento di un target di montaggio mediante questa operazione non danneggia il file system stesso. Il file system creato resta intatto. Puoi montare un'istanza EC2 nel tuo VPC utilizzando un altro target di montaggio.

Questa operazione richiede autorizzazioni per le seguenti operazioni sul file system:

- `elasticfilesystem:DeleteMountTarget`

> **Note**
>
> La chiamata `DeleteMountTarget` risponde mentre lo stato del target di montaggio è ancora `deleting`. È possibile verificare l'eliminazione del target di montaggio chiamando l'operazione DescribeMountTargets, che restituisce un elenco di descrizioni del target di montaggio per il file system specificato.

L'operazione richiede anche le autorizzazioni per la seguente azione di Amazon EC2 sull'interfaccia di rete del target di montaggio:

- `ec2:DeleteNetworkInterface`

## Sintassi della richiesta

```
DELETE /2015-02-01/mount-targets/MountTargetId HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MountTargetId

L'ID del target di montaggio da eliminare (String).

Limitazioni di lunghezza: lunghezza minima pari a 13. Lunghezza massima di 45.

Modello: `^fsmt-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 204
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

DependencyTimeout

Il servizio è scaduto nel tentativo di soddisfare la richiesta e il client dovrebbe riprovare a effettuare la chiamata.

Codice di stato HTTP: 504

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

MountTargetNotFound

Restituito se non è presente alcun target di montaggio con l'ID specificato trovato in Account AWS del chiamante.

Codice di stato HTTP: 404

## Esempi

Rimozione del target di montaggio di un file system

L'esempio seguente invia una richiesta DELETE per eliminare un target di montaggio specifico.

Richiesta di esempio

```
DELETE /2015-02-01/mount-targets/fsmt-9a13661e HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T232908Z
Authorization: <...>
```

Risposta di esempio

```
HTTP/1.1 204 No Content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3

- SDK AWS per Python
- SDK AWS per Ruby V3

# DeleteReplicationConfiguration

Elimina una configurazione di replica. L'eliminazione di una configurazione di replica termina il processo di replica. Dopo aver eliminato una configurazione di replica, il file system di destinazione diventa `Writeable` e la protezione da sovrascrittura della replica viene riattivata. Per ulteriori informazioni, consulta Eliminazione della configurazione di replica.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DeleteReplicationConfiguration`.

## Sintassi della richiesta

```
DELETE /2015-02-01/file-systems/SourceFileSystemId/replication-configuration HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

SourceFileSystemId

L'ID del file system di origine nella configurazione di replica.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 204
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

ReplicationNotFound

Restituito se il file system specificato non dispone di una configurazione di replica.

Codice di stato HTTP: 404

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DeleteTags

> **Note**
>
> OBSOLETO: `DeleteTags` è obsoleto e non viene mantenuto. Per rimuovere i tag da una risorsa EFS, utilizza l'operazione API UntagResource.

Elimina i tag specificati da un file system. Se la richiesta `DeleteTags` include una chiave di tag che non esiste, Amazon EFS la ignora e non causa un errore. Per ulteriori informazioni sui limiti dei tag, consulta Restrizioni sui tag nella Guida per l'utente di AWS Billing and Cost Management.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DeleteTags`.

## Sintassi della richiesta

```
POST /2015-02-01/delete-tags/FileSystemId HTTP/1.1
Content-type: application/json

{
   "TagKeys": [ "string" ]
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

FileSystemId

L'ID del file system di cui si desidera eliminare i tag (String).

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

TagKeys

Un elenco di chiavi di tag da eliminare.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Campo obbligatorio: sì

## Sintassi della risposta

```
HTTP/1.1 204
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeAccessPoints

Restituisce la descrizione di un punto di accesso Amazon EFS specifico, se `AccessPointId` viene fornito. Se si fornisce un EFS `FileSystemId`, restituisce le descrizioni di tutti i punti di accesso per quel file system. È possibile fornire un `AccessPointId` o un `FileSystemId` nella richiesta, ma non entrambi.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DescribeAccessPoints`.

## Sintassi della richiesta

```
GET /2015-02-01/access-points?
AccessPointId=AccessPointId&FileSystemId=FileSystemId&MaxResults=MaxResults&NextToken=NextToken
 HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

AccessPointId

(Facoltativo) Specifica un punto di accesso EFS da descrivere nella risposta; si esclude a vicenda con `FileSystemId`.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

FileSystemId

(Facoltativo) Se si fornisce un `FileSystemId`, EFS restituisce tutti i punti di accesso per quel file system; si esclude a vicenda con `AccessPointId`.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

MaxResults

(Facoltativo) Quando recuperi tutti i punti di accesso per un file system, puoi facoltativamente specificare il parametro `MaxItems` per limitare il numero di oggetti restituiti in una risposta. Il valore predefinito è 100.

Intervallo valido: valore minimo di 1.

NextToken

`NextToken` è presente se la risposta è impaginata. È possibile utilizzare `NextMarker` in una richiesta successiva per recuperare la pagina successiva di descrizioni dei punti di accesso.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
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"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### AccessPoints

Una serie di descrizioni dei punti di accesso.

Tipo: matrice di oggetti AccessPointDescription

### NextToken

Presente se ci sono più punti di accesso di quelli restituiti nella risposta. È possibile utilizzare il NextMarker nella richiesta successiva per recuperare le descrizioni aggiuntive.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

## Errori

AccessPointNotFound

Restituito se il valore `AccessPointId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per V3 JavaScript
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeAccountPreferences

Restituisce le impostazioni delle preferenze di Account AWS associate all'utente che effettua la richiesta in Regione AWS corrente.

## Sintassi della richiesta

```
GET /2015-02-01/account-preferences HTTP/1.1
Content-type: application/json

{
   "MaxResults": number,
   "NextToken": "string"
}
```

## Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

(Facoltativo) Quando recuperi le preferenze dell'account, puoi facoltativamente specificare il parametro `MaxItems` per limitare il numero di oggetti restituiti in una risposta. Il valore predefinito è 100.

Tipo: integer

Intervallo valido: valore minimo di 1.

Campo obbligatorio: no

NextToken

(Facoltativo) È possibile utilizzare `NextToken` in una richiesta successiva per recuperare la pagina successiva delle preferenze Account AWS se il payload della risposta è stato impaginato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

Campo obbligatorio: no

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ResourceIdPreference": {
      "ResourceIdType": "string",
      "Resources": [ "string" ]
   }
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### NextToken

Presente se ci sono più record di quelli restituiti nella risposta. Puoi utilizzare `NextToken` nella richiesta seguente per recuperare le descrizioni aggiuntive.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

### ResourceIdPreference

Descrive l'impostazione delle preferenze relative all'ID della risorsa Account AWS associata all'utente che effettua la richiesta in Regione AWS corrente.

Tipo: oggetto ResourceIdPreference

## Errori

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeBackupPolicy

Restituisce la policy di backup per il file system EFS specificato.

## Sintassi della richiesta

```
GET /2015-02-01/file-systems/FileSystemId/backup-policy HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

FileSystemId

Specifica il file system EFS per il quale recuperare `BackupPolicy`.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPolicy": {
      "Status": "string"
   }
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPolicy

Descrive la policy di backup del file system, indicando se i backup automatici sono attivati o disattivati.

Tipo: oggetto BackupPolicy

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

PolicyNotFound

Restituito se è valida la policy di file system predefinita per il file system EFS specificato.

Codice di stato HTTP: 404

ValidationException

Restituito se il servizio AWS Backup non è disponibile in Regione AWS, dove è stata effettuata la richiesta.

Codice di stato HTTP: 400

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeFileSystemPolicy

Restituisce `FileSystemPolicy` per il file system EFS specificato.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DescribeFileSystemPolicy`.

## Sintassi della richiesta

```
GET /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

FileSystemId

Specifica il file system EFS per cui eliminare `FileSystemPolicy`.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "FileSystemId": "string",
   "Policy": "string"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

FileSystemId

Specifica il file system EFS a cui `FileSystemPolicy` si applica.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Policy

`FileSystemPolicy` formattato JSON per il file system EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 20000.

Modello: `[\s\S]+`

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

PolicyNotFound

Restituito se è valida la policy di file system predefinita per il file system EFS specificato.

Codice di stato HTTP: 404

## Esempi

### Esempio

Questo esempio illustra un utilizzo di. DescribeFileSystemPolicy

#### Richiesta di esempio

```
GET /2015-02-01/file-systems/fs-01234567/policy HTTP/1.1
```

#### Risposta di esempio

```
{
    "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"
            }
        ]
    }
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per V3 JavaScript
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeFileSystems

Restituisce la descrizione di un file system Amazon EFS specifico se viene fornito il file system `CreationToken` o `FileSystemId`. In caso contrario, restituisce le descrizioni di tutti i file system appartenenti a Account AWS del chiamante in Regione AWS dell'endpoint che stai chiamando.

Quando recuperi tutte le descrizioni dei file system, puoi facoltativamente specificare il parametro `MaxItems` per limitare il numero di descrizioni in una risposta. Questo numero viene impostato automaticamente su 100. Se rimangono altre descrizioni del file system, Amazon EFS restituisce un token `NextMarker` opaco nella risposta. In questo caso, è necessario inviare una richiesta successiva con il parametro `Marker` di richiesta impostato sul valore `NextMarker`.

Per recuperare un elenco delle descrizioni del file system, questa operazione viene utilizzata in un processo iterativo, in cui `DescribeFileSystems` viene chiamato prima senza `Marker`, quindi l'operazione continua a chiamare con il parametro `Marker` impostato sul valore `NextMarker` della risposta precedente fino a quando la risposta non ha `NextMarker`.

L'ordine dei file system restituiti nella risposta di una chiamata `DescribeFileSystems` e l'ordine dei file system restituiti nelle risposte di un'iterazione di più chiamate non è specificato.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DescribeFileSystems`.

## Sintassi della richiesta

```
GET /2015-02-01/file-systems?
CreationToken=CreationToken&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems
 HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### CreationToken

(Facoltativo) Limita l'elenco al file system con questo token di creazione (String). Quando viene creato un file system Amazon EFS, viene specificato un token.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

FileSystemId

(Facoltativo) ID del file system di cui desideri recuperare la descrizione (String).

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Marker

(Facoltativo) Un token di impaginazione opaco restituito dalla precedente operazione `DescribeFileSystems` (String). Se presente, specifica di continuare l'elenco dal punto in cui era stata interrotta la chiamata.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

MaxItems

(Facoltativo) Specifica il numero (intero) massimo di file system da restituire nella risposta. Questo numero viene impostato automaticamente su 100. La risposta viene impaginata a 100 per pagina se sono presenti più di 100 file system.

Intervallo valido: valore minimo di 1.

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
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"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### FileSystems

Una serie di descrizioni del file system.

Tipo: matrice di oggetti FileSystemDescription

Marker

Presente se fornito dal chiamante nella richiesta (String).

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

NextMarker

Presente se vi sono più file system di quelli restituiti nella risposta (String). È possibile utilizzare `NextMarker` in una richiesta successiva per recuperare ulteriori descrizioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Esempi

### Recupero di un elenco di 10 file system

L'esempio seguente invia una richiesta GET all'endpoint `file-systems` (`elasticfilesystem.us-west-2.amazonaws.com/2015-02-01/file-systems`). La richiesta specifica un parametro `MaxItems` di query per limitare il numero di descrizioni del file system a 10.

#### Richiesta di esempio

```
GET /2015-02-01/file-systems?MaxItems=10 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T191208Z
Authorization: <...>
```

#### Risposta di esempio

```
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
         }
      }
   ]
```

```
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeLifecycleConfiguration

Restituisce l'oggetto `LifecycleConfiguration` corrente per il file system Amazon EFS specificato. La gestione del ciclo di vita utilizza l'oggetto `LifecycleConfiguration` per identificare quando spostare i file tra le classi di storage. Per un file system senza oggetto `LifecycleConfiguration`, la chiamata restituisce un array vuoto nella risposta.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DescribeLifecycleConfiguration`.

## Sintassi della richiesta

```
GET /2015-02-01/file-systems/FileSystemId/lifecycle-configuration HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

FileSystemId

L'ID del file system di cui si desidera recuperare l'oggetto `LifecycleConfiguration` (String).

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "LifecyclePolicies": [
```

```
      {
         "TransitionToArchive": "string",
         "TransitionToIA": "string",
         "TransitionToPrimaryStorageClass": "string"
      }
   ]
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LifecyclePolicies

Una serie di policy di gestione del ciclo di vita. EFS supporta al massimo una policy per file system.

Tipo: matrice di oggetti LifecyclePolicy

Membri della matrice: numero massimo di 3 elementi.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Esempi

### Recupero della configurazione del ciclo di vita per un file system

La richiesta seguente recupera l'oggetto `LifecycleConfiguration` per il file system specificato.

#### Richiesta di esempio

```
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: <...>
```

#### Risposta di esempio

```
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"
    }
  ]
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeMountTargets

Restituisce le descrizioni di tutti i target di montaggio correnti o un target di montaggio specifico, per un file system. Quando si richiedono tutti i target di montaggio correnti, l'ordine dei target di montaggio restituiti nella risposta non è specificato.

Questa operazione richiede le autorizzazioni per l'azione `elasticfilesystem:DescribeMountTargets`, sull'ID del file system specificato in `FileSystemId` o sul file system del target di montaggio specificato in `MountTargetId`.

## Sintassi della richiesta

```
GET /2015-02-01/mount-targets?
AccessPointId=AccessPointId&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems&MountTarg
 HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

AccessPointId

(Facoltativo) L'ID del punto di accesso di cui desideri elencare i target di montaggio. Deve essere incluso nella richiesta se nella stessa non è incluso `MountTargetId` o `FileSystemId`. Accetta un ID del punto di accesso o un ARN come input.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

FileSystemId

(Facoltativo) ID del file system di cui desideri elencare i target di montaggio (String). Deve essere incluso nella richiesta se non è incluso `MountTargetId` o `AccessPointId`. Accetta un ID del file system o un ARN come input.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Marker

(Facoltativo) Un token di impaginazione opaco restituito dalla precedente operazione `DescribeMountTargets` (String). Se presente, specifica di continuare l'elenco dal punto in cui era stata interrotta la chiamata precedente.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

MaxItems

(Facoltativo) Il numero massimo di target di montaggio da restituire nella risposta. Attualmente, questo numero viene impostato automaticamente su 10 e gli altri valori vengono ignorati. La risposta viene impaginata a 100 per pagina se si dispone di più di 100 target di montaggio.

Intervallo valido: valore minimo di 1.

MountTargetId

(Facoltativo) ID del target di montaggio da descrivere (String). Deve essere incluso nella richiesta se non è incluso `FileSystemId`. Accetta un ID di target di montaggio o un ARN come input.

Limitazioni di lunghezza: lunghezza minima pari a 13. Lunghezza massima di 45.

Modello: `^fsmt-[0-9a-f]{8,40}$`

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
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"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### Marker

Se la richiesta includeva `Marker`, la risposta restituisce tale valore in questo campo.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

### MountTargets

Restituisce i target di montaggio del file system sotto forma di matrice di oggetti `MountTargetDescription`.

Tipo: matrice di oggetti MountTargetDescription

### NextMarker

Se è presente un valore, vi sono più tag di montaggio da restituire. In una richiesta successiva, puoi fornire `Marker` nella richiesta con questo valore per recuperare il prossimo set di target di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

## Errori

AccessPointNotFound

Restituito se il valore `AccessPointId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

MountTargetNotFound

Restituito se non è presente alcun target di montaggio con l'ID specificato trovato in Account AWS del chiamante.

Codice di stato HTTP: 404

## Esempi

Recupero delle descrizioni dei target di montaggio creati per un file system

La richiesta seguente recupera le descrizioni dei target di montaggio creati per il file system specificato.

### Richiesta di esempio

```
GET /2015-02-01/mount-targets?FileSystemId=fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T191252Z
Authorization: <...>
```

### Risposta di esempio

```
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"
      }
   ]
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3

- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeMountTargetSecurityGroups

Restituisce i gruppi di sicurezza attualmente attivi per un target di montaggio. Questa operazione richiede che l'interfaccia di rete del target di montaggio sia stata creata e lo stato del ciclo di vita del target di montaggio non sia `deleted`.

Questa operazione richiede autorizzazioni per le seguenti azioni:

- azione `elasticfilesystem:DescribeMountTargetSecurityGroups` sul file system del target di montaggio.
- azione `ec2:DescribeNetworkInterfaceAttribute` sull'interfaccia di rete del target di montaggio.

## Sintassi della richiesta

```
GET /2015-02-01/mount-targets/MountTargetId/security-groups HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MountTargetId

L'ID del target di montaggio di cui vuoi recuperare i gruppi di sicurezza.

Limitazioni di lunghezza: lunghezza minima pari a 13. Lunghezza massima di 45.

Modello: `^fsmt-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "SecurityGroups": [ "string" ]
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

SecurityGroups

Un array di gruppi di sicurezza.

Tipo: matrice di stringhe

Membri della matrice: numero massimo di 100 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 11. Lunghezza massima di 43.

Modello: `^sg-[0-9a-f]{8,40}`

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

IncorrectMountTargetState

Restituito se il target di montaggio non è nello stato corretto per l'operazione.

Codice di stato HTTP: 409

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

MountTargetNotFound

Restituito se non è presente alcun target di montaggio con l'ID specificato trovato in Account AWS del chiamante.

Codice di stato HTTP: 404

## Esempi

Recupero dei gruppi di sicurezza in vigore per un file system

L'esempio seguente recupera i gruppi di sicurezza in vigore per l'interfaccia di rete associata a un target di montaggio.

Richiesta di esempio

```
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: <...>
```

Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Length: 57

{
"SecurityGroups" : [
"sg-188d9f74"
]
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeReplicationConfigurations

Recupera la configurazione di replica per un file system specifico. Se non viene specificato un file system, vengono recuperate tutte le configurazioni di replica relative a Account AWS in Regione AWS.

## Sintassi della richiesta

```
GET /2015-02-01/file-systems/replication-configurations?
FileSystemId=FileSystemId&MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

FileSystemId

È possibile recuperare la configurazione di replica per un file system specifico fornendo il relativo ID del file system.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

MaxResults

(Facoltativo) Puoi specificare il parametro `MaxItems` per limitare il numero di oggetti restituiti in una risposta. Il valore predefinito è 100.

Intervallo valido: valore minimo di 1.

NextToken

`NextToken` è presente se la risposta è impaginata. È possibile utilizzare `NextToken` in una richiesta successiva per recuperare la pagina successiva di output.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
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"
      }
   ]
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

È possibile utilizzare `NextToken` da una richiesta precedente in una richiesta successiva per recuperare ulteriori descrizioni.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

Replications

La raccolta di configurazioni di replica restituita.

Tipo: matrice di oggetti ReplicationConfigurationDescription

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

ReplicationNotFound

Restituito se il file system specificato non dispone di una configurazione di replica.

Codice di stato HTTP: 404

ValidationException

Restituito se il servizio AWS Backup non è disponibile in Regione AWS, dove è stata effettuata la richiesta.

Codice di stato HTTP: 400

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# DescribeTags

> **Note**
>
> OBSOLETO: l'azione `DescribeTags` è obsoleta e non viene mantenuta. Per visualizzare i tag associati alle risorse EFS, utilizza l'azione `ListTagsForResource` API.

Restituisce i tag associati a un file system. L'ordine dei tag restituiti nella risposta di una chiamata `DescribeTags` e l'ordine dei tag restituiti nelle risposte di un'iterazione a più chiamate (quando si utilizza l'impaginazione) non sono specificati.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DescribeTags`.

## Sintassi della richiesta

```
GET /2015-02-01/tags/FileSystemId/?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### FileSystemId

L'ID del file system da cui si desidera recuperare il set di tag.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

### Marker

(Facoltativo) Un token di impaginazione opaco restituito dalla precedente operazione `DescribeTags` (String). Se presente, specifica di continuare l'elenco dal punto in cui era stata interrotta la chiamata precedente.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

MaxItems

(Facoltativo) Il numero massimo di tag del file system da restituire nella risposta. Attualmente, questo numero viene impostato automaticamente su 100 e gli altri valori vengono ignorati. La risposta viene impaginata a 100 per pagina se sono presenti più di 100 tag.

Intervallo valido: valore minimo di 1.

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "Marker": "string",
   "NextMarker": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Marker

Se la richiesta includeva `Marker`, la risposta restituisce tale valore in questo campo.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

NextMarker

Se è presente un valore, vi sono più tag da restituire. In una richiesta successiva, puoi fornire il valore di `NextMarker` come valore del parametro `Marker` nella richiesta successiva per recuperare il prossimo set di tag.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

Tags

Restituisce i tag associati al file system come una serie di oggetti `Tag`.

Tipo: matrice di oggetti Tag

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Esempi

### Recupero dei tag associati a un file system

La richiesta seguente recupera i tag (coppie chiave-valore) associati al file system specificato.

Richiesta di esempio

```
GET /2015-02-01/tags/fs-01234567/ HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T215404Z
Authorization: <...>
```

Risposta di esempio

```
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"
        }
    ]
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS

- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# ListTagsForResource

Elenca tutti i tag di una risorsa EFS di primo livello. È necessario fornire l'ID risorsa di cui si desidera recuperare i tag.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:DescribeAccessPoints`.

## Sintassi della richiesta

```
GET /2015-02-01/resource-tags/ResourceId?MaxResults=MaxResults&NextToken=NextToken
 HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

(Facoltativo) Specifica il numero massimo di oggetti tag da restituire nella risposta. Il valore predefinito è 100.

Intervallo valido: valore minimo di 1.

NextToken

(Opzionale) Si può usare `NextToken` in una richiesta successiva per recuperare la pagina successiva delle descrizioni dei punti di accesso se il payload della risposta è stato impaginato.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

ResourceId

Specifica la risorsa EFS per la quale si desidera recuperare i tag. È possibile recuperare i tag per i file system EFS e i punti di accesso utilizzando questo endpoint API.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(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})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### NextToken

`NextToken` è presente se il payload di risposta è impaginato. È possibile utilizzare `NextToken` in una richiesta successiva per recuperare la pagina successiva di descrizioni dei punti di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

### Tags

Un array di tag per la risorsa EFS specificata.

Tipo: matrice di oggetti Tag

## Errori

AccessPointNotFound

Restituito se il valore `AccessPointId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# ModifyMountTargetSecurityGroups

Modifica il set di gruppi di sicurezza attivi per un target di montaggio.

Quando crei un target di montaggio, Amazon EFS crea anche una nuova interfaccia di rete. Per ulteriori informazioni, consulta CreateMountTarget. Questa operazione sostituisce i gruppi di sicurezza in vigore per l'interfaccia di rete associata a un target di montaggio con quelli `SecurityGroups` forniti nella richiesta. Questa operazione richiede che l'interfaccia di rete del target di montaggio sia stata creata e lo stato del ciclo di vita del target di montaggio non sia `deleted`.

Questa operazione richiede autorizzazioni per le seguenti azioni:

- azione `elasticfilesystem:ModifyMountTargetSecurityGroups` sul file system del target di montaggio.
- azione `ec2:ModifyNetworkInterfaceAttribute` sull'interfaccia di rete del target di montaggio.

## Sintassi della richiesta

```
PUT /2015-02-01/mount-targets/MountTargetId/security-groups HTTP/1.1
Content-type: application/json

{
   "SecurityGroups": [ "string" ]
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MountTargetId

L'ID del target di montaggio di cui si desidera modificare i gruppi di sicurezza.

Limitazioni di lunghezza: lunghezza minima pari a 13. Lunghezza massima di 45.

Modello: `^fsmt-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

SecurityGroups

Matrice con un massimo di cinque ID gruppo di sicurezza del VPC.

Tipo: matrice di stringhe

Membri della matrice: numero massimo di 100 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 11. Lunghezza massima di 43.

Modello: `^sg-[0-9a-f]{8,40}`

Campo obbligatorio: no

## Sintassi della risposta

```
HTTP/1.1 204
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

IncorrectMountTargetState

Restituito se il target di montaggio non è nello stato corretto per l'operazione.

Codice di stato HTTP: 409

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

MountTargetNotFound

Restituito se non è presente alcun target di montaggio con l'ID specificato trovato in Account AWS del chiamante.

Codice di stato HTTP: 404

SecurityGroupLimitExceeded

Restituito se la dimensione di `SecurityGroups` specificata nella richiesta è maggiore di cinque.

Codice di stato HTTP: 400

SecurityGroupNotFound

Restituito se uno dei gruppi di sicurezza specificati non esiste nel cloud privato virtuale (VPC) della sottorete.

Codice di stato HTTP: 400

## Esempi

Sostituisce i gruppi di sicurezza di un target di montaggio

L'esempio seguente sostituisce i gruppi di sicurezza in vigore per l'interfaccia di rete associata a un target di montaggio.

Richiesta di esempio

```
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"
  ]
}
```

### Risposta di esempio

```
HTTP/1.1 204 No Content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# PutAccountPreferences

Utilizza questa operazione per impostare la preferenza dell'account nel corrente Regione AWS per utilizzare ID di risorsa lunghi da 17 caratteri (63 bit) o brevi da 8 caratteri (32 bit) per il nuovo file system EFS e installare le risorse di destinazione. Tutti gli ID delle risorse esistenti non sono influenzati dalle modifiche apportate. È possibile impostare la preferenza ID durante il periodo di attivazione, poiché EFS passa a ID di risorse lunghi. Per ulteriori informazioni, consulta Gestione degli ID di risorse Amazon EFS.

> **Note**
>
> A partire da ottobre 2021, riceverai un errore se tenti di impostare la preferenza dell'account per utilizzare l'ID di risorsa in formato breve a 8 caratteri. Contatta il supporto AWS se ricevi un errore e devi utilizzare ID brevi per il file system e per installare le risorse di destinazione.

## Sintassi della richiesta

```
PUT /2015-02-01/account-preferences HTTP/1.1
Content-type: application/json

{
   "ResourceIdType": "string"
}
```

## Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

ResourceIdType

Specifica la preferenza dell'ID di risorsa EFS da impostare per l'utente Account AWS nel corrente Regione AWS per `LONG_ID` (17 caratteri) o `SHORT_ID` (8 caratteri).

> **Note**
>
> A partire da ottobre 2021, riceverai un errore quando imposti la preferenza dell'account su `SHORT_ID`. Contatta il supporto AWS se ricevi un errore e devi utilizzare ID brevi per il file system e per installare le risorse di destinazione.

Tipo: stringa

Valori validi: `LONG_ID | SHORT_ID`

Campo obbligatorio: sì

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceIdPreference": {
      "ResourceIdType": "string",
      "Resources": [ "string" ]
   }
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ResourceIdPreference

Descrive il tipo di risorsa e la relativa preferenza ID per Account AWS dell'utente nel corrente Regione AWS.

Tipo: oggetto ResourceIdPreference

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# PutBackupPolicy

Aggiorna la policy di backup del file system. Utilizza questa azione per avviare o interrompere i backup automatici del file system.

## Sintassi della richiesta

```
PUT /2015-02-01/file-systems/FileSystemId/backup-policy HTTP/1.1
Content-type: application/json

{
   "BackupPolicy": {
      "Status": "string"
   }
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

FileSystemId

Specifica per quale file system EFS aggiornare la policy di backup.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupPolicy

La policy di backup inclusa nella richiesta `PutBackupPolicy`.

Tipo: oggetto BackupPolicy

Campo obbligatorio: sì

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPolicy": {
      "Status": "string"
   }
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPolicy

Descrive la policy di backup del file system, indicando se i backup automatici sono attivati o disattivati.

Tipo: oggetto BackupPolicy

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

ValidationException

Restituito se il servizio AWS Backup non è disponibile in Regione AWS, dove è stata effettuata la richiesta.

Codice di stato HTTP: 400

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# PutFileSystemPolicy

Applica un `FileSystemPolicy` Amazon EFS a un file system Amazon EFS. Una policy di file system è una policy basata su risorse IAM e può contenere più istruzioni di policy. Un file system contiene sempre esattamente una policy del file system, che può essere la policy predefinita o una policy esplicita impostata o aggiornata utilizzando questa operazione API. Le policy del file system EFS hanno un limite di 20.000 caratteri. Quando viene impostata una policy esplicita, questa sostituisce la policy predefinita. Per ulteriori informazioni sulla politica del file system predefinita, vedere Politica del file system EFS predefinita.

> **Note**
>
> Le policy del file system EFS hanno un limite di 20.000 caratteri.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:PutFileSystemPolicy`.

## Sintassi della richiesta

```
PUT /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
Content-type: application/json

{
   "BypassPolicyLockoutSafetyCheck": boolean,
   "Policy": "string"
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### FileSystemId

ID del file system EFS per il quale si desidera creare o aggiornare `FileSystemPolicy`.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BypassPolicyLockoutSafetyCheck

(Facoltativo) Un valore booleano che specifica se ignorare o meno il controllo di sicurezza del blocco della `FileSystemPolicy`. Il controllo di sicurezza del blocco determina se la policy nella richiesta bloccherà, o impedirà, al principal IAM che sta effettuando la richiesta di fare richieste `PutFileSystemPolicy` future su questo file system. Imposta `BypassPolicyLockoutSafetyCheck` su `True` solo quando intendi impedire al principal IAM che sta effettuando la richiesta di effettuare richieste `PutFileSystemPolicy` successive su questo file system. Il valore predefinito è `False`.

Tipo: Booleano

Campo obbligatorio: no

Policy

`FileSystemPolicy` in fase di creazione. Accetta una definizione di policy in formato JSON. Le policy del file system EFS hanno un limite di 20.000 caratteri. Per ulteriori informazioni sugli elementi che costituiscono una policy del file system, consulta Policy basate sulle risorse all'interno di Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 20000.

Modello: `[\s\S]+`

Campo obbligatorio: sì

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "FileSystemId": "string",
   "Policy": "string"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

FileSystemId

Specifica il file system EFS a cui `FileSystemPolicy` si applica.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Policy

`FileSystemPolicy` formattato JSON per il file system EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 20000.

Modello: `[\s\S]+`

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

InvalidPolicyException

Restituito se `FileSystemPolicy` non è valido o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante. Restituito in caso di errore di controllo di sicurezza relativo al blocco delle policy.

Codice di stato HTTP: 400

## Esempi

### Crea un EFS FileSystemPolicy

La seguente richiesta crea un `FileSystemPolicy` che consente a tutti i principali AWS di installare il file system EFS specificato con autorizzazioni di lettura e scrittura.

Richiesta di esempio

```
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": ["*"]
            },
```

```
        }
    ]
}
```

Risposta di esempio

```
{
    "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-1:111122233334444:file-
system/fs-01234567"
        }
    ]
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python

- SDK AWS per Ruby V3

# PutLifecycleConfiguration

Utilizza questa azione per gestire lo storage per il file system. `LifecycleConfiguration` è costituito da uno o più oggetti `LifecyclePolicy` che definiscono quanto segue:

- **`TransitionToIA`** : quando spostare i file nel file system dalla classe di storage principale (classe di storage Standard) alla classe di storage Infrequent Access (IA).
- **`TransitionToArchive`** : quando spostare i file nel file system dalla classe di storage corrente (storage IA o Standard) allo storage di archivio.

  I file system non possono passare allo storage di archivio prima di passare allo storage IA. Pertanto, non TransitionToArchive deve essere impostato o deve essere successivo a TransitionTo IA.

  > **Note**
  >
  > La classe di archiviazione Archive è disponibile solo per i file system che utilizzano la modalità Elastic throughput e la modalità di prestazioni General Purpose.

- **`TransitionToPrimaryStorageClass`** : quando spostare i file nel file system sullo storage principale (classe di storage Standard) dopo avervi effettuato l'accesso nello storage IA o di archivio.

Per ulteriori informazioni, consulta Gestione dello storage del file system.

Ogni file system Amazon EFS supporta una configurazione del ciclo di vita, che si applica a tutti i file del file system. Se esiste già un oggetto `LifecycleConfiguration` per il file system specificato, una chiamata `PutLifecycleConfiguration` modifica la configurazione esistente. Una chiamata `PutLifecycleConfiguration` con un array `LifecyclePolicies` vuoto nel corpo della richiesta elimina qualsiasi `LifecycleConfiguration` esistente. Nella richiesta, specifica quanto segue:

- L'ID del file system per il quale state abilitando, disabilitando o modificando la gestione del ciclo di vita.
- Una matrice `LifecyclePolicies` di oggetti `LifecyclePolicy` che definiscono quando spostare i file nello storage IA, nello storage di archivio e nuovamente nello storage principale.

> **Note**
>
> Amazon EFS richiede che ogni oggetto `LifecyclePolicy` abbia una sola transizione, quindi la matrice `LifecyclePolicies` deve essere strutturata con oggetti `LifecyclePolicy` separati. Per ulteriori informazioni, consulta le richieste di esempio nelle sezioni seguenti.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:PutLifecycleConfiguration`.

Per applicare un oggetto `LifecycleConfiguration` a un file system crittografato, sono necessarie le stesse autorizzazioni AWS Key Management Service di quando hai creato il file system crittografato.

## Sintassi della richiesta

```
PUT /2015-02-01/file-systems/FileSystemId/lifecycle-configuration HTTP/1.1
Content-type: application/json

{
   "LifecyclePolicies": [
      {
         "TransitionToArchive": "string",
         "TransitionToIA": "string",
         "TransitionToPrimaryStorageClass": "string"
      }
   ]
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### FileSystemId

L'ID del file system per il quale stai creando l'oggetto `LifecycleConfiguration` (stringa).

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

### LifecyclePolicies

Una matrice di oggetti `LifecyclePolicy` che definiscono l'oggetto `LifecycleConfiguration` del file system. Un `LifecycleConfiguration` oggetto indica alla gestione del ciclo di vita quanto segue:

- **`TransitionToIA`** : quando spostare i file nel file system dalla classe di storage principale (classe di storage Standard) alla classe di storage Infrequent Access (IA).
- **`TransitionToArchive`** : quando spostare i file nel file system dalla classe di storage corrente (storage IA o Standard) allo storage di archivio.

  I file system non possono passare allo storage di archivio prima di passare allo storage IA. Pertanto, non TransitionToArchive deve essere impostato o deve essere successivo a IA. TransitionTo

  > **Note**
  >
  > La classe di archiviazione Archive è disponibile solo per i file system che utilizzano la modalità Elastic throughput e la modalità di prestazioni General Purpose.

- **`TransitionToPrimaryStorageClass`** : quando spostare i file nel file system sullo storage principale (classe di storage Standard) dopo avervi effettuato l'accesso nello storage IA o di archivio.

> **Note**
>
> Quando si utilizza il comando `put-lifecycle-configuration` CLI o l'azione `PutLifecycleConfiguration` API, Amazon EFS richiede che ogni oggetto `LifecyclePolicy` abbia una sola transizione. Ciò significa che, nel corpo di una richiesta, `LifecyclePolicies` deve essere strutturato come una matrice di oggetti

`LifecyclePolicy`, ossia un oggetto per ogni transizione di storage. Per ulteriori informazioni, consulta le richieste di esempio nelle sezioni seguenti.

Tipo: matrice di oggetti LifecyclePolicy

Membri della matrice: numero massimo di 3 elementi.

Campo obbligatorio: sì

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "LifecyclePolicies": [
      {
         "TransitionToArchive": "string",
         "TransitionToIA": "string",
         "TransitionToPrimaryStorageClass": "string"
      }
   ]
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LifecyclePolicies

Una serie di policy di gestione del ciclo di vita. EFS supporta al massimo una policy per file system.

Tipo: matrice di oggetti LifecyclePolicy

Membri della matrice: numero massimo di 3 elementi.

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Esempi

Creazione di una configurazione del ciclo di vita

L'esempio seguente crea un oggetto `LifecyclePolicy` utilizzando l'azione `PutLifecycleConfiguration`. Questo esempio crea una policy del ciclo di vita che richiede a EFS di eseguire queste operazioni:

- Spostare tutti i file del file system a cui non è stato effettuato l'accesso nello storage Standard negli ultimi 30 giorni nello storage IA.
- Spostare tutti i file del file system a cui non è stato effettuato l'accesso nello storage Standard negli ultimi 90 giorni nello storage IA.
- Riportare i file nello storage Standard dopo avervi effettuato l'accesso nello storage IA o di archivio. La classe di archiviazione Archive è disponibile solo per i file system che utilizzano la modalità Elastic throughput e la modalità di prestazioni General Purpose.

Per ulteriori informazioni, consulta Classi di storage EFS e Gestione dello storage del file system.

### Richiesta di esempio

```
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"
      }
   ]
}
```

### Risposta di esempio

```
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"
```

```
      }
    ]
}
```

Richiesta put-lifecycle-configuration CLI di esempio

Questo esempio illustra un utilizzo di. PutLifecycleConfiguration

Richiesta di esempio

```
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
```

Risposta di esempio

```
{
   "LifecyclePolicies": [
       {
           "TransitionToArchive": "AFTER_90_DAYS"
       },
       {
           "TransitionToIA": "AFTER_30_DAYS"
       },
       {
           "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
       }
   ]
}
```

Disattivazione della gestione del ciclo di vita

L'esempio seguente disattiva la gestione del ciclo di vita per il file system specificato.

Richiesta di esempio

```
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": [ ]
}
```

Risposta di esempio

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-type: application/json
Content-Length: 86

{
   "LifecyclePolicies": [ ]
}
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per V3 JavaScript
- SDK AWS per PHP V3
- SDK AWS per Python

- SDK AWS per Ruby V3

# TagResource

Crea un tag per una risorsa EFS. È possibile creare tag per i file system e gli access point EFS utilizzando questa operazione API.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:TagResource`.

## Sintassi della richiesta

```
POST /2015-02-01/resource-tags/ResourceId HTTP/1.1
Content-type: application/json

{
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### ResourceId

L'ID che specifica la risorsa EFS per la quale desideri creare un tag.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(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})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

### Tags

Una matrice di oggetti `Tag` da aggiungere. Ogni oggetto `Tag` è una coppia chiave-valore.

Tipo: matrice di oggetti Tag

Campo obbligatorio: sì

## Sintassi della risposta

```
HTTP/1.1 200
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

## Errori

AccessPointNotFound

Restituito se il valore `AccessPointId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Esempi

Creazione di tag su un file system

La richiesta seguente crea tre tag (`"key1"`, `"key2"` e `"key3"`) nel file system specificato.

### Richiesta di esempio

```
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"
        }
    ]
}
```

### Risposta di esempio

```
HTTP/1.1 204 no content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2

- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# UntagResource

Rimuove i tag da una risorsa EFS. È possibile rimuovere tag per i file system e gli access point EFS utilizzando questa operazione API.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:UntagResource`.

## Sintassi della richiesta

```
DELETE /2015-02-01/resource-tags/ResourceId?tagKeys=TagKeys HTTP/1.1
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

ResourceId

Specifica la risorsa EFS da cui si desidera rimuovere i tag.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(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})$`

Campo obbligatorio: sì

TagKeys

Le chiavi delle coppie chiave-valore associate ai tag da rimuovere dalla risorsa EFS specificata.

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Modello: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta non ha un corpo della richiesta.

## Sintassi della risposta

```
HTTP/1.1 200
```

## Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

## Errori

AccessPointNotFound

Restituito se il valore `AccessPointId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per JavaScript V3
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# UpdateFileSystem

Aggiorna la modalità di throughput o la quantità di throughput assegnato di un file system esistente.

## Sintassi della richiesta

```
PUT /2015-02-01/file-systems/FileSystemId HTTP/1.1
Content-type: application/json

{
   "ProvisionedThroughputInMibps": number,
   "ThroughputMode": "string"
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### FileSystemId

L'ID del file system che si desidera aggiornare.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

### ProvisionedThroughputInMibps

(Facoltativo) La velocità effettiva, misurata in mebibyte al secondo (MiBps), che si desidera fornire per un file system in fase di creazione. Obbligatorio se `ThroughputMode` è impostato su `provisioned`. I valori validi sono 1-3414 MiBps, con il limite superiore a seconda della regione. Per aumentare questo limite, contatta AWS Support. Per ulteriori informazioni, consulta Quote di Amazon EFS che è possibile incrementare nella Guida per l'utente di Amazon EFS.

Tipo: double

Intervallo valido: valore minimo di 1.0.

Campo obbligatorio: no

ThroughputMode

(Facoltativo) Aggiorna la modalità di trasmissione del file system. Se non state aggiornando la modalità di throughput, non è necessario fornire questo valore nella richiesta. Se `ThroughputMode` è impostato su `provisioned`, è necessario impostare anche un valore per `ProvisionedThroughputInMibps`.

Tipo: stringa

Valori validi: `bursting | provisioned | elastic`

Campo obbligatorio: no

## Sintassi della risposta

```
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"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 202.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### AvailabilityZoneId

L'identificatore univoco e coerente della zona di disponibilità in cui si trova il file system, valido solo per i file system a zona singola. Ad esempio, `use1-az1` è un ID di zona di disponibilità per la regione us-east-1 Regione AWS e identifica la stessa posizione in ogni Account AWS.

Tipo: stringa

### AvailabilityZoneName

Descrive la zona di disponibilità AWS in cui si trova il file system, valida solo per i file system a zona singola. Per ulteriori informazioni, consulta Utilizzo delle classi di archiviazione EFS nella Guida per l'utente di Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

### CreationTime

L'ora di creazione del file system, in secondi (da 1970-01-01T00:00:00Z).

Tipo: Timestamp

CreationToken

Stringa opaca specificata nella richiesta.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Encrypted

Valore booleano che, se "true", indica che il file system è crittografato.

Tipo: Booleano

FileSystemArn

Il nome della risorsa Amazon (ARN) per il file system Amazon EFS in formato `arn:aws:elasticfilesystem:`*`region`*`:`*`account-id`*`:file-system/`*`file-system-id`* . Esempio con dati campione: `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Tipo: stringa

FileSystemId

L'ID del file system, assegnato da Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

FileSystemProtection

Descrive la protezione del file system.

Tipo: oggetto FileSystemProtectionDescription

KmsKeyId

L'ID della AWS KMS key da utilizzare per proteggere il file system crittografato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^([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 di vita del file system.

Tipo: stringa

Valori validi: `creating | available | updating | deleting | deleted | error`

Name

È possibile aggiungere tag a un file system, incluso un tag `Name`. Per ulteriori informazioni, consulta CreateFileSystem. Se il file system ha un tag `Name`, Amazon EFS restituisce il valore in questo campo.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 256.

Modello: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

NumberOfMountTargets

Il numero attuale di target di montaggio del file system. Per ulteriori informazioni, consulta CreateMountTarget.

Tipo: integer

Intervallo valido: valore minimo di 0.

OwnerId

Account AWS che ha creato il file system.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

PerformanceMode

Le modalità di prestazioni dei file system.

Tipo: stringa

Valori validi: `generalPurpose | maxIO`

ProvisionedThroughputInMibps

La quantità di velocità effettiva assegnata, misurata in MiBps, per il file system. Valido per i file system che utilizzano `ThroughputMode` impostato su `provisioned`.

Tipo: double

Intervallo valido: valore minimo di 1.0.

SizeInBytes

L'ultima dimensione misurata nota (in byte) dei dati memorizzati nel file system, nel relativo campo `Value` e l'ora in cui tale dimensione è stata determinata nel campo `Timestamp`. Il valore `Timestamp` è il numero intero di secondi dal 1970-01-01T 00:00:00 Z. Il valore `SizeInBytes` non rappresenta la dimensione di un'istantanea coerente del file system, ma è coerente quando non vi sono operazioni di scrittura sul file system. Ossia, `SizeInBytes` rappresenta la dimensione effettiva solo se il file system non viene modificato per un periodo superiore a un paio d'ore. Altrimenti, il valore non corrisponde alla dimensione esatta che aveva il file system in qualsiasi momento.

Tipo: oggetto FileSystemSize

Tags

I tag associati al file system, presentati come una serie di oggetti `Tag`.

Tipo: matrice di oggetti Tag

ThroughputMode

Visualizza la modalità di throughput per un file system. Per ulteriori informazioni, consulta Modalità di throughput nella Guida per l'utente di Amazon EFS.

Tipo: stringa

Valori validi: `bursting | provisioned | elastic`

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InsufficientThroughputCapacity

Restituito se la capacità non è sufficiente per fornire un throughput aggiuntivo. Questo valore può essere restituito quando si tenta di creare un file system in modalità di throughput assegnato, quando si tenta di aumentare la velocità di trasmissione effettiva assegnata di un file system esistente o quando si tenta di modificare un file system esistente dalla modalità Bursting alla modalità Con provisioning. Riprova più tardi.

Codice di stato HTTP: 503

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

ThroughputLimitExceeded

Restituito se la modalità di throughput o la quantità di throughput assegnata non possono essere modificate perché è stato raggiunto il limite di throughput di 1024 MiB/s.

Codice di stato HTTP: 400

TooManyRequests

Restituito se non si attendono almeno 24 ore prima di modificare la modalità di throughput o di ridurre il valore del Provisioned Throughput.

Codice di stato HTTP: 429

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per V3 JavaScript
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

# UpdateFileSystemProtection

Aggiorna la protezione del file system.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:UpdateFileSystemProtection`.

## Sintassi della richiesta

```
PUT /2015-02-01/file-systems/FileSystemId/protection HTTP/1.1
Content-type: application/json

{
   "ReplicationOverwriteProtection": "string"
}
```

## Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

### FileSystemId

L'ID del file system che si desidera aggiornare.

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

## Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

### ReplicationOverwriteProtection

Lo stato della replica del file system sovrascrive la protezione.

- `ENABLED` - Non è possibile utilizzare un file system come file system di destinazione in un'altra configurazione di replica. Il file system è scrivibile. La protezione da sovrascrittura della replica è `ENABLED` per impostazione predefinita.

- `DISABLED` - È possibile utilizzare un file system come file system di destinazione in una configurazione di replica. Il file system è di sola lettura e viene modificato solo dalla replica EFS.
- `REPLICATING`: il file system è in uso come file system di destinazione in una configurazione di replica. Il file system è di sola lettura e viene modificato solo dalla replica EFS.

Se la configurazione di replica viene eliminata, la protezione da sovrascrittura della replica del file system viene riattivata e il file system diventa scrivibile.

Tipo: stringa

Valori validi: `ENABLED | DISABLED | REPLICATING`

Campo obbligatorio: no

## Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ReplicationOverwriteProtection": "string"
}
```

## Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

### ReplicationOverwriteProtection

Lo stato della replica del file system sovrascrive la protezione.

- `ENABLED` - Non è possibile utilizzare un file system come file system di destinazione in un'altra configurazione di replica. Il file system è scrivibile. La protezione da sovrascrittura della replica è `ENABLED` per impostazione predefinita.
- `DISABLED` - È possibile utilizzare un file system come file system di destinazione in una configurazione di replica. Il file system è di sola lettura e viene modificato solo dalla replica EFS.
- `REPLICATING`: il file system è in uso come file system di destinazione in una configurazione di replica. Il file system è di sola lettura e viene modificato solo dalla replica EFS.

Se si elimina la configurazione di replica, la protezione da sovrascrittura del file system viene riattivata e il file system diventa scrivibile.

Tipo: stringa

Valori validi: `ENABLED | DISABLED | REPLICATING`

## Errori

BadRequest

Restituito se la richiesta non è valida o contiene un errore, ad esempio un valore di parametro non valido o un parametro obbligatorio mancante.

Codice di stato HTTP: 400

FileSystemNotFound

Restituito se il valore `FileSystemId` specificato non esiste in Account AWS del richiedente.

Codice di stato HTTP: 404

IncorrectFileSystemLifeCycleState

Restituito se lo stato del ciclo di vita del file system non è “disponibile”.

Codice di stato HTTP: 409

InsufficientThroughputCapacity

Restituito se la capacità non è sufficiente per fornire un throughput aggiuntivo. Questo valore può essere restituito quando si tenta di creare un file system in modalità di throughput assegnato, quando si tenta di aumentare la velocità di trasmissione effettiva assegnata di un file system esistente o quando si tenta di modificare un file system esistente dalla modalità Bursting alla modalità Con provisioning. Riprova più tardi.

Codice di stato HTTP: 503

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

ReplicationAlreadyExists

Restituito se il file system è già incluso in una configurazione di replica.

Codice di stato HTTP: 409

ThroughputLimitExceeded

Restituito se la modalità di throughput o la quantità di throughput assegnata non possono essere modificate perché è stato raggiunto il limite di throughput di 1024 MiB/s.

Codice di stato HTTP: 400

TooManyRequests

Restituito se non si attendono almeno 24 ore prima di modificare la modalità di throughput o di ridurre il valore del Provisioned Throughput.

Codice di stato HTTP: 429

### Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- SDK AWS per .NET
- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- AWSSDK per V3 JavaScript
- SDK AWS per PHP V3
- SDK AWS per Python
- SDK AWS per Ruby V3

## Tipi di dati

Sono supportati i tipi di dati seguenti:

- AccessPointDescription
- BackupPolicy
- CreationInfo
- Destination
- DestinationToCreate
- FileSystemDescription
- FileSystemProtectionDescription
- FileSystemSize
- LifecyclePolicy
- MountTargetDescription
- PosixUser
- ReplicationConfigurationDescription
- ResourceIdPreference
- RootDirectory
- Tag

# AccessPointDescription

Fornisce una descrizione di un punto di accesso al file system EFS.

## Indice

AccessPointArn

Il nome della risorsa Amazon (ARN) associato al punto di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}$`

Campo obbligatorio: no

AccessPointId

L'ID del punto di accesso, assegnato da Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

Campo obbligatorio: no

ClientToken

La stringa opaca specificata nella richiesta per garantire la creazione idempotent.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: no

FileSystemId

ID del file system EFS a cui si applica il punto di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: no

LifeCycleState

Identifica la fase del ciclo di vita del punto di accesso.

Tipo: stringa

Valori validi: `creating | available | updating | deleting | deleted | error`

Campo obbligatorio: no

Name

Il nome del punto di accesso. Questo è il valore del tag `Name`.

Tipo: string

Campo obbligatorio: no

OwnerId

Identifica il proprietario (Account AWS) della risorsa del punto di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

Campo obbligatorio: no

PosixUser

Identità POSIX completa, inclusi ID utente, ID gruppo e ID gruppo secondario sul punto di accesso utilizzato per tutte le operazioni di file dai client NFS che utilizzano il punto di accesso.

Tipo: oggetto PosixUser

Campo obbligatorio: no

RootDirectory

La directory nel file system EFS che il punto di accesso espone come directory principale ai client NFS che utilizzano il punto di accesso.

Tipo: oggetto RootDirectory

Campo obbligatorio: no

Tags

I tag associati al punto di accesso, presentati come una serie di oggetti Tag.

Tipo: matrice di oggetti Tag

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# BackupPolicy

La policy di backup per il file system utilizzata per creare backup giornalieri automatici. Se il valore dello status è pari a `ENABLED`, viene eseguito automaticamente il backup del file system. Per ulteriori informazioni, consulta Backup automatici.

## Indice

Status

Descrive lo stato delle policy di backup per il file system.

- **`ENABLED`** : EFS esegue automaticamente il backup del file system.
- **`ENABLING`** : EFS attiva i backup automatici per il file system.
- **`DISABLED`** : disattiva i backup automatici per il file system.
- **`DISABLING`** : EFS disattiva i backup automatici per il file system.

Tipo: stringa

Valori validi: `ENABLED | ENABLING | DISABLED | DISABLING`

Campo obbligatorio: sì

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# CreationInfo

Obbligatorio se `RootDirectory` > `Path` specificato non esiste. Specifica gli ID POSIX e le autorizzazioni da applicare a `RootDirectory` > `Path` del punto di accesso. Se la directory principale del punto di accesso non esiste, EFS la crea con queste impostazioni quando un client si connette al punto di accesso. Quando si specifica `CreationInfo`, è necessario includere valori per tutte le proprietà.

Amazon EFS crea una directory principale solo se hai fornito CreationInfo: OwnUid, OwnGID e autorizzazioni per la directory. Se non fornisci queste informazioni, Amazon EFS non crea la directory principale. Se la directory principale non esiste, i tentativi di montaggio utilizzando il punto di accesso avranno esito negativo.

> **Important**
>
> Se non si fornisce `CreationInfo` e il `RootDirectory` specificato non esiste, i tentativi di montare il file system utilizzando il punto di accesso avranno esito negativo.

## Indice

OwnerGid

Specifica l'ID gruppo POSIX da applicare a `RootDirectory`. Accetta valori compresi tra 0 e 2^32 (4294967295).

Tipo: long

Intervallo valido: valore minimo di 0. Valore pari a 50.

Campo obbligatorio: sì

OwnerUid

Specifica l'ID utente POSIX da applicare a `RootDirectory`. Accetta valori compresi tra 0 e 2^32 (4294967295).

Tipo: long

Intervallo valido: valore minimo di 0. Valore pari a 50.

Campo obbligatorio: sì

Permissions

Specifica le autorizzazioni POSIX da applicare a `RootDirectory`, nel formato di un numero ottale che rappresenta i bit di modalità del file.

Tipo: String

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 4 caratteri.

Pattern: `^[0-7]{3,4}$`

Campo obbligatorio: sì

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- AWS SDK per Java V2
- SDK AWS per Ruby V3

# Destination

Descrive, nella configurazione di replica, il file system di destinazione.

## Indice

FileSystemId

ID del file system Amazon EFS di destinazione.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

Region

Regione AWS in cui si trova il file system di destinazione.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Campo obbligatorio: sì

Status

Descrive lo stato del file system EFS di destinazione.

- Lo stato `Paused` si verifica a seguito della disattivazione della regione di origine o di destinazione dopo la creazione della configurazione di replica. Per riprendere la replica per la regione, devi attivare nuovamente Regione AWS. Per ulteriori informazioni, consulta Gestione di Regioni AWS nella Guida di riferimento generale di AWS.
- Lo stato `Error` si verifica quando il file system di origine o di destinazione (o entrambi) si trova in uno stato di errore irreversibile. Per ulteriori informazioni, consulta Monitoraggio dello stato di replica nella Guida per l'utente di Amazon EFS. Devi eliminare la configurazione di replica e ripristinare il backup più recente del file system non riuscito (di origine o di destinazione) su un nuovo file system.

Tipo: stringa

Valori validi: `ENABLED | ENABLING | DELETING | ERROR | PAUSED | PAUSING`

Campo obbligatorio: sì

LastReplicatedTimestamp

L'ora in cui la sincronizzazione più recente è stata completata correttamente nel file system di destinazione. Tutte le modifiche ai dati sul file system di origine apportate prima di questo periodo sono state replicate correttamente nel file system di destinazione. Qualsiasi modifica apportata dopo questo periodo potrebbe non essere replicata completamente.

Tipo: Timestamp

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# DestinationToCreate

Descrive, nella configurazione di replica, il file system di destinazione nuovo o esistente.

## Indice

AvailabilityZoneName

Per creare un file system che utilizza lo storage a zona singola, specifica il nome della zona di disponibilità in cui creare il file system di destinazione.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: no

FileSystemId

L'ID del file system da utilizzare per la destinazione. La replica da sovrascrittura della replica del file system deve essere disabilitata. Se non si fornisce un ID, EFS crea un nuovo file system per la destinazione di replica.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: no

KmsKeyId

Specifica la chiave AWS Key Management Service (AWS KMS) utilizzata per crittografare il file system di destinazione. Se non specifichi una chiave KMS, Amazon EFS utilizza la tua chiave KMS predefinita per Amazon EFS, `/aws/elasticfilesystem`. Questo ID può essere in uno dei seguenti formati:

- ID chiave: un identificatore univoco della chiave, ad esempio `1234abcd-12ab-34cd-56ef-1234567890ab`.

- ARN: un nome della risorsa Amazon (ARN) per la chiave, ad esempio `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- Alias chiave: un nome di visualizzazione creato in precedenza per una chiave, ad esempio `alias/projectKey1`.
- ARN alias della chiave: un ARN per un alias della chiave, ad esempio `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^([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/_-]+))))$`

Campo obbligatorio: no

Region

Per creare un file system che utilizza lo storage regionale, specifica Regione AWS in cui creare il file system di destinazione.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# FileSystemDescription

Una descrizione del file system.

## Indice

CreationTime

L'ora di creazione del file system, in secondi (da 1970-01-01T00:00:00Z).

Tipo: Timestamp

Campo obbligatorio: sì

CreationToken

Stringa opaca specificata nella richiesta.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: sì

FileSystemId

L'ID del file system, assegnato da Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

LifeCycleState

La fase del ciclo di vita del file system.

Tipo: stringa

Valori validi: `creating | available | updating | deleting | deleted | error`

Campo obbligatorio: sì

NumberOfMountTargets

Il numero attuale di target di montaggio del file system. Per ulteriori informazioni, consulta CreateMountTarget.

Tipo: integer

Intervallo valido: valore minimo di 0.

Campo obbligatorio: sì

OwnerId

Account AWS che ha creato il file system.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

Campo obbligatorio: sì

PerformanceMode

Le modalità di prestazioni dei file system.

Tipo: stringa

Valori validi: `generalPurpose | maxIO`

Campo obbligatorio: sì

SizeInBytes

L'ultima dimensione misurata nota (in byte) dei dati memorizzati nel file system, nel relativo campo `Value` e l'ora in cui tale dimensione è stata determinata nel campo `Timestamp`. Il valore `Timestamp` è il numero intero di secondi dal 1970-01-01T 00:00:00 Z. Il valore `SizeInBytes` non rappresenta la dimensione di un'istantanea coerente del file system, ma è coerente quando non vi sono operazioni di scrittura sul file system. Ossia, `SizeInBytes` rappresenta la dimensione effettiva solo se il file system non viene modificato per un periodo superiore a un

paio d'ore. Altrimenti, il valore non corrisponde alla dimensione esatta che aveva il file system in qualsiasi momento.

Tipo: oggetto FileSystemSize

Campo obbligatorio: sì

Tags

I tag associati al file system, presentati come una serie di oggetti `Tag`.

Tipo: matrice di oggetti Tag

Campo obbligatorio: sì

AvailabilityZoneId

L'identificatore univoco e coerente della zona di disponibilità in cui si trova il file system, valido solo per i file system a zona singola. Ad esempio, `use1-az1` è un ID di zona di disponibilità per la regione us-east-1 Regione AWS e identifica la stessa posizione in ogni Account AWS.

Tipo: string

Campo obbligatorio: no

AvailabilityZoneName

Descrive la zona di disponibilità AWS in cui si trova il file system, valida solo per i file system a zona singola. Per ulteriori informazioni, consulta Utilizzo delle classi di archiviazione EFS nella Guida per l'utente di Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: no

Encrypted

Valore booleano che, se "true", indica che il file system è crittografato.

Tipo: Booleano

Campo obbligatorio: no

FileSystemArn

Il nome della risorsa Amazon (ARN) per il file system Amazon EFS in formato `arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id` . Esempio con dati campione: `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Tipo: string

Campo obbligatorio: no

FileSystemProtection

Descrive la protezione del file system.

Tipo: oggetto FileSystemProtectionDescription

Campo obbligatorio: no

KmsKeyId

L'ID della AWS KMS key da utilizzare per proteggere il file system crittografato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `^([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/_-]+))))$`

Campo obbligatorio: no

Name

È possibile aggiungere tag a un file system, incluso un tag `Name`. Per ulteriori informazioni, consulta CreateFileSystem. Se il file system ha un tag `Name`, Amazon EFS restituisce il valore in questo campo.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 256.

Modello: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Campo obbligatorio: no

ProvisionedThroughputInMibps

La quantità di velocità effettiva assegnata, misurata in MiBps, per il file system. Valido per i file system che utilizzano `ThroughputMode` impostato su `provisioned`.

Tipo: double

Intervallo valido: valore minimo di 1.0.

Campo obbligatorio: no

ThroughputMode

Visualizza la modalità di throughput per un file system. Per ulteriori informazioni, consulta Modalità di throughput nella Guida per l'utente di Amazon EFS.

Tipo: stringa

Valori validi: `bursting | provisioned | elastic`

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# FileSystemProtectionDescription

Descrive la protezione del file system.

## Indice

ReplicationOverwriteProtection

Lo stato della replica del file system sovrascrive la protezione.

- `ENABLED` - Non è possibile utilizzare un file system come file system di destinazione in un'altra configurazione di replica. Il file system è scrivibile. La protezione da sovrascrittura della replica è `ENABLED` per impostazione predefinita.
- `DISABLED` - È possibile utilizzare un file system come file system di destinazione in una configurazione di replica. Il file system è di sola lettura e viene modificato solo dalla replica EFS.
- `REPLICATING`: il file system è in uso come file system di destinazione in una configurazione di replica. Il file system è di sola lettura e viene modificato solo dalla replica EFS.

Se si elimina la configurazione di replica, la protezione da sovrascrittura del file system viene riattivata e il file system diventa scrivibile.

Tipo: stringa

Valori validi: `ENABLED | DISABLED | REPLICATING`

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# FileSystemSize

L'ultima dimensione misurata nota (in byte) dei dati memorizzati nel file system, nel relativo campo `Value` e l'ora in cui tale dimensione è stata determinata nel campo `Timestamp`. Il valore non rappresenta la dimensione di un'istantanea coerente del file system, ma è coerente quando non vi sono operazioni di scrittura sul file system. Ossia, il valore rappresenta la dimensione effettiva solo se il file system non viene modificato per un periodo superiore a un paio d'ore. Altrimenti, il valore non corrisponde alla dimensione esatta che aveva il file system in qualsiasi momento.

## Indice

Value

L'ultima dimensione misurata nota (in byte) dei dati archiviati nel file system.

Tipo: long

Intervallo valido: valore minimo di 0.

Campo obbligatorio: sì

Timestamp

L'ora in cui è stata determinata la dimensione dei dati restituiti nel campo `Value`. Il valore è il numero intero di secondi dal 1970-01-01T 00:00:00 Z.

Tipo: Timestamp

Campo obbligatorio: no

ValueInArchive

L'ultima dimensione misurata nota (in byte) dei dati memorizzati nella classe di storage EFS di archivio.

Tipo: long

Intervallo valido: valore minimo di 0.

Campo obbligatorio: no

ValueInIA

L'ultima dimensione misurata nota (in byte) dei dati memorizzati nella classe di storage EFS ad accesso infrequente.

Tipo: long

Intervallo valido: valore minimo di 0.

Campo obbligatorio: no

ValueInStandard

L'ultima dimensione misurata nota (in byte) dei dati memorizzati nella classe di storage EFS Standard.

Tipo: long

Intervallo valido: valore minimo di 0.

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# LifecyclePolicy

Descrive una policy utilizzata dalla gestione del ciclo di vita che specifica quando trasferire i file da e verso le classi di storage. Per ulteriori informazioni, consulta Gestione dello storage del file system.

> **Note**
>
> Quando si utilizza il comando `put-lifecycle-configuration` CLI o l'azione `PutLifecycleConfiguration` API, Amazon EFS richiede che ogni oggetto `LifecyclePolicy` abbia una sola transizione. Ciò significa che nel corpo di una richiesta, `LifecyclePolicies` deve essere strutturato come un array di oggetti `LifecyclePolicy`, un oggetto per ogni transizione. Per ulteriori informazioni, consulta le richieste di esempio in PutLifecycleConfiguration.

## Indice

TransitionToArchive

Il numero di giorni dopo l'ultimo accesso ai file nello storage principale (la classe di storage Standard) entro cui spostarli nello storage di archiviazione. Le operazioni sui metadati, ad esempio la creazione di un elenco di contenuti di una directory, non contano come accesso ai file.

Tipo: stringa

Valori validi: `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`

Campo obbligatorio: no

TransitionToIA

Il numero di giorni dopo l'ultimo accesso ai file nello storage primario (classe di archiviazione Standard) in cui spostarli nello storage ad accesso infrequente (IA). Le operazioni sui metadati, ad esempio la creazione di un elenco di contenuti di una directory, non contano come accesso ai file.

Tipo: stringa

Valori validi: `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`

Campo obbligatorio: no

TransitionToPrimaryStorageClass

Possibilità di riportare o meno i file nello storage primario (Standard) dopo avervi effettuato l'accesso nello storage IA o di archivio. Le operazioni sui metadati, ad esempio la creazione di un elenco di contenuti di una directory, non contano come accesso ai file.

Tipo: stringa

Valori validi: `AFTER_1_ACCESS`

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# MountTargetDescription

Fornisce una descrizione di un bersaglio di montaggio.

## Indice

FileSystemId

L'ID del file system a cui la destinazione di montaggio.

Tipo: String

Limitazioni di lunghezza: lunghezza massima di 128.

Pattern: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

LifeCycleState

Stato del ciclo di 100.

Tipo: String

Valori validi: `creating | available | updating | deleting | deleted | error`

Campo obbligatorio: sì

MountTargetId

ID del target di montaggio assegnato dal sistema.

Tipo: String

Vincoli di. Lunghezza massima di 100.

Pattern: `^fsmt-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

SubnetId

L'ID della sottorete del target di montaggio.

Tipo: String

Vincoli di. Lunghezza massima di 100.

Pattern: `^subnet-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

AvailabilityZoneId

L'identificatore univoco e coerente della zona di disponibilità in cui risiede il mount target. Ad esempio, `use1-az1` è un ID AZ per la regione us-east-1 e ha la stessa posizione in ogni. Account AWS

Tipo: string

Required: No

AvailabilityZoneName

Il nome della zona di disponibilità in cui si trova la destinazione di montaggio. Le zone di disponibilità sono mappate in modo indipendente con i nomi di ciascuna di esseAccount AWS. Ad esempio, la tua zona `us-east-1a` di disponibilità Account AWS potrebbe non essere la stessa `us-east-1a` di un'altraAccount AWS.

Tipo: String

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Required: No

IpAddress

Indirizzo in cui è possibile montare il file system utilizzando il mount target.

Tipo: String

Vincoli di 10. Lunghezza massima di 100.

Modello: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Required: No

NetworkInterfaceId

L'ID dell'interfaccia di rete creata da Amazon EFS quando ha creato la destinazione di montaggio.

Tipo: string

Required: No

OwnerId

Account AWSL'ID proprietario della risorsa.

Tipo: String

Vincoli di.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

Required: No

VpcId

L'ID VPC in cui è configurato il target di montaggio.

Tipo: string

Required: No

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- AWS SDK per Java V2
- SDK AWS per Ruby V3

# PosixUser

L'identità POSIX completa, inclusi l'ID utente, l'ID gruppo e gli eventuali ID di gruppo secondari, sul punto di accesso utilizzato per tutte le operazioni del file system eseguite dai client NFS che utilizzano il punto di accesso.

## Indice

Gid

ID gruppo POSIX utilizzato per tutte le operazioni del file system che utilizzano questo punto di accesso.

Tipo: long

Intervallo valido: valore minimo di 0. Valore massimo pari a 4294967295.

Campo obbligatorio: sì

Uid

ID utente POSIX utilizzato per tutte le operazioni del file system che utilizzano questo punto di accesso.

Tipo: long

Intervallo valido: valore minimo di 0. Valore massimo pari a 4294967295.

Campo obbligatorio: sì

SecondaryGids

ID gruppo POSIX secondari utilizzati per tutte le operazioni del file system che utilizzano questo punto di accesso.

Tipo: matrice di matrice lunga

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 16 elementi.

Intervallo valido: valore minimo di 0. Valore massimo pari a 4294967295.

Required: No

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- AWS SDK per Java V2
- SDK AWS per Ruby V3

# ReplicationConfigurationDescription

Descrive la configurazione di replica per un file system specifico.

## Indice

CreationTime

Descrive quando è stata creata la configurazione di replica.

Tipo: Timestamp

Campo obbligatorio: sì

Destinations

Una matrice di oggetti di destinazione. È supportato un solo oggetto di destinazione.

Tipo: matrice di oggetti Destination

Campo obbligatorio: sì

OriginalSourceFileSystemArn

Il nome della risorsa Amazon (ARN) del file system EFS originale nella configurazione di replica.

Tipo: stringa

Campo obbligatorio: sì

SourceFileSystemArn

Il nome della risorsa Amazon (ARN) del file system EFS originale nella configurazione di replica.

Tipo: stringa

Campo obbligatorio: sì

SourceFileSystemId

ID del file system Amazon EFS di origine che viene replicato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 128.

Modello: `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Campo obbligatorio: sì

SourceFileSystemRegion

Il file system EFS di origine Regione AWS in cui si trova.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 64 caratteri.

Modello: `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Campo obbligatorio: sì

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# ResourceIdPreference

Descrive il tipo di risorsa e la relativa preferenza ID per Account AWS dell'utente nel corrente Regione AWS.

## Indice

ResourceIdType

Identifica la preferenza EFS Resource ID, `LONG_ID` (17 caratteri) o `SHORT_ID` (8 caratteri).

Tipo: stringa

Valori validi: `LONG_ID | SHORT_ID`

Campo obbligatorio: no

Resources

Identifica le risorse Amazon EFS a cui si applica l'impostazione delle preferenze ID `FILE_SYSTEM` e `MOUNT_TARGET`.

Tipo: matrice di stringhe

Valori validi: `FILE_SYSTEM | MOUNT_TARGET`

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# RootDirectory

Specifica la directory del file system Amazon EFS a cui il punto di accesso fornisce l'accesso. Il punto di accesso espone il percorso del file system specificato come directory principale del file system alle applicazioni che utilizzano il punto di accesso. I client NFS che utilizzano il punto di accesso possono accedere solo ai dati contenuti nel punto di accesso `RootDirectory` e nelle relative sottodirectory.

## Indice

CreationInfo

(Facoltativo) Specifica gli ID POSIX e le autorizzazioni da applicare a `RootDirectory` del punto di accesso. Se `RootDirectory` > `Path` specificato non esiste, EFS crea la directory principale utilizzando le impostazioni `CreationInfo` quando un client si connette a un punto di accesso. Quando si specifica il `CreationInfo`, è necessario fornire valori per tutte le proprietà.

> **Important**
>
> Se non si fornisce `CreationInfo` e il parametro specificato `RootDirectory` > `Path` non esiste, i tentativi di montare il file system utilizzando il punto di accesso non riusciranno.

Tipo: oggetto CreationInfo

Campo obbligatorio: no

Path

Specifica il percorso del file system EFS da esporre come directory principale ai client NFS utilizzando il punto di accesso per accedere al file system EFS. Un percorso può avere fino a quattro sottodirectory. Se il percorso specificato non esiste, è necessario fornire il parametro `CreationInfo`.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 100.

Modello: `^(\/|(\/(?!\.)+[^$#<>;`|&?{}^*/\n]+){1,4})$`

Campo obbligatorio: no

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- SDK AWS per Java V2
- SDK AWS per Ruby V3

# Tag

Un tag è una coppia chiave-valore. I caratteri consentiti sono lettere, spazi e numeri che possono essere rappresentati in formato UTF-8, più i caratteri `+ - = . _ : /` speciali

## Indice

Key

La chiave tag (String). La chiave non può iniziare con `aws:`.

Tipo: String

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 128 caratteri.

Pattern: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Campo obbligatorio: sì

Value

Il valore della chiave del tag.

Tipo: String

Limitazioni di lunghezza: lunghezza massima di 256.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Campo obbligatorio: sì

## Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK AWS specifici della lingua, consulta quanto segue:

- SDK AWS per C++
- SDK AWS per Go
- AWS SDK per Java V2
- SDK AWS per Ruby V3

# Informazioni aggiuntive per Amazon EFS

Qui di seguito è possibile trovare alcune informazioni aggiuntive su Amazon EFS, incluse caratteristiche che sono ancora supportate ma non necessariamente consigliate.

Argomenti



## Backup dei file system Amazon EFS tramite AWS Data Pipeline

Questo argomento fornisce informazioni sull'utilizzo AWS Data Pipeline, che è una soluzione di backup e ripristino legacy per i file system EFS.

> **Note**
>
> AWS Backup è la soluzione di backup e ripristino consigliata per i file system EFS. Per ulteriori informazioni, consulta Backup dei file system di Amazon EFS.

Con AWS Data Pipeline, si crea una pipeline di dati utilizzando il AWS Data Pipeline servizio. Questa pipeline copia i dati dal file system Amazon EFS (denominato file system di produzione) a un altro file system Amazon EFS (denominato file system di backup).

AWS Data Pipeline è costituito da modelli che implementano quanto segue:

- Backup automatici basati su una pianificazione definita dall'utente (ad esempio, oraria, giornaliera, settimanale o mensile).
- Rotazione automatica dei backup, dove i backup più vecchi vengono sostituiti con il backup più recente in base al numero di backup che si desidera conservare.
- Backup più rapidi tramite rsync, che esegue solamente il backup delle modifiche apportate tra un backup e quello successivo.
- Efficienza dello storage dei backup utilizzando collegamenti fissi. Un collegamento fisso è una voce di directory che associa un nome a un file su un file system. Configurando un collegamento fisso, è possibile eseguire un ripristino completo dei dati da qualsiasi backup memorizzando solo ciò che è stato modificato tra un backup e l'altro.

Dopo aver configurato la soluzione di backup, questo tutorial guidato illustra come accedere ai backup per ripristinare i dati. Questa soluzione di backup dipende dall'esecuzione di script su GitHub cui sono ospitati ed è quindi soggetta a disponibilità. GitHub Se si desidera eliminare questa dipendenza e ospitare gli script in un bucket Amazon S3, consulta Hosting degli script rsync in un bucket Amazon S3.

> **Important**
>
> È necessario utilizzare questa soluzione nello stesso modo AWS Data Pipeline in cui Regione AWS si utilizza il file system. Poiché AWS Data Pipeline non è supportato negli Stati Uniti orientali (Ohio), questa soluzione non funziona in tale regione AWS . Se si desidera eseguire il backup del file system utilizzando questa soluzione, si consiglia di utilizzare il file system in uno degli altri file supportati Regione AWS.

Argomenti



## Prestazioni per i backup di Amazon EFS utilizzando AWS Data Pipeline

Quando si eseguono il backup e il ripristino dei dati, le prestazioni dei file system sono soggette a Prestazioni Amazon EFS, tra cui la capacità di base e quella di Burst Throughput. Il throughput utilizzato dalla soluzione di backup conta ai fini del throughput totale del file system. La tabella seguente fornisce alcuni suggerimenti sulle dimensioni del file system Amazon EFS e delle istanze Amazon EC2 adatte per questa soluzione, presupponendo che la finestra di backup sia ampia 15 minuti.

| Dimensioni EFS (Dimensione media del file 30 MB) | Volume delle modifiche giornaliere | Ore di Burst rimanenti | Numero minimo di agenti di backup |
|---|---|---|---|
| 256 GB | Meno di 25 GB | 6.75 | 1 - m3.medium |
| 512 GB | Meno di 50 GB | 7.75 | 1 - m3.large |
| 1.0 TB | Meno di 75 GB | 11.75 | 2 - m3.large* |
| 1.5 TB | Meno di 125 GB | 11.75 | 2 - m3.xlarge* |
| 2.0 TB | Meno di 175 GB | 11.75 | 3 - m3.large* |
| 3.0 TB | Meno di 250 GB | 11.75 | 4 - m3.xlarge* |

* Queste stime si basano sul presupposto che i dati archiviati in un file system EFS da 1 TB o più grande siano organizzati in modo che il backup possa essere distribuito su più nodi di backup. Lo script di esempio con nodi multipli divide il carico di backup su più nodi in base al contenuto della cartella di primo livello del file system EFS.

Ad esempio, se ci sono due nodi di backup, un nodo esegue il backup di tutti i file e le cartelle pari presenti nella cartella di primo livello. Il nodo dispari fa lo stesso per i file e le cartelle dispari. In un altro esempio, con sei cartelle nel file system Amazon EFS e quattro nodi di backup, il primo nodo esegue il backup della prima e della quinta cartella. Il secondo nodo esegue il backup della seconda e della sesta cartella e il terzo e il quarto nodo il back up della terza e della quarta cartella.

## Considerazioni sul backup di Amazon EFS con AWS Data Pipeline

Quando si decide di implementare una soluzione di backup di Amazon EFS utilizzando AWS Data Pipelineè necessario tenere in considerazione quanto segue:

- Questo approccio al backup EFS richiede una serie di AWS risorse. Per questa soluzione, è necessario creare quanto segue:

- Un file system di produzione e uno di backup che contiene una copia completa del file system di produzione. Il sistema contiene anche eventuali modifiche incrementali ai dati nel periodo di rotazione dei backup.
- Istanze Amazon EC2, i cui cicli di vita sono gestiti da AWS Data Pipeline, che eseguono ripristini e backup pianificati.
- Uno programmato regolarmente per il backup dei dati. AWS Data Pipeline
- E AWS Data Pipeline per ripristinare i backup.

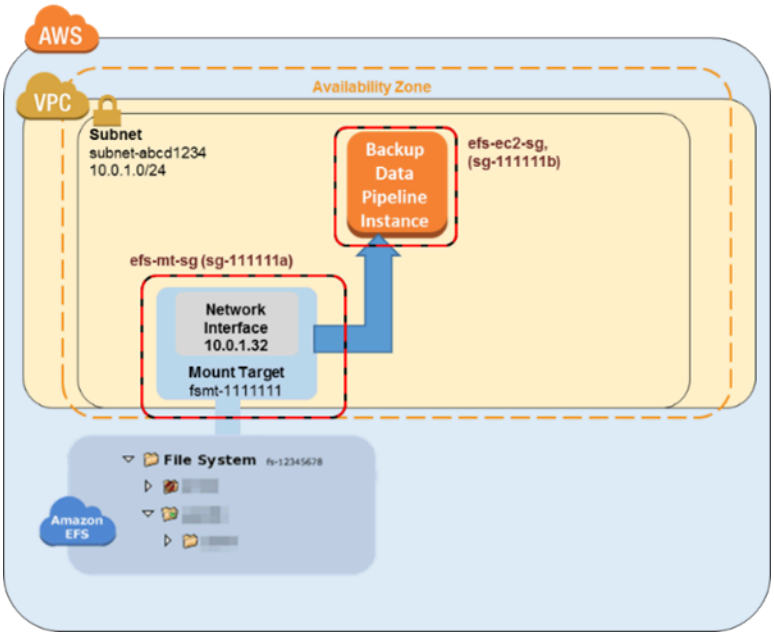
  Se questa soluzione viene implementata, questi servizi saranno fatturati sull'account. Per ulteriori informazioni, consulta le pagine con i prezzi di Amazon EFS, Amazon EC2 e AWS Data Pipeline.
- Questa soluzione non è una soluzione di backup offline. Per garantire un backup completamente coerente e completo, sospendere tutte le scritture sui file del file system o smontare il file system durante il backup. È consigliabile eseguire tutti i backup durante i tempi di inattività pianificati o le ore non di picco.

## Ipotesi per il backup di Amazon EFS con AWS Data Pipeline

Questo scenario fa alcune ipotesi e dichiara i valori di esempio come segue:

- Prima di iniziare, questo scenario presuppone che sia stata già completata Nozioni di base.
- Dopo aver completato l'esercitazione sulle nozioni di base, sono disponibili due gruppi di sicurezza, una sottorete della VPC e un target di montaggio del file system di cui si desidera eseguire il backup. Per la parte restante di questo scenario, è possibile utilizzare i seguenti valori di esempio:
  - L'ID del file system di cui si esegue il backup in questo scenario è `fs-12345678`.
  - Il gruppo di sicurezza del file system associato al target di montaggio è denominato `efs-mt-sg (sg-1111111a)`.
  - Il gruppo di sicurezza che concede alle istanze Amazon EC2 la possibilità di connettersi al target di montaggio dell'EFS di produzione è denominato `efs-ec2-sg (sg-1111111b)`.
  - La sottorete della VPC è associata all'ID `subnet-abcd1234`.
  - L'indirizzo IP del target di montaggio del file system di origine di cui si desidera eseguire il backup è `10.0.1.32:/`.
  - L'esempio presuppone che il file system di produzione sia un sistema di gestione dei contenuti che distribuisce file multimediali con una dimensione media di 30 MB.

Le precedenti ipotesi ed esempi sono riflessi nel seguente diagramma di configurazione iniziale.




# Come eseguire il backup di un file system Amazon EFS con AWS Data Pipeline

Segui le procedure in questa sezione per eseguire il backup o ripristinare il file system Amazon EFS con AWS Data Pipeline.

Argomenti

- Fase 1: Creazione del file system Amazon EFS di backup
- Passaggio 2: scarica il AWS Data Pipeline modello per i backup
- Fase 3: Creazione di una data pipeline per il backup
- Fase 4: Accesso ai backup di Amazon EFS

## Fase 1: Creazione del file system Amazon EFS di backup

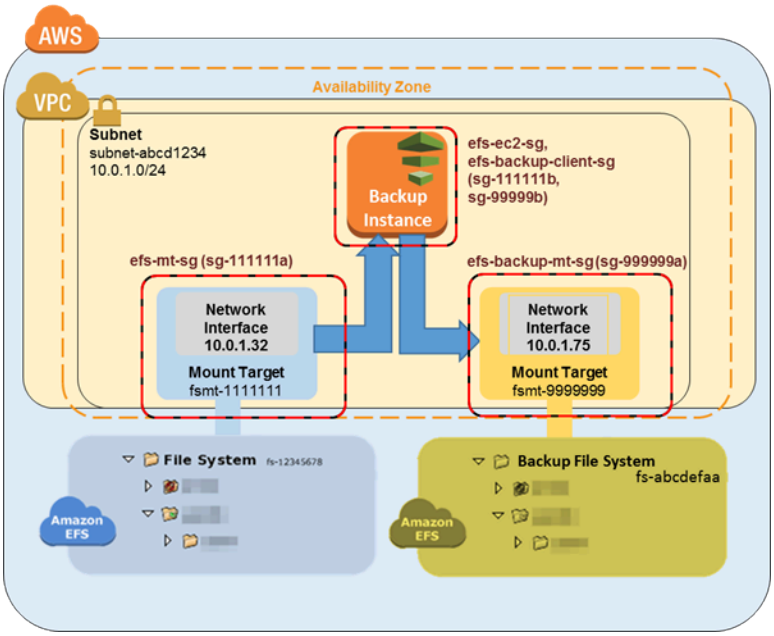
In questo scenario, è necessario creare gruppi di sicurezza, file system e target di montaggio separati per dividere i backup dall'origine dati. In questa prima fase, saranno create tali risorse:

1. Prima di tutto, crea due nuovi gruppi di sicurezza. Il gruppo di sicurezza di esempio per il target di montaggio di backup è `efs-backup-mt-sg (sg-9999999a)`. Il gruppo di sicurezza di esempio per l'istanza EC2 da cui accedere al target di montaggio è `efs-backup-ec2-sg (sg-9999999b)`. Ricordati di creare questi gruppi di sicurezza nella stessa VPC del volume EFS

di cui si desidera eseguire il backup. In questo esempio, la VPC associato alla sottorete `subnet-abcd1234`. Per ulteriori informazioni sulla creazione dei gruppi di sicurezza, consulta Creazione dei gruppi di sicurezza.

2. Quindi, crea un backup del file system Amazon EFS. In questo esempio l'ID del file system è `fs-abcdefaa`. Per ulteriori informazioni sulla creazione dei file system, consulta Creazione di file system Amazon EFS.
3. Infine, crea un punto di montaggio per il file system EFS di backup e ipotizza che assuma il valore di `10.0.1.75:/`. Per ulteriori informazioni sulla creazione di target di montaggio, consulta Creazione e gestione di target di montaggio e gruppi di sicurezza.

Dopo aver completato questo primo passo, la configurazione dovrebbe essere simile al diagramma di esempio seguente.




## Passaggio 2: scarica il AWS Data Pipeline modello per i backup

AWS Data Pipeline ti aiuta a elaborare e spostare i dati in modo affidabile tra diversi servizi di AWS elaborazione e storage a intervalli specifici. Utilizzando la AWS Data Pipeline console, è possibile creare definizioni di pipeline preconfigurate, note come modelli. Puoi utilizzare questi modelli per iniziare rapidamente. AWS Data Pipeline Per questo scenario, è fornito un modello per rendere più semplice il processo di configurazione delle pipeline di backup.

Quando implementato, questo modello consente di creare una data pipeline che avvia una singola istanza Amazon EC2 nel momento specificato per eseguire il backup dei dati dal file system di

produzione a quello di backup. Questo modello dispone di un certo numero di valori segnaposto. Fornisci i valori corrispondenti per quei segnaposto nella sezione Parametri della AWS Data Pipeline console. Scarica il AWS Data Pipeline modello per i backup su BackupDataPipeline1-Node-EFS .json da. GitHub

> **Note**
>
> Questo modello fa inoltre riferimento ed esegue uno script per l'esecuzione dei comandi di backup. È possibile scaricare lo script prima di creare la pipeline per rivedere le operazioni eseguite. Per rivedere lo script, scarica efs-backup.sh da. GitHub Questa soluzione di backup dipende dall'esecuzione di script ospitati su GitHub ed è soggetta a GitHub disponibilità. Se si desidera eliminare questa dipendenza e ospitare gli script in un bucket Amazon S3, consulta Hosting degli script rsync in un bucket Amazon S3.

## Fase 3: Creazione di una data pipeline per il backup

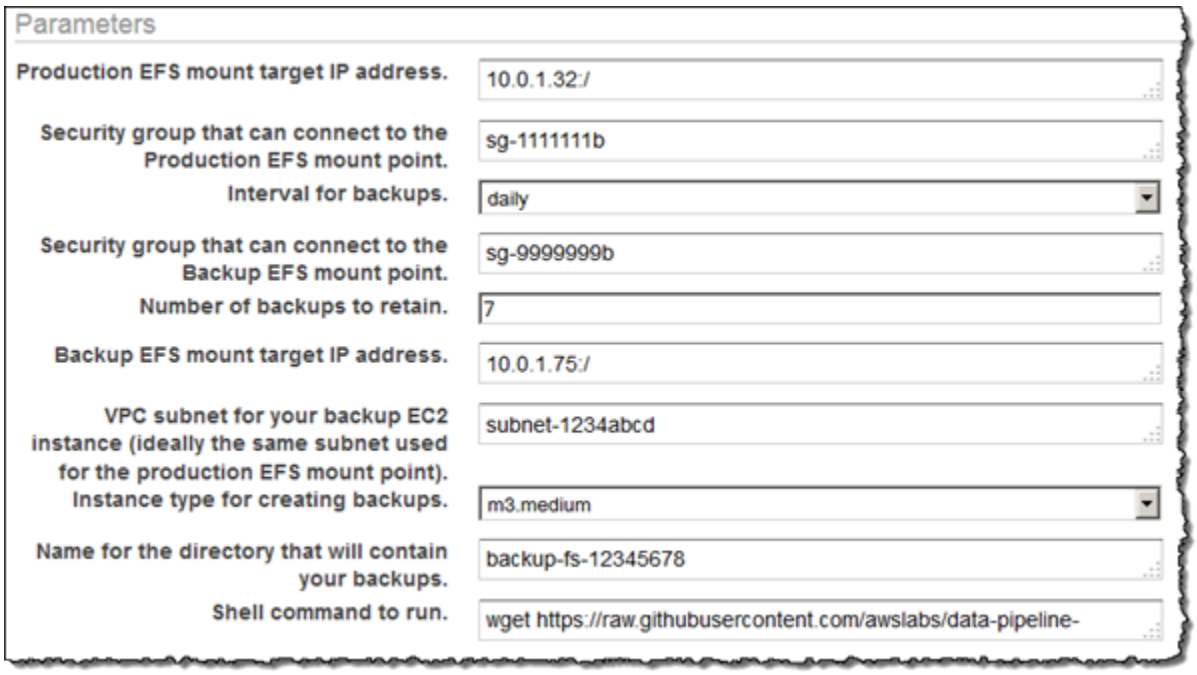
Utilizza la procedura seguente per creare la data pipeline.

Creazione di una data pipeline per i backup di Amazon EFS

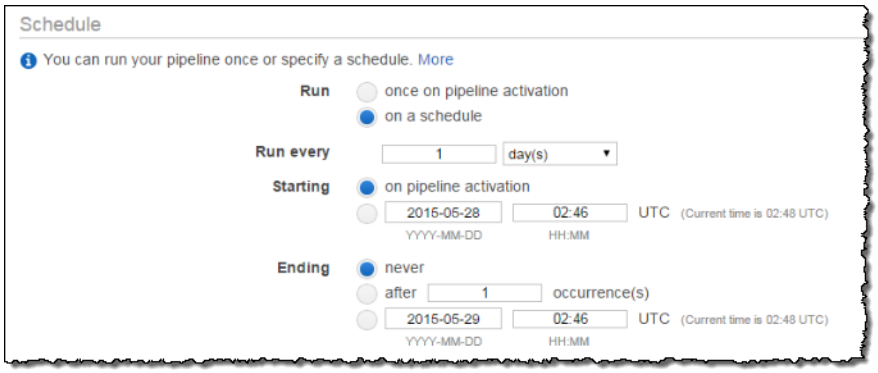
1. Apri la AWS Data Pipeline console all'indirizzo https://console.aws.amazon.com/datapipeline/.

   > **Important**
   >
   > Assicurati di lavorare nello stesso modo in cui lavori con Regione AWS i tuoi file system Amazon EFS.

2. Scegli Crea nuova pipeline.
3. Aggiungi i valori per Nome e una descrizione facoltativa in Descrizione.
4. Per Origine scegli Importa una definizione e scegli Carica file locale.
5. Nel file explorer, naviga fino al modello salvato in Passaggio 2: scarica il AWS Data Pipeline modello per i backup e quindi scegli Apri.
6. In Parametri, aggiungi i dettagli dei file system EFS di backup e di produzione.




7. Configura le opzioni in Pianifica per definire la pianificazione del backup di Amazon EFS. Il backup dell'esempio viene eseguito una volta ogni giorno e i backup vengono conservati per una settimana. Quando un backup è più vecchio di sette giorni, viene sostituito con il backup successivo.




> **Note**
>
> È consigliabile specificare l'avvio dell'esecuzione durante un orario non di picco.

8. (Facoltativo) Specificare una posizione Amazon S3 per registrare log della pipeline, configurare un ruolo IAM personalizzato o aggiungere dei tag per descrivere la pipeline.
9. Quando la pipeline è configurata, scegli Attiva.

A questo punto la data pipeline Amazon EFS è configurata e attivata. Per ulteriori informazioni in merito AWS Data Pipeline, consulta la AWS Data Pipeline Developer Guide. A questo punto, è possibile eseguire immediatamente il backup di test, oppure attendere che il backup venga eseguito all'ora pianificata.

## Fase 4: Accesso ai backup di Amazon EFS

Il backup di Amazon EFS è stato ora creato, attivato ed è in esecuzione con la programmazione definita. Questa fase illustra come accedere ai backup di EFS. I backup sono memorizzati nel file system EFS di backup precedentemente creato nel formato seguente.

```
backup-efs-mount-target:/efs-backup-id/[backup interval].[0-backup retention]-->
```

Utilizzando i valori dello scenario di esempio, il backup dei file system si trova in `10.1.0.75:/fs-12345678/daily.[0-6]`, dove `daily.0` è il backup più recente e `daily.6` è il più vecchio dei sette backup a rotazione.

L'accesso ai backup offre la possibilità di ripristinare i dati del file system di produzione. È possibile scegliere di ripristinare un intero file system, oppure è possibile scegliere di ripristinare dei singoli file.

### Fase 4.1: Ripristino di un intero backup Amazon EFS

Il ripristino di una copia di backup di un file system Amazon EFS richiede un'altra copia AWS Data Pipeline, simile a quella in Fase 3: Creazione di una data pipeline per il backup cui hai configurato. Tuttavia, la pipeline di ripristino funziona in senso inverso rispetto alla pipeline di backup. Di solito, questi ripristini non sono programmati per avviarsi automaticamente.

Come per i backup, i ripristini possono essere effettuati in parallelo per rispettare i tempi di ripristino. Ricorda che al momento della creazione di una data pipeline, è necessario pianificare il momento nel quale la si desidera mandare in esecuzione. Scegliendo di eseguirla all'attivazione, si fa partire immediatamente il processo di ripristino. È consigliabile creare una pipeline di ripristino solo quando è necessario eseguire un ripristino, oppure quando si ha già chiaro in mente uno specifico intervallo di tempo.

La capacità di burst è consumata sia dall'EFS di backup che da quello di ripristino. Per ulteriori informazioni sulle prestazioni, consultare Prestazioni Amazon EFS. La seguente procedura mostra come creare e implementare la pipeline di ripristino.

Per creare una data pipeline per il ripristino di EFS

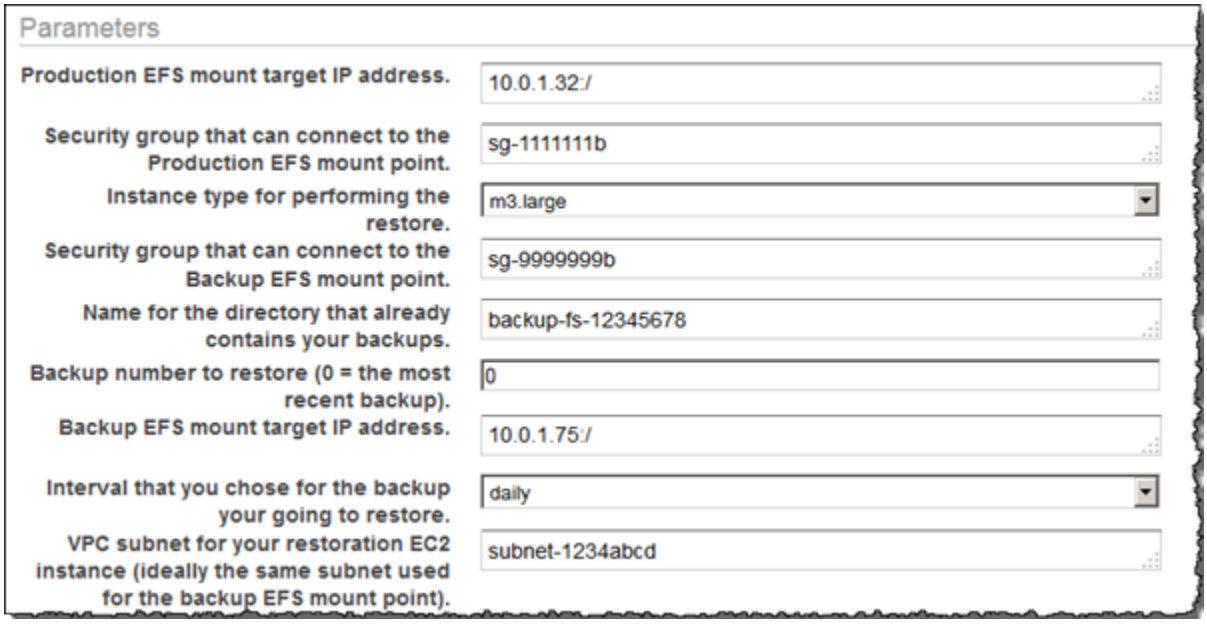
1. Scaricare il modello di data pipeline per il ripristino dei dati dal file system EFS di backup. Questo modello avvia una singola istanza Amazon EC2 in base alla dimensione specificata. Si avvia solo quando l'utente ne indica l'avvio. Scarica il AWS Data Pipeline modello per i backup su RestoreDataPipeline1-Node-EFS .json da. GitHub

   > **Note**
   >
   > Questo modello fa inoltre riferimento ed esegue uno script per l'esecuzione dei comandi di ripristino. È possibile scaricare lo script prima di creare la pipeline per rivedere le operazioni eseguite. Per rivedere lo script, scarica efs-restore.sh da. GitHub

2. Apri la AWS Data Pipeline console all'indirizzo https://console.aws.amazon.com/datapipeline/.

   > **Important**
   >
   > Assicurati di lavorare nello stesso Regione AWS modo dei tuoi file system Amazon EFS e Amazon EC2.

3. Scegli Crea nuova pipeline.
4. Aggiungi i valori per Nome e una descrizione facoltativa in Descrizione.
5. Per Origine scegli Importa una definizione e scegli Carica file locale.
6. Nel file explorer, naviga fino al modello salvato in Fase 1: Creazione del file system Amazon EFS di backup e quindi scegli Apri.
7. In Parametri, aggiungi i dettagli dei file system EFS di backup e di produzione.




8. Poiché i ripristini di solito vengono eseguiti solo quando sono necessari, è possibile programmare il ripristino affinché sia eseguito once on pipeline activation (una volta all'attivazione della pipeline). Oppure è possibile pianificare un ripristino in un istante futuro a scelta, ad esempio durante una finestra temporale in un orario non di picco.
9. (Facoltativo) Specificare una posizione Amazon S3 per registrare log della pipeline, configurare un ruolo IAM personalizzato o aggiungere dei tag per descrivere la pipeline.
10. Quando la pipeline è configurata, scegli Attiva.

A questo punto la data pipeline Amazon EFS di ripristino è configurata e attivata. Ora, quando è necessario ripristinare un backup sul file system EFS di produzione, è sufficiente attivarlo dalla AWS Data Pipeline console. Per ulteriori informazioni, consulta la Guida per gli sviluppatori di AWS Data Pipeline .

Fase 4.2: Ripristino di singoli file dai backup di Amazon EFS

È possibile ripristinare i file dai backup del file system Amazon EFS avviando un'istanza Amazon EC2 per montare temporaneamente i file system EFS di produzione e di backup. L'istanza EC2 deve essere membro di entrambi i gruppi di sicurezza dei client EFS (in questo esempio, efs-ec2-sg e). efs-backup-clients-sg Entrambi i target di montaggio EFS possono essere montati da questa istanza di ripristino. Ad esempio, un'istanza EC2 di ripristino può creare i seguenti punti di montaggio. Qui viene usata l'opzione `-o ro` per montare l'EFS di backup in modalità di sola lettura per evitare modifiche accidentali al backup durante il tentativo di ripristino dallo stesso.

```
mount -t nfs source-efs-mount-target:/ /mnt/data
```

```
mount -t nfs -o ro backup-efs-mount-target:/fs-12345678/daily.0 /mnt/backup>
```

Dopo aver montato le destinazioni, è possibile copiare i file da `/mnt/backup` al percorso appropriato in `/mnt/data` nel terminale utilizzando il comando `cp -p`. Ad esempio, un'intera home directory (con le autorizzazioni associate al file system) può essere copiata ricorsivamente con il comando seguente.

```
sudo cp -rp /mnt/backup/users/my_home /mnt/data/users/my_home
```

È possibile ripristinare un singolo file eseguendo il seguente comando.

```
sudo cp -p /mnt/backup/user/my_home/.profile /mnt/data/users/my_home/.profile
```

> **Warning**
>
> Quando si ripristinano manualmente singoli file di dati, fare attenzione a non modificare accidentalmente il backup stesso. In caso contrario, questo potrebbe risultare danneggiato.

## Risorse aggiuntive di backup

La soluzione di backup presentata in questa procedura dettagliata utilizza modelli per. AWS Data Pipeline I modelli utilizzati in Passaggio 2: scarica il AWS Data Pipeline modello per i backup e Fase 4.1: Ripristino di un intero backup Amazon EFS utilizzano entrambi una singola istanza Amazon EC2 per eseguire il loro lavoro. Tuttavia, non esiste alcun vero limite al numero istanze parallele che è possibile eseguire per il backup o il ripristino dei dati nei file system Amazon EFS. In questo argomento, puoi trovare collegamenti ad altri AWS Data Pipeline modelli configurati per più istanze EC2 che puoi scaricare e utilizzare per la tua soluzione di backup. È inoltre possibile trovare istruzioni su come modificare i modelli al fine di includere istanze aggiuntive.

Argomenti

- Utilizzo di modelli aggiuntivi
- Aggiunta di istanze backup aggiuntive
- Aggiunta di istanze di ripristino aggiuntive

- Hosting degli script rsync in un bucket Amazon S3

## Utilizzo di modelli aggiuntivi

Puoi scaricare i seguenti modelli aggiuntivi da: GitHub

- 2-node-EFS BackupPipeline .json: questo modello avvia due istanze Amazon EC2 parallele per eseguire il backup del file system Amazon EFS di produzione.
- 2-node-EFS RestorePipeline .json: questo modello avvia due istanze Amazon EC2 parallele per ripristinare un backup del file system Amazon EFS di produzione.

## Aggiunta di istanze backup aggiuntive

È possibile aggiungere nodi aggiuntivi ai modelli di backup utilizzati in questo scenario. Per aggiungere un nodo, modificare la seguente sezione del modello `2-Node-EFSBackupDataPipeline.json`.

> **Important**
>
> Se si stanno utilizzando nodi aggiuntivi, non è possibile utilizzare spazi nei nomi di file e cartelle memorizzati nella directory di livello superiore. In caso contrario, i file e le cartelle non sono sottoposti a backup né ripristinati. Tutti i file e le sottocartelle che si trovano almeno un livello sotto il livello superiore vengono sottoposti a backup e ripristino come previsto.

- Creare un'ulteriore risorsa EC2 per ogni nodo aggiuntivo che si desidera creare (in questo esempio, una quarta istanza EC2).

```
{
"id": "EC2Resource4",
"terminateAfter": "70 Minutes",
"instanceType": "#{myInstanceType}",
"name": "EC2Resource4",
"type": "Ec2Resource",
"securityGroupIds" : [ "#{mySrcSecGroupID}","#{myBackupSecGroupID}" ],
"subnetId": "#{mySubnetID}",
"associatePublicIpAddress": "true"
},
```

- Creare un'operazione di data pipeline aggiuntiva per ogni nodo aggiuntivo (in questo caso, attività `BackupPart4`), assicurarsi di configurare le seguenti sezioni:
  - Aggiornare il riferimento `runs0n` alla risorsa EC2 precedentemente creata (in questo esempio `EC2Resource4`).
  - Incrementare gli ultimi due valori di `scriptArgument` affinché siano pari alla porzione di backup di cui ogni nodo è responsabile e al numero totale di nodi. Per `"2"` e `"3"` nel seguente esempio, la porzione di backup è `"3"` per il quarto nodo perché in questo esempio la logica di calcolo richiede di iniziare il conteggio a partire da 0.

```
{
"id": "BackupPart4",
"name": "BackupPart4",
"runsOn": {
"ref": "EC2Resource4"
},
"command": "wget https://raw.githubusercontent.com/awslabs/data-pipeline-samples/
master/samples/EFSBackup/efs-backup-rsync.sh\nchmod a+x efs-backup-rsync.sh\n./efs-
backup-rsync.sh $1 $2 $3 $4 $5 $6 $7",
"scriptArgument": ["#{myEfsSource}","#{myEfsBackup}", "#{myInterval}",
 "#{myRetainedBackups}","#{myEfsID}", "3", "4"],
"type": "ShellCommandActivity",
"dependsOn": {
"ref": "InitBackup"
},
"stage": "true"
},
```

- Incrementare l'ultimo valore in tutti i valori di `scriptArgument` esistenti al numero di nodi (in questo esempio `"4"`).

```
{
"id": "BackupPart1",
...
"scriptArgument": ["#{myEfsSource}","#{myEfsBackup}", "#{myInterval}",
 "#{myRetainedBackups}","#{myEfsID}", "1", "4"],
...
},
{
"id": "BackupPart2",
...
```

```
"scriptArgument": ["#{myEfsSource}","#{myEfsBackup}", "#{myInterval}",
 "#{myRetainedBackups}","#{myEfsID}", "2", "4"],
...
},
{
"id": "BackupPart3",
...
"scriptArgument": ["#{myEfsSource}","#{myEfsBackup}", "#{myInterval}",
 "#{myRetainedBackups}","#{myEfsID}", "0", "4"],
...
},
```

- Aggiornare l'attività `FinalizeBackup` e aggiungere la nuova operazione di backup all'elenco `dependsOn` (in questo caso `BackupPart4`).

```
{
"id": "FinalizeBackup", "name": "FinalizeBackup", "runsOn": { "ref":
"EC2Resource1" }, "command": "wget
https://raw.githubusercontent.com/awslabs/data-pipeline-samples/master/samples/
EFSBackup/efs-backup-end.sh\nchmod a+x
efs-backup-end.sh\n./efs-backup-end.sh $1 $2", "scriptArgument": ["#{myInterval}",
"#{myEfsID}"], "type": "ShellCommandActivity", "dependsOn": [ { "ref":
 "BackupPart1" },
{ "ref": "BackupPart2" }, { "ref": "BackupPart3" }, { "ref": "BackupPart4" } ],
 "stage":
"true"
```

## Aggiunta di istanze di ripristino aggiuntive

È possibile aggiungere nodi ai modelli di ripristino utilizzati in questo scenario. Per aggiungere un nodo, modificare la seguente sezione del modello `2-Node-EFSRestorePipeline.json`.

- Creare un'ulteriore risorsa EC2 per ogni nodo aggiuntivo che si desidera creare (in questo caso, una terza istanza EC2 chiamata `EC2Resource3`).

```
{
"id": "EC2Resource3",
"terminateAfter": "70 Minutes",
"instanceType": "#{myInstanceType}",
"name": "EC2Resource3",
"type": "Ec2Resource",
```

```
"securityGroupIds" : [ "#{mySrcSecGroupID}","#{myBackupSecGroupID}" ],
"subnetId": "#{mySubnetID}",
"associatePublicIpAddress": "true"
},
```

- Creare un'operazione di data pipeline aggiuntiva per ogni nodo aggiuntivo (in questo caso, attività `RestorePart3`). Assicurarsi di configurare le seguenti sezioni:
  - Aggiornare il riferimento `runsOn` affinché punti alla `EC2Resource` precedentemente creata (in questo esempio `EC2Resource3`).
  - Incrementare gli ultimi due valori di `scriptArgument` affinché siano pari alla porzione di backup di cui ogni nodo è responsabile e al numero totale di nodi. Per `"2"` e `"3"` nel seguente esempio, la porzione di backup è `"3"` per il quarto nodo perché in questo esempio la logica di calcolo richiede di iniziare il conteggio a partire da 0.

```
{
"id": "RestorePart3",
"name": "RestorePart3",
"runsOn": {
"ref": "EC2Resource3"
},
"command": "wget https://raw.githubusercontent.com/awslabs/data-pipeline-samples/
master/samples/EFSBackup/efs-restore-rsync.sh\nchmod a+x efs-restore-rsync.sh\n./efs-
backup-rsync.sh $1 $2 $3 $4 $5 $6 $7",
"scriptArgument": ["#{myEfsSource}","#{myEfsBackup}", "#{myInterval}",
 "#{myBackup}","#{myEfsID}", "2", "3"],
"type": "ShellCommandActivity",
"dependsOn": {
"ref": "InitBackup"
},
"stage": "true"
},
```

- Incrementare l'ultimo valore in tutti i valori di `scriptArgument` esistenti al numero di nodi (in questo esempio `"3"`).

```
{
"id": "RestorePart1",
...
"scriptArgument": ["#{myEfsSource}","#{myEfsBackup}", "#{myInterval}",
 "#{myBackup}","#{myEfsID}", "1", "3"],
...
```

```
},
{
"id": "RestorePart2",
...
"scriptArgument": ["#{myEfsSource}","#{myEfsBackup}", "#{myInterval}",
 "#{myBackup}","#{myEfsID}", "0", "3"],
...
},
```

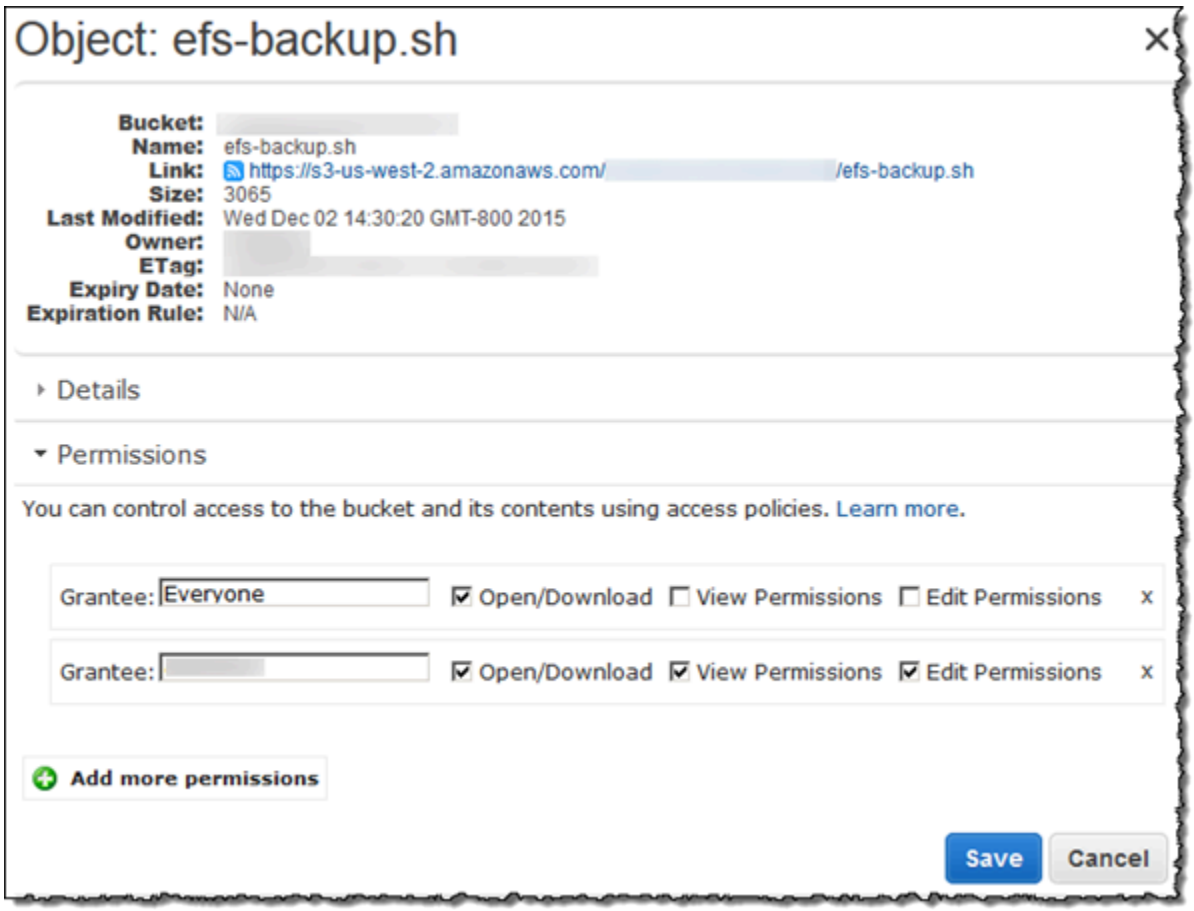
## Hosting degli script rsync in un bucket Amazon S3

Questa soluzione di backup dipende dall'esecuzione di script rsync ospitati in un repository su Internet. GitHub Pertanto, questa soluzione di backup è soggetta alla disponibilità del GitHub repository. Questo requisito significa che se il GitHub repository rimuove questi script o se il GitHub sito web va offline, la soluzione di backup implementata in precedenza non funziona.

Se preferisci eliminare questa GitHub dipendenza, puoi scegliere di ospitare gli script in un bucket Amazon S3 di tua proprietà. Qui di seguito, è possibile scoprire i passaggi necessari per l'hosting degli script in proprio.

### Attivazione dell'hosting degli script rsync in un bucket Amazon S3

1. Registrati AWS e crea un utente amministrativo: se ne hai già uno Account AWS, vai avanti e passa al passaggio successivo. In caso contrario, consulta Configurazione.
2. Crea un bucket Amazon S3 - Se disponi già di un bucket sul quale desideri ospitare lo script rsync, procedi e passa al passaggio successivo. Per le istruzioni, consulta Crea un bucket nella Guida per l'utente di Amazon Simple Storage Service.
3. Scarica gli script e i modelli di rsync: scarica tutti gli script e i modelli rsync nella cartella EFSBackup da. GitHub Annota il percorso sul computer in cui sono stati scaricati questi file.
4. Carica gli script rsync sul bucket S3 - Per istruzioni su come caricare oggetti nel bucket S3, consulta Aggiunta di un oggetto a un bucket nella Guida per l'utente di Amazon Simple Storage Service.
5. Modifica le autorizzazioni per gli script rsync caricati per consentire a Tutti di eseguire su di essi le operazioni Apri/Scarica. Per istruzioni su come modificare le autorizzazioni su un oggetto nel bucket S3, consulta Modifica delle autorizzazioni sugli oggetti nella Guida per l'utente di Amazon Simple Storage Service.




6. Aggiorna i modelli - Modifica l'istruzione `wget` nel parametro `shellCmd` in modo che punti al bucket Amazon S3 dove è stato posizionato lo script di avvio. Salva il modello aggiornato e utilizza tale modello durante la seguente procedura in [Fase 3: Creazione di una data pipeline per il backup](#).

> **Note**
>
> Ti consigliamo di limitare l'accesso al tuo bucket Amazon S3 per includere l'account IAM che attiva la soluzione di backup AWS Data Pipeline per questa soluzione. Per ulteriori informazioni, consulta [Modifica delle autorizzazioni dei bucket](#) nella Guida per l'utente di Amazon Simple Storage Service.

Ora stai ospitando gli script rsync per questa soluzione di backup e i tuoi backup non dipendono più dalla disponibilità. GitHub

# Montaggio dei file system senza l'assistente per il montaggio di EFS

> **Note**
>
> In questa sezione, puoi imparare a montare il tuo file system Amazon EFS senza il amazon-efs-utils pacchetto. Per utilizzare la crittografia dei dati in transito con i propri file system, è necessario montare il file system con Transport Layer Security (TLS). A tale scopo, consigliamo di utilizzare il amazon-efs-utils pacchetto. Per ulteriori informazioni, consulta Utilizzo degli amazon-efs-utils strumenti.

Qui di seguito, è possibile imparare a installare il client NFS (Network File System) e a montare il file system Amazon EFS su un'istanza Amazon EC2. È inoltre possibile trovare una spiegazione del comando `mount` e le opzioni disponibili per la specifica del nome DNS (Domain Name System) del file system nel comando `mount`. Inoltre, è possibile scoprire come utilizzare il file `fstab` per rimontare automaticamente il file system dopo un riavvio del sistema.

> **Note**
>
> Prima di installare un file system, è necessario creare, configurare e avviare le risorse AWS correlate. Per istruzioni dettagliate, vedi Guida introduttiva ad Amazon Elastic File System.

> **Note**
>
> Prima di montare il file system, devi creare gruppi di sicurezza VPC per le tue istanze Amazon EC2 e montare destinazioni con l'accesso in entrata e in uscita richiesto. Per ulteriori informazioni, consulta Utilizzo di gruppi di sicurezza VPC per istanze Amazon EC2 e destinazioni di montaggio.

Argomenti

- Montaggio su Amazon EC2 con un nome DNS
- Montaggio con un indirizzo IP

## Supporto per NFS

Amazon EFS supporta Network File System 4.0 e 4.1 (NFSv4) e i protocolli NFSv4.0 quando il file system viene montato su istanze Amazon EC2. Anche se NFSv4.0 è supportato, si consiglia di usare NFSv4.1. Il montaggio del file system Amazon EFS sull'istanza Amazon EC2 richiede anche un client NFS che supporta il protocollo NFSv4 scelto. Le istanze Amazon EC2 Mac che eseguono macOS Big Sur supportano solo NFS v4.0.

Amazon EFS non supporta l'opzione `nconnect` di montaggio.

> **Note**
>
> A partire dalle versioni del kernel Linux 5.4.*, il client Linux NFS utilizza un valore `read_ahead_kb` predefinito di 128 KB. Si consiglia di aumentare questo valore a 15 MB. Per ulteriori informazioni, consulta Ottimizzazione della dimensione read_ahead_kb di NFS.

Per ottenere prestazioni ottimali e per evitare un'ampia gamma di noti bug dei client NFS, consigliamo di lavorare con un kernel Linux recente. Se si sta utilizzando una distribuzione Linux enterprise, consigliamo di attenersi alle seguenti indicazioni:

- Amazon Linux 2
- Amazon Linux 2017.09 o versioni successive
- Red Hat Enterprise Linux (e derivati come CentOS) versione 7 e successive
- Ubuntu 16.04 LTS e versioni più recenti
- SLES 12 Sp2 o versioni successive

Se si sta usando un'altra distribuzione o un kernel personalizzato, consigliamo un kernel versione 4.3 o più recente.

> **Note**
>
> RHEL 6.9 potrebbe non essere una scelta ottimale per determinati carichi di lavoro a causa di Prestazioni scadenti durante l'apertura di svariati file in parallelo.

> **Note**
>
> Il montaggio di file system Amazon EFS con istanze Amazon EC2 che eseguono Microsoft Windows non è supportato.

### Risoluzione dei problemi con versioni di AMI e kernel

Per risolvere i problemi correlati a specifiche versioni di AMI o kernel durante l'utilizzo di Amazon EFS da un'istanza EC2, consulta Risoluzione dei problemi di AMI e kernel.

## Installazione del client NFS

Per montare il file system Amazon EFS sull'istanza Amazon EC2, è necessario prima installare un client NFS. Per collegarsi all'istanza EC2 e installare un client NFS, è necessario disporre del nome pubblico su DNS dell'istanza EC2 e di un nome utente per accedere. Il nome utente per l'istanza è generalmente `ec2-user`.

Per connettersi all'istanza EC2 e installare il client NFS

1. Connettiti all'istanza EC2. Tenere nota dei seguenti punti sulla connessione all'istanza:

   - Per connettersi all'istanza da un computer che esegue Mac OS o Linux, è necessario specificare il file .pem nel client SSH con l'opzione `-i` e il percorso della chiave privata.
   - Per connetterti alla tua istanza da un computer che esegue Windows, puoi usare uno dei due MindTerm o PuTTY. Se si prevede di usare PuTTY, è necessario installarlo e usare la procedura seguente per convertire il file .pem in un file .ppk.

   Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per l'utente Amazon EC2 per le istanze Linux:

   - Connessione all'istanza Linux da Windows tramite PuTTY

- Connessione all'istanza Linux tramite SSH

  Il file della chiave non può essere pubblicamente visibile per SSH. Per impostare le autorizzazioni, è possibile utilizzare il comando chmod 400 ***filename***.pem. Per ulteriori informazioni, consulta Creazione di una coppia di chiavi.

2. (Facoltativo) Scaricare gli aggiornamenti e riavviare.

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

3. Riconnettersi all'istanza EC2 dopo averla riavviata.
4. Installare il client NFS.

   Se si sta utilizzando un'AMI Amazon Linux o Red Hat Linux, installare il client NFS con il seguente comando.

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

   Se si sta usando un'AMI Ubuntu Amazon EC2 installare il client NFS con il comando seguente.

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

5. Avviare il servizio NFS utilizzando il comando seguente. Per RHEL 7:

```
$ sudo service nfs start
```

   Per RHEL 8:

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

6. Verificare che il servizio NFS sia stato avviato, come indicato di seguito.

```
$ 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
```

Se si utilizza un kernel personalizzato (e si crea quindi un'AMI personalizzata), è necessario includere almeno il modulo client kernel NFSv4.1 client e il corretto assistente per il montaggio NFS4.

> **Note**
>
> Scegliendo Amazon Linux AMI 2016.03.0 o Amazon Linux AMI 2016.09.0 all'avvio dell'istanza Amazon EC2, non è necessario installare `nfs-utils` perché il pacchetto è già incluso per default nell'AMI.

Passaggio successivo: montaggio del file system

Utilizza una delle procedure riportate qui di seguito per montare il file system.

- Montaggio su Amazon EC2 con un nome DNS
- Montaggio con un indirizzo IP
- Montaggio automatico del file system Amazon EFS

## Opzioni di montaggio NFS consigliate

Consigliamo i seguenti valori predefiniti per le opzioni di montaggio su Linux:

- `noresvport`: indica al client NFS di usare una nuova porta TCP (Transmission Control Protocol) di origine quando la connessione di rete viene ripristinata. Il software client NFS incluso nelle versioni precedenti del kernel Linux (versioni v5.4 e precedenti) include un comportamento che fa sì che i client NFS, dopo la disconnessione, tentino di riconnettersi sulla stessa porta sorgente TCP. Questo comportamento non è conforme al TCP RFC e può impedire a questi client di ristabilire rapidamente le connessioni a un file system EFS.

  L'uso dell'opzione `noresvport` aiuta a garantire che i client NFS si riconnettano in modo trasparente al file system EFS, mantenendo una disponibilità ininterrotta durante la riconnessione dopo un evento di ripristino della rete.

> **Important**
>
> Si consiglia vivamente di utilizzare l'opzione `noresvport` di montaggio per garantire che il file system EFS abbia una disponibilità ininterrotta dopo una riconnessione o un evento di ripristino della rete.
> Considera l'utilizzo dell'helper di montaggio EFS per montare i file system. L'helper di montaggio EFS utilizza opzioni di montaggio NFS ottimizzate per i file system Amazon EFS.

- `rsize=1048576`: imposta il numero massimo di byte di dati che il client NFS è in grado di ricevere per ogni richiesta READ della rete. Questo valore si applica per la lettura dei dati da un file in un file system EFS. È consigliabile utilizzare la dimensione massima possibile (fino a `1048576`) per evitare una riduzione delle prestazioni.
- `wsize=1048576`: imposta il numero massimo di byte di dati che il client NFS è in grado di inviare per ogni richiesta WRITE della rete. Questo valore si applica per la scrittura dei dati in un file in un file system EFS. È consigliabile utilizzare la dimensione massima possibile (fino a `1048576`) per evitare una riduzione delle prestazioni.
- `hard`: imposta il comportamento di ripristino del client NFS dopo il timeout di una richiesta NFS, in modo che la richiesta NFS venga ritentata a tempo indeterminato fino alla risposta del server. È consigliabile utilizzare l'opzione di montaggio hard (`hard`) per garantire l'integrità dei dati. Se utilizzi un mofintaggio `soft`, imposta il parametro `timeo` su almeno `150` decisecondi (15 secondi). In questo modo consenti di ridurre al minimo il rischio di danneggiamento dei dati che è insito nei montaggi soft.
- `timeo=600`: imposta il valore di timeout utilizzato dal client NFS in attesa di una risposta prima di ripetere la richiesta NFS su 600 decisecondi (60 secondi). Se è necessario modificare il parametro timeout (`timeo`), si consiglia di utilizzare un valore di almeno `150`, che è pari a 15 secondi. In questo modo è possibile evitare una riduzione delle prestazioni.
- `retrans=2`: imposta su 2 il numero di volte che il client NFS ritenta una richiesta prima di eseguire un'altra operazione di ripristino.
- `_netdev`: se presente in `/etc/fstab` impedisce al client di tentare di montare il file system EFS fino a quando la rete non è stata abilitata.
- `nofail`: se l'istanza EC2 deve avviarsi indipendentemente dallo stato del montaggio del file system EFS, aggiungere l'opzione `nofail` alla voce del file system nel file `/etc/fstab`.

Se non usi i valori predefiniti precedenti, tieni presente quanto segue:

- In generale, evita di impostare opzioni di montaggio diverse dai valori predefiniti in quanto possono causare una riduzione delle prestazioni e altri problemi. Ad esempio, la modifica della dimensione dei buffer di lettura o scrittura o la disabilitazione del caching degli attributi possono ridurre le prestazioni.
- Amazon EFS ignora le porte di origine. La modifica delle porte di origine di Amazon EFS non ha alcun effetto.
- Amazon EFS non supporta l'opzione `nconnect` di montaggio.
- Amazon EFS non supporta nessuna delle varianti di sicurezza di Kerberos. Ad esempio, il seguente comando di montaggio non ha esito positivo.

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

- È consigliabile montare il file system utilizzando il nome DNS. Questo nome risolve l'indirizzo IP del target del montaggio Amazon EFS nella stessa zona di disponibilità dell'istanza Amazon EC2. Se utilizzi un target di montaggio in una zona di disponibilità diversa da quella dell'istanza Amazon EC2 incorri nei costi EC2 standard per i dati inviati nelle zone di disponibilità. Potresti anche osservare un aumento delle latenze per le operazioni del file system.
- Per ulteriori opzioni di montaggio e una spiegazione dettagliata delle impostazioni predefinite, consulta le pagine `man fstab` e `man nfs` della documentazione di Linux.

## Montaggio su Amazon EC2 con un nome DNS

> **Note**
>
> Prima di montare il file system, devi aggiungere una regola al gruppo di sicurezza di target di montaggio che consenta l'accesso NFS in entrata dal gruppo di sicurezza EC2. Per ulteriori informazioni, consulta Utilizzo di gruppi di sicurezza VPC per istanze Amazon EC2 e destinazioni di montaggio.

- Nome DNS del file system - L'opzione di montaggio più semplice prevede l'utilizzo del nome DNS del file system. Il nome DNS del file system viene risolto automaticamente nell'indirizzo IP del target di montaggio nella zona di disponibilità dell'istanza Amazon EC2 che vi si connette. È

possibile ottenere questo nome DNS dalla console, oppure, se si dispone dell'ID del file system, è possibile costruirlo usando la seguente convenzione.

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

> **Note**
>
> La risoluzione DNS per i nomi DNS del file system richiede che il file system Amazon EFS disponga di un target di montaggio nella stessa zona di disponibilità dell'istanza client.

- Utilizzando il nome DNS del file system, è possibile montare un file system sull'istanza Amazon EC2 Linux con il comando seguente.

  ```
  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
  ```

- Utilizzando il nome DNS del file system, puoi montare un file system sulla tua istanza Mac Amazon EC2 eseguendo una versione macOS supportata (Big Sur, Monterey, Ventura) con il seguente comando.

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

  > **Important**
  >
  > È necessario usare `mountport=2049` per connettersi correttamente al file system EFS durante il montaggio su istanze Mac EC2 che eseguono versioni macOS supportate.

- Montaggio del nome DNS di destinazione - Nel dicembre 2016, abbiamo introdotto i nomi DNS per i file system. Abbiamo continuare a fornire un nome DNS per ogni target di montaggio di ogni zona di disponibilità per mantenere la compatibilità con le versioni precedenti. Il formato generico di un nome DNS di un target di montaggio è il seguente.

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

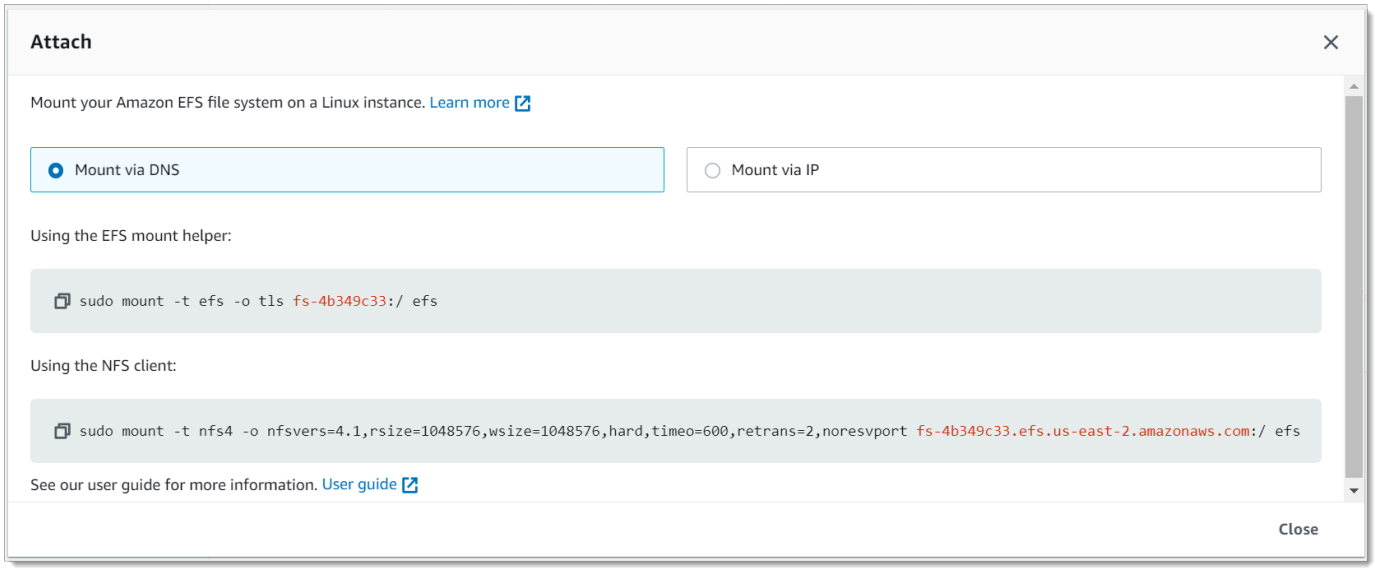
> **Note**
>
> È supportata la risoluzione dei nomi DNS di destinazione tra le zone di disponibilità.

In alcuni casi, è possibile eliminare un target di montaggio e quindi crearne uno nuovo nella stessa zona di disponibilità. In questo caso, il nome DNS per il nuovo target di montaggio in quella zona di disponibilità è lo stesso nome DNS del precedente target di montaggio.

È possibile visualizzare e copiare i comandi esatti per montare il file system nella finestra di dialogo Allega.

Visualizzazione dei comandi di montaggio per il file system

1. Nella console Amazon EFS, scegli il file system che desideri montare per visualizzare la relativa pagina dei dettagli.
2. Per visualizzare i comandi di montaggio da utilizzare per questo file system, scegli Allega in alto a destra.




   La schermata Allega mostra i comandi esatti da usare per il montaggio del file system.
3. La vista Monta tramite DNS predefinita mostra il comando per montare il file system utilizzando il nome DNS del file system durante il montaggio con l'helper di montaggio EFS o un client NFS.

Per un elenco dei sistemi che supportano Amazon Regione AWS EFS, consulta Amazon Elastic File System nel Riferimenti generali di AWS.

Per poter utilizzare un nome DNS nel comando `mount`, devono essere soddisfatte le seguenti condizioni:

- L'istanza EC2 che desidera connettersi deve essere posizionata all'interno di una VPC e deve essere configurata in modo da utilizzare il server DNS fornito da Amazon. Per ulteriori informazioni sul server DNS di Amazon, consulta Impostazioni delle opzioni DHCP nella Guida per l'utente di Amazon VPC.
- La VPC dell'istanza EC2 che si connette deve avere sia la risoluzione DNS che i nomi host DNS abilitati. Per ulteriori informazioni, consulta Visualizzazione degli hostname DNS dell'istanza EC2 nella Guida per l'utente di Amazon VPC.
- L'istanza EC2 che si connette deve trovarsi all'interno dello stesso VPC del file system EFS. Per ulteriori informazioni sull'accesso e il montaggio di un file system da un'altra posizione o da un altro VPC, consultare Procedura dettagliata: creare e montare un file system in locale con una VPN AWS Direct Connect e Scenario: Montaggio di un file system da un VPC diverso .

> **Note**
>
> Prima di montare il file system, consigliamo di attendere 90 secondi dopo la creazione di un target di montaggio. Questa attesa consente ai record DNS di propagarsi completamente nel luogo in Regione AWS cui si trova il file system.

## Montaggio con un indirizzo IP

In alternativa al montaggio del file system Amazon EFS utilizzando il nome DNS, le istanze Amazon EC2 possono montare un file system utilizzando l'indirizzo IP del target di montaggio. Il montaggio tramite indirizzo IP funziona in ambienti in cui il DNS è disattivato, ad esempio VPC con hostname DNS disabilitati.

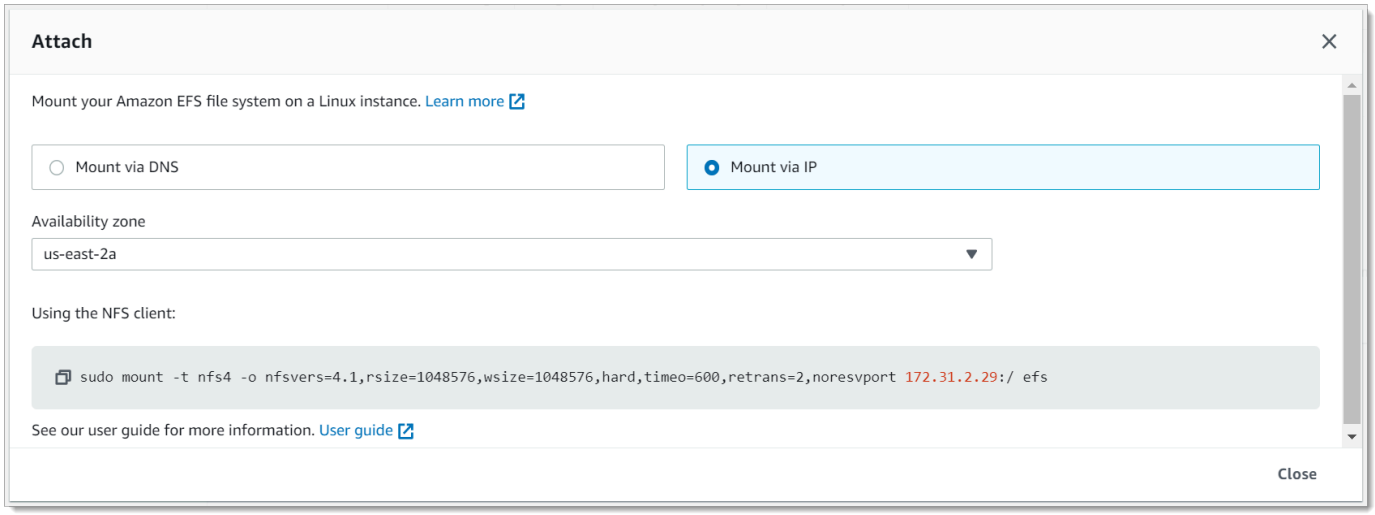
È anche possibile configurare il montaggio di un file system utilizzando l'indirizzo IP del target di montaggio come opzione di fallback per le applicazioni configurate per montare il file system utilizzando per default il nome DNS. Quando si esegue la connessione a un indirizzo IP di un target di montaggio, le istanze EC2 dovrebbero eseguire il montaggio utilizzando l'indirizzo IP del target di montaggio presente nella stessa zona di disponibilità dell'istanza che si connette.

È possibile visualizzare e copiare i comandi esatti per montare il file system nella finestra di dialogo Allega.

> **Note**
>
> Prima di montare il file system, devi aggiungere una regola al gruppo di sicurezza di target di montaggio che consenta l'accesso NFS in entrata dal gruppo di sicurezza EC2. Per ulteriori informazioni, consulta Utilizzo di gruppi di sicurezza VPC per istanze Amazon EC2 e destinazioni di montaggio.

Visualizzazione e copia dei comandi esatti per montare il file system EFS utilizzando l'indirizzo IP del target di montaggio

1. Apri la console Amazon Elastic File System alla pagina https://console.aws.amazon.com/efs/.
2. Nella console Amazon EFS, scegli il file system che desideri montare per visualizzare la relativa pagina dei dettagli.
3. Per visualizzare i comandi di montaggio da utilizzare per questo file system, scegli Allega in alto a destra.




4. La schermata Allega mostra i comandi esatti da usare per il montaggio del file system.

   Scegli Monta tramite IP per visualizzare il comando per montare il file system utilizzando l'indirizzo IP del target di montaggio nella zona di disponibilità selezionata con un client NFS.

- Utilizzando l'indirizzo IP di un target di montaggio nel comando `mount`, puoi montare un file system sulla tua istanza Amazon EC2 Linux con il seguente comando.

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

- Utilizzando l'indirizzo IP di un target di montaggio nel comando `mount`, puoi montare un file system sulla tua istanza Amazon EC2 Mac che esegue macOS Big Sur con il seguente comando.

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

> **Important**
>
> È necessario usare `mountport=2049` per connettersi correttamente al file system EFS durante il montaggio su istanze Mac EC2 che eseguono macOS Big Sur.

## Montaggio con un indirizzo IP in AWS CloudFormation

È inoltre possibile montare il file system utilizzando un indirizzo IP in un AWS CloudFormation modello. Per maggiori informazioni, consulta storage-efs-mountfilesystem-ip-addr.config nel repository elastic-beanstalk-samplesawsdocs/ per i file di configurazione forniti dalla comunità su. GitHub

# Cronologia dei documenti

- Versione API: 01-02-2015
- Ultimo aggiornamento della documentazione: 13 marzo 2024

Nella tabella seguente sono descritte importanti modifiche apportate alla Guida per l'utente di Amazon Elastic File System a partire da luglio 2018. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| Limite di throughput elastico aumentato | Il limite di throughput elastico è stato aumentato per specifiche. Regioni AWS Per ulteriori informazioni, consulta Throughput elastico totale predefinito per tutti i client connessi in ciascuno di essi. Regione AWS | 13 marzo 2024 |
| Aumento di IOPS | I file system che utilizzano la velocità effettiva elastica possono generare un massimo di 90.000 letture per dati a cui si accede raramente. Per ulteriori informazioni sulle prestazioni, consulta Riepilogo delle prestazioni. | 22 gennaio 2024 |
| Politica AWS gestita esistente aggiornata | Autorizzazione `elasticfilesystem:UpdateFileSystemProtection` aggiunta alla AmazonElasticFileSystemFullAccess politica esistente per consentire ai responsabili di aggiornare | 27 novembre 2023 |

| | | |
|---|---|---|
| | la protezione su un file system. Per ulteriori informazioni, consulta gli aggiornamenti di Amazon EFS alle policy AWS gestite. | |
| Replica su file system esistente | I file system possono ora essere replicati su file system esistenti, semplificando la sincronizzazione delle modifiche tra i file system a scopo di failback. Per ulteriori informazioni consulta File system di destinazione. | 27 novembre 2023 |
| Protezione aggiunta del file system | La protezione da sovrascrittura della replica è stata aggiunta ai file system ed è abilitata per impostazione predefinita. La protezione impedisce che il file system venga utilizzato come destinazione in una configurazione di replica. Per ulteriori informazioni, consulta Protezione del file system. | 27 novembre 2023 |
| Nuova classe di storage, tipi di file system e policy sul ciclo di vita | Amazon EFS ora offre la classe di storage di archivio EFS, i tipi di file system e la policy del ciclo di vita di Transizione all'archivio. Per ulteriori informazioni consulta Tipi di file system e classi di storage. | 26 novembre 2023 |

| | | |
|---|---|---|
| Aumento di IOPS | I file system con throughput Elastic supportano ora un massimo di 65.000 operazioni di lettura e 50.000 operazioni di scrittura IOPS per i dati ad accesso infrequente, e ora supportano 250.000 operazioni di lettura IOPS per i dati ad accesso frequente. Per ulteriori informazioni sulle prestazioni, consulta Riepilogo delle prestazioni. | 26 novembre 2023 |
| Eliminazione della configurazione di replica dal file system di origine | Le configurazioni di replica possono ora essere eliminate dal file system di origine. Per ulteriori informazioni, consulta Eliminazione della configurazione di replica. | 19 settembre 2023 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti nella regione Israele (Tel Aviv). | 7 agosto 2023 |
| Miglioramento delle prestazioni dei file system in modalità a scopi generali | I file system in modalità a scopi generali di Amazon EFS ora supportano fino a 55.000 operazioni di lettura al secondo e 25.000 operazioni di scrittura. Per ulteriori informazioni, consulta Quote per i file system Amazon EFS. | 3 agosto 2023 |

| | | |
|---|---|---|
| Il limite di throughput fornito è aumentato | Il limite di throughput assegnato è stato aumentato per specifiche. Regioni AWS Per ulteriori informazioni, consulta Throughput totale predefinito per tutti i client connessi in ciascuno di essi. Regione AWS | 21 giugno 2023 |
| Supporto esteso a livello regionale per la replica EFS | La replica EFS è ora disponibile in tutti i paesi Regioni AWS in cui è disponibile EFS. Per ulteriori dettagli, consulta Replica di Amazon EFS. | 28 aprile 2023 |
| Aumento del limite di throughput elastico | Il limite di throughput elastico è stato aumentato per specifiche. Regioni AWS Per ulteriori informazioni, consulta la tabella Throughput elastico totale predefinito per tutti i client connessi in ciascuno di essi. Regione AWS | 17 aprile 2023 |
| Elastic sostituisce Bursting come modalità di throughput predefinita | La modalità di throughput predefinita (e consigliata) per i file system è ora Elastic anziché Bursting. Per ulteriori informazioni sui privilegi, consultare Modalità di throughput. | 13 aprile 2023 |
| Supporto aggiuntivo aggiunto Regione AWS | Amazon EFS è ora disponibile nella Regione Asia Pacifico (Melbourne). | 12 aprile 2023 |

| | | |
|---|---|---|
| Supporto aggiunto per macOS Ventura | Amazon EFS può ora essere installato su istanze Mac EC2 in esecuzione su macOS Ventura. Per ulteriori informazioni, consulta Distribuzioni supportate. | 10 aprile 2023 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile nella Regione Asia Pacifico (Hyderabad). | 16 febbraio 2023 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti in Europa (Spagna) Regione AWS. | 19 gennaio 2023 |
| Il limite dei punti di accesso per i file system è aumentato | Il numero massimo di punti di accesso che un singolo file system può avere è passato da 120 a 1.000. Per ulteriori informazioni, consulta la pagina Quote di risorse. | 17 gennaio 2023 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti in Europa (Zurigo) Regione AWS. | 15 dicembre 2022 |
| Supporto aggiunto per le policy relative al ciclo di vita giornaliero | Ora puoi selezionare un giorno per la transizione alla policy del ciclo di vita IA. Per ulteriori informazioni, consulta Uso delle policy del ciclo di vita. | 27 novembre 2022 |

| | | |
|---|---|---|
| Latenze in lettura e scrittura ridotte | Le latenze per la lettura e la scrittura dei dati di file sono state ridotte sia per lo storage a zona singola che per i file system di storage Standard. Per ulteriori informazioni sulle prestazioni, consulta Riepilogo delle prestazioni. | 27 novembre 2022 |
| Aggiunta della modalità di throughput | La modalità di throughput elastico viene aggiunta come opzione di throughput per i file system Amazon EFS. Per ulteriori informazioni, consulta Elastic throughput. | 27 novembre 2022 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti nella regione Medio Oriente (Emirati Arabi Uniti). | 17 ottobre 2022 |
| Supporto aggiunto per Replica EFS | Amazon EFS ha rimosso un limite precedente in base al quale la replica EFS non supportava socket e named pipe o FIFO. | 15 settembre 2022 |
| Il limite per il numero di blocchi di file per connessione è aumentato | Il numero di blocchi di file per connessione è aumentato da 8192 a 65.536. Per ulteriori informazioni, consulta Quote per i client NFS. | 4 maggio 2022 |

| | | |
|---|---|---|
| È stato rimosso il limite per i processi che utilizzano blocchi di file | Amazon EFS ha rimosso un limite precedente in base al quale un massimo di 256 processi su una singola istanza potevano utilizzar e blocchi di file contempor aneamente. Per ulteriori informazioni, consulta Quote per i client NFS. | 4 maggio 2022 |
| È stato aggiunto Regione AWS supporto aggiuntivo | Amazon EFS è ora disponibi le nella Regione Asia Pacific (Giacarta) Regione AWS. | 27 gennaio 2022 |
| Supporto aggiunto per Replica EFS | Utilizza EFS Replication per replicare i dati e i metadati su un file system EFS su un altro file system EFS Regione AWS di tua scelta. Per ulteriori informazioni, consulta Replica in Amazon EFS. | 25 gennaio 2022 |
| Il file system e le risorse di target di montaggio utilizzan o il formato ID risorsa a 17 caratteri | Al nuovo file system Amazon EFS e alle risorse dei target di montaggio vengono ora assegnati ID di 17 caratteri . Per ulteriori informazioni, consulta l'argomento relativo agli ID di risorsa. | 22 ottobre 2021 |

| | | |
|---|---|---|
| Supporto aggiunto per EFS Intelligent-Tiering | EFS Intelligent-Tiering utilizza EFS Lifecycle Managemen t per monitorare i modelli di accesso ai file ed è progettat o per la transizione automatic a dei file da e verso le classi di storage Infrequent Access (IA) corrispondenti. Per ulteriori informazioni, consulta EFS Intelligent-Tiering ed EFS Lifecycle Management. | 2 settembre 2021 |
| Supporto aggiunto per testare il formato ID risorsa a 17 caratteri | Amazon EFS passerà dall'uso di ID di 8 caratteri a ID di 17 caratteri per file system e target di montaggio il 1° ottobre 2021. Durante questa transizione, puoi attivare e iniziare a utilizzare ID di risorsa da 17 caratteri per volta. Regione AWS Per ulteriori informazioni, consulta l'argomento relativo agli ID di risorsa. | 5 maggio 2021 |

| | | |
|---|---|---|
| Supporto aggiunto per il montaggio di file system a zona singola da una zona di disponibilità diversa utilizzando l'helper di montaggio Amazon EFS | Ora puoi utilizzare l'assistente di montaggio EFS per montare un file system Amazon EFS che utilizza classi di storage a zona singola su un'istanza EC2 che si trova in una zona di disponibilità diversa. Puoi utilizzare la nuova opzione az per specificare la zona di disponibilità del file system Amazon EFS. Per ulteriori informazioni, consulta Montaggio di file system con classi di storage a zona singola. | 6 aprile 2021 |
| Supporto aggiunto per classi di storage EFS a zona singola | Le classi di storage Amazon EFS a zona singola archiviano i dati in modo ridondante all'interno di una singola zona di disponibilità in Regione AWS. Le classi di storage EFS a zona singola e ad accesso infrequente (One Zone-IA) sono un'opzione conveniente per l'archiviazione dei dati che non richiede la resilienza Multi-AZ delle classi di storage EFS Standard e Standard-IA. Per ulteriori informazioni, consulta Uso delle classi di storage EFS. | 9 marzo 2021 |

| | | |
|---|---|---|
| Supporto aggiuntivo aggiunto Regione AWS | Amazon EFS è ora disponibile per tutti gli utenti nella regione Asia Pacifico (Osaka) Regione AWS. | 3 marzo 2021 |
| È stato aggiunto il supporto per le istanze Amazon EC2 macOS che eseguono macOS Big Sur | Ora puoi montare il tuo file system Amazon EFS da istanze macOS EC2 che eseguono macOS Big Sur utilizzando l'helper di montaggio EFS o il comando di montaggio NFS. Per ulteriori informazioni, consulta Montaggio con l'helper di montaggio EFS o Montaggio dei file system senza l'helper di montaggio EFS. | 23 febbraio 2021 |
| La nuova console Amazon EFS è disponibile nella AWS GovCloud (US) regione | La nuova console Amazon EFS è ora disponibile in AWS GovCloud (US) Regione AWS. | 10 febbraio 2021 |
| Support aggiunto per la nuova CloudWatch metrica Amazon EFS `MeteredIOBytes` | Puoi usare `MeteredIOBytes` per misurare il numero di byte per ciascuna operazione del file system, tra cui la lettura e la scrittura di dati oltre alle operazioni di metadati. Le operazioni di lettura vengono misurate a un terzo della velocità delle altre operazioni. Per ulteriori informazioni, consulta i CloudWatchparametri Amazon per Amazon EFS. | 28 gennaio 2021 |

| | | |
|---|---|---|
| Amazon EFS aumenta la velocità di lettura del file system del 300% | I file system Amazon EFS misurano le richieste di lettura a una velocità di un terzo rispetto alle altre richieste. | 28 gennaio 2021 |
| Support aggiunto per la nuova CloudWatch metrica Amazon EFS `StorageBytes` | Puoi usare `StorageBytes` per misurare e monitorare la dimensione del file system in byte, inclusa la quantità di dati archiviati nelle classi di storage Standard e Infrequent Access. Per ulteriori informazioni, consulta i CloudWatch parametri Amazon per Amazon EFS. | 11 gennaio 2021 |
| Utilizzalo AWS Transfer Family per accedere ai file system Amazon EFS | Puoi utilizzarlo AWS Transfer Family per trasferire file da e verso i tuoi file system Amazon EFS. Per ulteriori informazioni, vedere Utilizzo AWS Transfer Family per accedere ai file nel file system EFS. | 6 gennaio 2021 |
| Utilizzare AWS Systems Manager per gestire il client Amazon EFS (`amazon-efs-utils`) | Puoi usarlo AWS Systems Manager per installare o aggiornare automaticamente i client Amazon EFS (`amazon-efs-utils` ) sulle tue istanze EC2. Per ulteriori informazioni, consulta Utilizzo di AWS Systems Manager per installare o aggiornare automaticamente i client Amazon EFS. | 29 settembre 2020 |

| | | |
|---|---|---|
| Applicazione della creazione di file system crittografati | Puoi utilizzare la chiave di condizione `elasticfilesystem:Encrypted` AWS Identity and Access Management (IAM) per imporre agli utenti di creare file system Amazon EFS crittografati a riposo. Per ulteriori informazioni, consulta Applicazione della creazione di file system Amazon EFS crittografati a riposo. | 16 settembre 2020 |
| Il throughput per client di Amazon EFS è aumentato del 100% | EFS ora supporta fino a 500 MB/s di throughput per client, un aumento del 100% rispetto al precedente limite di 250 MB/s. Per ulteriori informazioni, consulta Quote per i file system Amazon EFS. | 23 luglio 2020 |
| Supporto aggiunto per i backup automatici giornalieri dei file system Amazon EFS | I backup giornalieri automatici sono sempre abilitati per impostazione predefinita quando crei un file system utilizzando la console EFS. Per ulteriori informazioni, consulta Using AWS Backup with Amazon EFS. | 16 luglio 2020 |

| | | |
|---|---|---|
| Il nuovo flusso di lavoro Quick Create semplifica la creazione di file system Amazon EFS | Utilizzando l'opzione Quick Create nella console EFS, è possibile creare un file system EFS utilizzando le impostazioni consigliate dal servizio con un solo pulsante. Per ulteriori informazioni, consulta il file system CreateyYour Amazon EFS. | 16 luglio 2020 |
| È ora disponibile la console Amazon EFS | La nuova console EFS semplifica l'utilizzo di Amazon EFS e semplifica la gestione dei file system EFS. | 16 luglio 2020 |
| Amazon EFS aumenta la velocità di trasmissione effettiva di file system | I file system Amazon EFS che utilizzano il throughput Bursting ora hanno un throughput minimo di 1 MiB/s. Per ulteriori informazioni sui privilegi, consultare Modalità di throughput. | 30 giugno 2020 |
| Miglioramento delle prestazioni dei file system in modalità General Purpose | I file system per General Purpose di Amazon EFS ora supportano fino a 35.000 operazioni di lettura al secondo, con un incremento del 400% rispetto al precedente limite di 7.000. Per ulteriori informazioni, consulta Quote per i file system Amazon EFS. | 1 Aprile 2020 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti di Pechino e Ningxia Regioni AWS. | 22 gennaio 2020 |

| | | |
|---|---|---|
| Supporto aggiunto per l’autorizzazione IAM per client NFS | Ora puoi usare AWS Identity and Access Management (IAM) per gestire l'accesso NFS a un file system Amazon EFS. Per ulteriori informazioni, consulta Usare AWS IAM per controllare l'accesso NFS ad Amazon EFS. | 13 gennaio 2020 |
| Aggiunto il supporto per i punti di accesso EFS | I punti di accesso Amazon EFS sono punti di accesso specifici dell'applicazione in un file system Amazon EFS che semplificano la gestione dell'accesso dell'applicazione ai set di dati condivisi. Per ulteriori informazioni, consultare Utilizzo dei punti di accesso Amazon EFS. | 13 gennaio 2020 |
| Support aggiunto per il ripristino AWS Backup parziale. | È ora possibile ripristinare file e directory specifici utilizzando un ripristino parziale, oltre a ripristinare un punto di ripristino completo. Per ulteriori informazioni, consulta Using AWS Backup with Amazon EFS. | 13 gennaio 2020 |

| | | |
|---|---|---|
| Supporto aggiunto per i ruoli collegati ai servizi | Amazon EFS utilizza ora un ruolo collegato ai servizi basato su IAM, che semplific a la configurazione di EFS aggiungendo automaticamente le autorizzazioni necessari e. Per ulteriori informazioni, consulta la sezione relativa all'utilizzo di ruoli collegati ai servizi per Amazon EFS. | 10 dicembre 2019 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibi le per tutti gli utenti in Europa (Stoccolma). Regione AWS | 20 novembre 2019 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibi le per tutti gli utenti in Asia Pacifico (Hong Kong) Regione AWS. | 20 novembre 2019 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibi le per tutti gli utenti del Sud America (San Paolo) Regione AWS. | 20 novembre 2019 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibi le per tutti gli utenti del Medio Oriente (Bahrain) Regione AWS. | 20 novembre 2019 |

| | | |
|---|---|---|
| Aggiunta una nuova policy di gestione del ciclo di vita di 7 giorni | La gestione del ciclo di vita dispone ora di una policy aggiuntiva per spostare i dati nella conveniente classe di storage ad accesso infrequente dopo 7 giorni. Per ulteriori informazioni, consulta Gestione del ciclo EFS. | 6 novembre 2019 |
| Aggiunto il supporto per endpoint VPC di interfaccia | Puoi stabilire una connessio ne privata tra il cloud privato virtuale (VPC, Virtual Private Cloud) e Amazon EFS per chiamare l'API EFS. Per ulteriori informazioni, consulta Utilizzo degli endpoint VPC. | 22 ottobre 2019 |
| Monta un file system EFS all'avvio di una nuova istanza EC2. | È ora possibile configurare nuove istanze Amazon EC2 per montare i file system EFS all'avvio nella procedura guidata di avvio delle istanze EC2. Per ulteriori informazi oni, consulta Fase 2. Crea le risorse EC2 e avvia l'istanza EC2. | 17 ottobre 2019 |
| Supporto per le quote di servizio aggiunte | Ora puoi visualizzare tutti i limiti di Amazon EFS nella console Quote di servizio. Per ulteriori dettagli, consulta Limiti per Amazon EFS. | 10 settembre 2019 |

| | | |
|---|---|---|
| Aggiunta di nuove policy di gestione del ciclo di vita | Quando si utilizza la gestione del ciclo di vita, è ora possibile scegliere tra una delle quattro policy del ciclo di vita per definire quando i file vengono trasferiti nella classe di storage Infrequent Access più conveniente. Per ulteriori informazioni, consulta Gestione del ciclo EFS. | 9 luglio 2019 |
| Gestione del ciclo di vita EFS ora disponibile su tutti i file system EFS. | La funzionalità di gestione del ciclo di vita EFS è ora disponibile su tutti i file system EFS. È stata ora rimossa una restrizione precedent e basata su quando è stato creato un file system. Per ulteriori informazioni, consulta Gestione del ciclo EFS. | 9 luglio 2019 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibi le per tutti gli utenti in Europa (Parigi) Regione AWS. | 12 giugno 2019 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibi le per tutti gli utenti in Asia Pacifico (Mumbai) Regione AWS. | 5 giugno 2019 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibi le per tutti gli utenti in Canada (Central) Regione AWS. | 1 maggio 2019 |

| | | |
|---|---|---|
| Aggiornamento API: i tag fanno ora parte del payload CreateFileSystem operativo | Ora puoi includere tag quando utilizzi le CreateFileSystem operazioni AWS API e CLI per creare un file system Amazon EFS. Per ulteriori informazioni, consulta CreateFileSystemCreazione di un file system utilizzando la AWS CLI. | 19 febbraio 2019 |
| Nuove funzionalità: classe di storage Accesso non frequente EFS e la gestione del ciclo di vita di storage EFS | L'accesso non frequente Amazon EFS è una classe di storage a basso costo per file ai quali l'accesso non viene effettuato di frequente. La gestione del ciclo di vita EFS esegue la transizione dei file automaticamente da storage Standard ad Accesso non frequente. Per ulteriori informazioni, consultare Classi di storage EFS. | 13 febbraio 2019 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti in Europa (Londra) Regione AWS. | 23 gennaio 2019 |
| AWS Backup Integrazione dei servizi con Amazon EFS | È possibile eseguire il backup dei file system Amazon EFS utilizzando AWS Backup un servizio di backup completamente gestito, centralizzato e automatizzato per il backup dei dati tra AWS servizi nel cloud e in locale. Per ulteriori dettagli, consulta AWS Backup e Amazon EFS. | 16 gennaio 2019 |

| | | |
|---|---|---|
| Aggiunto il supporto per la connessione Gateway Transit ai sistemi di storage on-premise. | I file system Amazon EFS sono ora accessibili utilizzando le connessioni Gateway Transit ai sistemi di storage on-premise. Per ulteriori informazioni, vedi Montaggio da un altro account o VPC e Scenario: Montaggio di un file system da un VPC diverso. | 6 dicembre 2018 |
| EFS File Sync fa ora parte del nuovo AWS DataSync servizio. | AWS DataSync è un servizio di trasferimento dati gestito che semplifica la sincronizzazione di grandi quantità di dati tra sistemi di storage locali e AWS servizi di archiviazione. Per ulteriori informazioni, consulta Trasferimento di file da file system locali ad Amazon EFS Using AWS DataSync. | 26 novembre 2018 |
| Aggiunto il supporto per la connessione VPN e peering VPC interregionale | Amazon EFS è ora accessibile tramite connessioni VPN e peering VPC interregionale. Per ulteriori informazioni, consulta Trasferimento di file da file system locali ad Amazon EFS Using AWS DataSync. | 23 ottobre 2018 |

| | | |
|---|---|---|
| Aggiunto il supporto per la connessione VPN e peering VPC interregionale | I file system Amazon EFS sono ora accessibili tramite connessioni VPN e peering VPC interregionale. Per ulteriori informazioni, consultare Montaggio da un altro account o VPC e Come funziona Amazon EFS con Direct Connect e le VPN. | 23 ottobre 2018 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti nella regione Asia Pacifico (Singapore) Regione AWS. | 13 luglio 2018 |
| Presentazione della modalità Provisioned Throughput | È ora possibile effettuare il provisioning di throughput per un file system nuovo o esistente con la nuova modalità Provisioned Throughput. Per ulteriori informazioni sui privilegi, consultare Modalità di throughput. | 12 luglio 2018 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti nella regione Asia Pacifico (Tokyo) Regione AWS. | 11 luglio 2018 |

Nella tabella seguente sono descritte importanti modifiche apportate alla Guida per l'utente di Amazon Elastic File System a partire da luglio 2018.

| Modifica | Descrizione | Data della modifica |
| --- | --- | --- |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti nella Regione Asia Pacifico (Seoul) AWS . | 30 maggio 2018 |
| È stato aggiunto il supporto per la matematica CloudWatch metrica | La matematica metrica consente di interrogare più CloudWatch metriche e utilizzare espressioni matematiche per creare nuove serie temporali basate su queste metriche. Per ulteriori informazioni, consulta Utilizzo della matematica dei parametri con Amazon EFS. | 4 aprile 2018 |
| Aggiunta del set di strumenti open source `amazon-efs-utils` e della crittografia dei dati in transito | Gli strumenti `amazon-efs-utils` sono un set di file eseguibili open source che semplificano diversi aspetti dell'utilizzo di Amazon EFS, come ad esempio l'operazione di montaggio. L'utilizzo non comporta costi aggiuntivi e puoi `amazon-efs-utils` scaricare questi strumenti da. GitHub Per ulteriori informazioni, consulta Utilizzo degli amazon-efs-utils strumenti.<br><br>Inoltre, in questa versione, Amazon EFS supporta ora la crittografia dei dati in transito tramite tunneling Transport Layer Security (TLS). Per ulteriori informazioni, consulta Crittografia dei dati in Amazon EFS. | 4 aprile 2018 |
| Limiti del file system aggiornati per Regione AWS | Amazon EFS ha incrementato il limite del numero di file system disponibili a tutti gli account in ogni Regione AWS. Per ulteriori informazioni, consulta Quote di risorse di Amazon EFS che non puoi modificare. | 15 marzo 2018 |
| Regione AWS Supporto aggiuntivo aggiunto | Amazon EFS è ora disponibile per tutti gli utenti negli Stati Uniti occidentali (California settentrionale) Regione AWS. | 14 marzo 2018 |

| Modifica | Descrizione | Data della modifica |
| --- | --- | --- |
| Crittografia dei dati a riposo | Amazon EFS supporta ora la crittografia dei dati a riposo. Per ulteriori informazioni, consulta Crittografia dei dati in Amazon EFS. | 14 agosto 2017 |
| Aggiunto il supporto di una regione aggiuntiva | Amazon EFS è ora disponibile per tutti gli utenti nella regione Europa (Francoforte). | 20 luglio 2017 |
| Nomi di file system che utilizzano DNS (Domain Name System) | Amazon EFS supporta ora i nomi DNS per i file system. Un nome su DNS di un file system viene risolto automaticamente in un indirizzo IP di destinazione per il montaggio nella zona di disponibilità dell'istanza Amazon EC2 che vi si connette. Per ulteriori informazioni, consulta Montaggio su Amazon EC2 con un nome DNS. | 20 dicembre 2016 |
| Miglioramento del supporto dei tag per i file system | Amazon EFS supporta ora 50 tag per ogni file system. Per ulteriori informazioni sui tag in Amazon EFS, consulta Aggiunta di tag alle risorse Amazon ECS. | 29 agosto 2016 |
| Disponibilità generale | Amazon ECS è ora disponibile nelle regioni Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon) ed Europa (Irlanda). | 28 giugno 2016 |
| Aumento del limite dei file system | Aumento da 5 a 10 del numero di file system Amazon EFS che possono essere creati per account in ogni Regione AWS . | 21 agosto 2015 |
| Aggiornamento dell'esercitazione sulle nozioni di base | L'esercitazione sulle nozioni di base è stata aggiornata per semplificare il processo di acquisizione delle nozioni di base. | 17 agosto 2015 |
| Nuova guida | Questa è la prima versione della Guida per l’utente di Amazon Elastic File System. | 26 maggio 2015 |

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.