aws

Guida per l'utente

Amazon Elastic File System

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Elastic File System: Guida per l'utente

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in qualsiasi modo che possa causare confusione tra i clienti o in qualsiasi modo che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Cos'è Amazon Elastic File System? 1
È la prima volta che utilizzi Amazon EFS? 2
Come funziona 3
Come funziona Amazon EFS con Amazon EC2 4
Come funziona Amazon EFS con AWS Direct Connect e AWS Managed VPN 7
Come funziona Amazon EFS con AWS Backup 8
Funzionalità 9
Autenticazione e controllo degli accessi 9
Coerenza dei dati in Amazon EFS 9
Disponibilità e durabilità 10
Replica 17
Nozioni di base 18
Prerequisiti 18
Crea il file system e avvia l' EC2 istanza 18
Trasferisci i file sul tuo file system 19
Prerequisiti 19
Pulizia delle risorse 20
Installazione del client EFS 22
Dipendenze per gli strumenti EFS 22
Distribuzioni supportate 23
Installazione manuale del client EFS 25
Installazione del client Amazon EFS su istanze Amazon EC2 Linux 25
Installazione del client Amazon EFS su altre distribuzioni Linux 26
Installazione del client EFS su istanze EC2 Mac 26
Installazione automatica del client EFS 27
Comportamento del client Amazon EFS durante l'installazione 27
Sistemi operativi supportati da Systems Manager 28
Configurazione AWS Systems Manager per l'installazione del client EFS 29
Installazione e aggiornamento `botocore` 31
Aggiornamento di `stunnel` 31
Risoluzione dei problemi con l'installazione di stunnel 33
Attivazione della modalità FIPS 35
Creazione e gestione di risorse 36
Riepilogo dell'implementazione 37

Risorsa IDs ... 38
Token di creazione e idempotenza ... 39
Creazione di file system ... 39
Autorizzazioni IAM richieste per la creazione di file system ... 40
Opzioni di configurazione per i file system ... 40
Eliminazione dei file system ... 56
Creazione di policy del file system ... 57
Creazione di access point ... 60
Eliminazione dei punti di accesso ... 63
Applicazione di tag alle risorse ... 63
Nozioni di base sui tag ... 64
Limitazioni applicate ai tag ... 64
Utilizzo di tag per il controllo degli accessi ... 65
Assegnazione di tag alle risorse ... 65
Tutorial: Creazione di sottodirectory scrivibili per utente ... 66
Montaggio del file system ... 69
Considerazioni sul montaggio per Linux ... 69
Uso dell'helper di montaggio di EFS ... 71
Impostazioni di montaggio utilizzate dall'helper di montaggio EFS ... 73
Ottenimento dei log per il supporto ... 74
Prerequisiti ... 75
Montaggio su Linux EC2 ... 76
Montaggio su Mac EC2 ... 78
Montaggio da una regione diversa ... 80
Montaggio dei file system a zona singola ... 81
Montaggio con autorizzazione IAM ... 85
Montaggio con punti di accesso EFS ... 86
Montaggio di più istanze EC2 ... 86
Montaggio da un altro account o VPC ... 88
Utilizzo di NFS ... 91
Prerequisiti ... 92
Supporto per NFS ... 92
Installazione del client NFS ... 93
Impostazioni di montaggio NFS consigliate ... 95
Montaggio su EC2 DNS ... 97
Montaggio con un indirizzo IP ... 100

Montaggio automatico dei file system 102
Nuove EC2 istanze Linux 102
Istanze EC2 Linux esistenti 104
Istanze Linux e Mac che utilizzano NFS 108
Smontaggio dei file system 110
Tutorial: Creare e montare un file system utilizzando il AWS CLI 111
Prerequisiti 112
Configurazione del AWS CLI 113
Fase 1: Creare risorse EC2 114
Fase 2: Creare risorse EFS 120
Fase 3: montare e testare il file system 123
Fase 4: pulizia 126
Tutorial: Montaggio con client locali 128
Prerequisiti 129
Fase 1: Crea le tue risorse EFS 131
Fase 2: installare il client NFS 133
Fase 3: Montare il file system Amazon EFS File System sul client on-premise 133
Fase 4: Eliminazione delle risorse e protezione dell'account AWS 135
Opzionale: crittografia dei dati in transito 136
Tutorial: monta un file system da un altro VPC 139
Prerequisiti 140
Fase 1: Determinare l'ID della zona di disponibilità del target di montaggio 140
Fase 2: Determinare l'indirizzo IP di destinazione del montaggio 141
Fase 3: Aggiungere una voce host per la destinazione di montaggio 142
Fase 4: Montare il file system utilizzando l'helper di montaggio EFS 142
Passaggio 5: ripulisci le risorse e proteggi le Account AWS 144
Risoluzione dei problemi con il montaggio 145
Montaggio fallito del file system su un'istanza Windows 145
Accesso rifiutato dal server 145
Il montaggio automatico non funziona e l'istanza non risponde 146
Il montaggio di molteplici file system Amazon EFS in /etc/fstab ha esito negativo 146
Il comando di montaggio ha esito negativo con il messaggio di errore "tipo fs errato" 147
Il comando di montaggio ha esito negativo con il messaggio di errore "opzione di montaggio errata" 148
Montaggio con punti di accesso non riuscito 148

Il montaggio del file system ha esito negativo immediatamente dopo la creazione del file system ... 149
Il montaggio di un file system rimane in attesa e quindi ha esito negativo con un errore di timeout ... 149
Il montaggio di un file system con NFS usando il nome DNS ha esito negativo ... 150
Il montaggio del file system ha esito negativo con "nfs not responding" (nfs non risponde) ... 151
Lo stato del ciclo di vita della destinazione di montaggio è bloccato ... 151
Lo stato del ciclo di vita di Mount Target mostra un errore ... 151
Il comando di montaggio non risponde ... 152
Il client montato viene disconnesso ... 152
Le operazioni su un file system appena montato restituiscono l'errore "handle del file errato" ... 153
Esito negativo dello smontaggio di un file system ... 153
Trasferimento dei dati ... 155
Usando AWS DataSync ... 155
Usando AWS Transfer Family ... 156
Prerequisiti per l'utilizzo AWS Transfer Family con Amazon EFS ... 156
Configurazione del file system EFS per AWS Transfer Family ... 157
Gestione dei file system ... 162
Comprendere lo stato del file system ... 162
Gestione dei target di montaggio ... 163
Monta obiettivi e zone di disponibilità ... 164
Creazione di destinazioni di montaggio ... 167
Eliminazione degli obiettivi di montaggio ... 173
Modifica del VPC di destinazione del montaggio ... 175
Modifica dei gruppi di sicurezza di Mount Target ... 175
Gestione della velocità di trasmissione effettiva ... 177
Gestione del ciclo di vita dello storage ... 179
Operazioni del file system per la gestione del ciclo di vita ... 180
Configurazione delle politiche del ciclo di vita ... 180
Gestione dell'accesso ai file system crittografati ... 183
Gestione delle chiavi KMS per i file system EFS ... 184
Monitoraggio ... 186
Strumenti di monitoraggio ... 187
Strumenti automatici ... 187
Strumenti di monitoraggio manuali ... 188

Misurazione di un file system 188
Misurazione degli oggetti 189
Dimensioni misurate del file system 190
Misurazione della velocità di trasmissione effettiva 192
Visualizzazione della dimensione della classe di storage 193
Monitoraggio delle metriche con CloudWatch 194
CloudWatch metriche 195
Accesso alle metriche CloudWatch 201
Utilizzo delle metriche CloudWatch 203
Utilizzo della matematica metrica con le metriche CloudWatch 204
Monitoraggio dei tentativi di montaggio riusciti e falliti 210
Creazione di allarmi 212
Registrazione delle chiamate API di CloudTrail con 214
Informazioni su Amazon EFS in CloudTrail 214
Informazioni sulle voci del file di log Amazon EFS 215
Voci dei file di log di Amazon encrypted-at-rest EFS per i file system 222
Utilizzo dei report di fatturazione e utilizzo 223
Utilizzo dei tag per l'allocazione dei costi 223
Tag per l'allocazione dei costi definiti dall'utente 224
Report di fatturazione 225
Report di utilizzo 226
Comprensione dei report di utilizzo e fatturazione 227
Monitoraggio delle operazioni nei report di utilizzo 231
Specifiche prestazionali 232
Riepilogo delle prestazioni 232
Classi di archiviazione 234
Modalità prestazionali 235
Modalità di velocità di trasmissione effettiva 236
Scelta di una modalità di throughput 236
Produttività elastica 237
Throughput assegnato 237
Restrizioni al cambio di velocità effettiva e alla modifica della quantità assegnata 240
Suggerimenti per le prestazioni 240
I/O Dimensioni medie 240
Ottimizzazione dei carichi di lavoro che richiedono throughput e IOPS elevati 241
Connessioni simultanee 241

Modello di richiesta ... 241
Impostazioni di installazione del client NFS ... 242
Ottimizzazione delle prestazioni dei file di piccole dimensioni ... 243
Ottimizzazione delle prestazioni della directory ... 243
Ottimizzazione della dimensione read_ahead_kb di NFS ... 244
Risoluzione dei problemi di prestazioni ... 245
Impossibile creare un file system EFS ... 246
Accesso negato ai file consentiti sul file system NFS ... 246
Errori durante l'accesso alla console Amazon EFS ... 246
L' EC2 istanza Amazon si blocca ... 247
Blocco di un'applicazione che esegue la scrittura di grandi quantità di dati ... 247
Prestazioni scadenti durante l'apertura di svariati file in parallelo ... 248
Impostazioni NFS personalizzate che causano ritardi nelle operazioni di scrittura ... 248
La creazione di backup con Oracle Recovery Manager è lenta ... 249
Risoluzione dei problemi di AMI e kernel ... 249
Non è possibile eseguire il comando chown ... 250
Il file system continua a eseguire ripetutamente delle operazioni a causa di un bug del client ... 250
Client in deadlock ... 250
Il recupero dell'elenco dei file di una grande cartella impiega molto tempo ... 251
Backup e replica dei dati ... 252
Backup di file system ... 252
Come AWS Backup funziona con Amazon EFS ... 253
Autorizzazioni IAM richieste ... 255
Prestazioni di backup ... 255
Gestione dei backup automatici ... 256
Replica dei file system ... 257
Costi ... 258
Prestazioni di replica ... 259
Autorizzazioni IAM richieste ... 259
Configurazione della replica su un nuovo file system ... 260
Configurazione della replica su un file system esistente ... 264
Replica su più account AWS ... 270
Visualizzazione dei dettagli della replica ... 275
Eliminazione di configurazioni di replica ... 280
Utilizzo della replica ... 282

Protezione dei dati 283
Crittografia dei dati 284
AWS KMS 285
Crittografia dei dati a riposo 288
Crittografia dei dati in transito 289
Risoluzione dei problemi di crittografia 291
Gestione dell'identità e degli accessi 293
Destinatari 294
Autenticazione con identità 295
Gestione dell'accesso con policy 298
Funzionamento di Amazon Elastic File System con IAM 301
Esempi di policy basate su identità 308
Esempi di policy basate su risorse 312
AWS politiche gestite 316
Utilizzo di tag con Amazon EFS 322
Utilizzo di ruoli collegati ai servizi per Amazon EFS 325
Risoluzione dei problemi 330
Controllo dell'accesso ai dati del file system 332
Policy del file system predefinita 333
Operazioni EFS per client 333
Chiavi di condizione EFS per client 333
Esempi di policy del file system 334
Controllo dell'accesso di rete 334
Utilizzo dei gruppi di sicurezza VPC 335
Uso di endpoint VPC 337
Utenti, gruppi e autorizzazioni a livello NFS 339
Autorizzazioni di file e directory 340
Esempi di casi d'uso e autorizzazioni del file system EFS 341
Autorizzazioni ID utente e di gruppo per file e directory all'interno di un file system 342
No Root Squashing 343
Caching delle autorizzazioni 346
Modifica della proprietà degli oggetti del file system 346
Punti di accesso EFS 346
Utilizzo dei punti di accesso 346
Applicazione dell'identità dell'utente 347
Applicazione di una directory principale 348

Utilizzo di punti di accesso nelle policy IAM ... 350
Blocco dell'accesso pubblico ai file system ... 351
Blocco dell'accesso pubblico con AWS Transfer Family ... 352
Significato di "pubblico" ... 352
Convalida della conformità ... 354
Resilienza ... 356
Isolamento della rete ... 357
Quote ... 358
Quote per Amazon EFS che è possibile incrementare ... 358
Richiesta di aumento delle quote ... 361
Quote di risorse di Amazon EFS che non puoi modificare ... 361
Limiti per i client NFS ... 363
Quote per i file system Amazon EFS ... 364
Funzionalità NFSv4 2.0 e 4.1 non supportate ... 365
Ulteriori considerazioni ... 366
Risoluzione degli errori di funzionamento dei file relativi alle quote ... 366
Il comando ha esito negativo con l'errore "Quota disco superata" ... 367
Il comando ha esito negativo con l'errore "Errore di I/O" ... 367
Il comando ha esito negativo con l'errore "Nome del file troppo lungo" ... 368
Il comando ha esito negativo con l'errore "File non trovato" ... 368
Il comando ha esito negativo con l'errore "Troppi link" ... 368
Il comando ha esito negativo con l'errore "File troppo grande" ... 369
API Amazon EFS ... 370
Endpoint API ... 370
IPv4 endpoint ... 371
Endpoint dual-stack (e) IPv4 IPv6 ... 371
Specificazione degli endpoint ... 372
Versione API ... 372
Argomenti correlati ... 372
Gestione della frequenza massima di richieste della Query API per Amazon EFS ... 373
Polling ... 373
Tentativi ripetuti o elaborazione batch ... 373
Calcolo dell'intervallo di attesa ... 373
Operazioni ... 374
CreateAccessPoint ... 376
CreateFileSystem ... 384

CreateMountTarget ... 400
CreateReplicationConfiguration ... 415
CreateTags ... 421
DeleteAccessPoint ... 424
DeleteFileSystem ... 426
DeleteFileSystemPolicy ... 430
DeleteMountTarget ... 433
DeleteReplicationConfiguration ... 437
DeleteTags ... 440
DescribeAccessPoints ... 443
DescribeAccountPreferences ... 448
DescribeBackupPolicy ... 451
DescribeFileSystemPolicy ... 454
DescribeFileSystems ... 458
DescribeLifecycleConfiguration ... 464
DescribeMountTargets ... 468
DescribeMountTargetSecurityGroups ... 474
DescribeReplicationConfigurations ... 478
DescribeTags ... 482
ListTagsForResource ... 487
ModifyMountTargetSecurityGroups ... 491
PutAccountPreferences ... 495
PutBackupPolicy ... 498
PutFileSystemPolicy ... 501
PutLifecycleConfiguration ... 507
TagResource ... 516
UntagResource ... 520
UpdateFileSystem ... 523
UpdateFileSystemProtection ... 531
Tipi di dati ... 534
AccessPointDescription ... 536
BackupPolicy ... 539
CreationInfo ... 540
Destination ... 542
DestinationToCreate ... 545
FileSystemDescription ... 549

FileSystemProtectionDescription 554
FileSystemSize 555
LifecyclePolicy 557
MountTargetDescription 559
PosixUser 563
ReplicationConfigurationDescription 565
ResourceIdPreference 567
RootDirectory 568
Tag 570
Cronologia dei documenti 571
..... dxcviii

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. Poiché Amazon EFS dispone di una semplice interfaccia di servizi Web, è possibile 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), quindi le applicazioni e gli strumenti che usi oggi funzionano perfettamente 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 EKS e. AWS Lambda 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 della stessa. 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 un'unica zona di disponibilità. L'archiviazione dei dati in un'unica 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, vedereSpecifiche prestazionali di 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 Protezione dei dati 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. È possibile abilitare la crittografia a riposo durante la creazione di un file system EFS. 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 dei client NFS ad Amazon 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 delle identità e degli accessi per Amazon EFS e Controllo dell'accesso di rete ai file system EFS per i client NFS.

> **Note**
>
> L'utilizzo di Amazon EFS con EC2 istanze Amazon 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 Come funziona Amazon EFS.
3. Prova l'esercizio. Nozioni di base

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

- Creazione e gestione di risorse EFS
- Gestione dei file system EFS
- API Amazon EFS

Come funziona Amazon EFS

Amazon Elastic File System (EFS) fornisce un file system semplice, senza server set-and-forget ed elastico. Con Amazon EFS, puoi creare un file system, montare il file system su un' EC2 istanza Amazon e quindi leggere e scrivere dati da e verso il tuo file system. Puoi montare un file system EFS nel tuo cloud privato virtuale (VPC), tramite il protocollo Network File System versioni 4.0 e 4.1 (NFSv4). Ti consigliamo di utilizzare un client Linux NFSv4 .1 di ultima generazione, come quelli disponibili nelle versioni più recenti di Amazon Linux, Amazon Linux 2, Red Hat, Ubuntu e macOS Big AMIs Sur, insieme all'helper di montaggio EFS. Per istruzioni, consultare Installazione del client Amazon EFS.

Per un elenco di Amazon EC2 Linux e macOS Amazon Machine Images (AMIs) che supportano questo protocollo, consulta. Supporto per NFS Per alcuni AMIs, è necessario installare un client NFS per montare il file system sulla propria EC2 istanza Amazon. Per istruzioni, consultare Installazione del client NFS.

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

Per un elenco di Regioni AWS dove è possibile creare un file system EFS, vedere Riferimenti generali di Amazon Web Services.

Per accedere al file system EFS in un VPC, è necessario creare uno o più target di montaggio nel VPC. Una destinazione di montaggio fornisce un indirizzo IP per un NFSv4 endpoint in cui è possibile montare un file system EFS. Il file system viene montato utilizzando il nome DNS (Domain Name Service), che si risolve nell'indirizzo IP della destinazione di montaggio 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. Quindi tutte le EC2 istanze in quella zona di disponibilità condividono la destinazione di montaggio.

> **Note**
>
> Un file system EFS può avere destinazioni di montaggio in un solo 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. Per ulteriori informazioni sugli obiettivi di montaggio, vedereGestione dei target di montaggio.

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 Utenti, gruppi e autorizzazioni a livello di Network File System (NFS).

Puoi montare i tuoi file system EFS sui server dei data center locali quando sei connesso al tuo Amazon VPC AWS Direct Connect con o. AWS VPN Puoi montare i tuoi file system EFS su server locali per migrare set di dati su EFS, abilitare scenari di cloud bursting o eseguire il backup dei dati locali su Amazon EFS.

Di seguito, puoi trovare una descrizione del modo in cui Amazon EFS funziona con altri servizi.

Argomenti

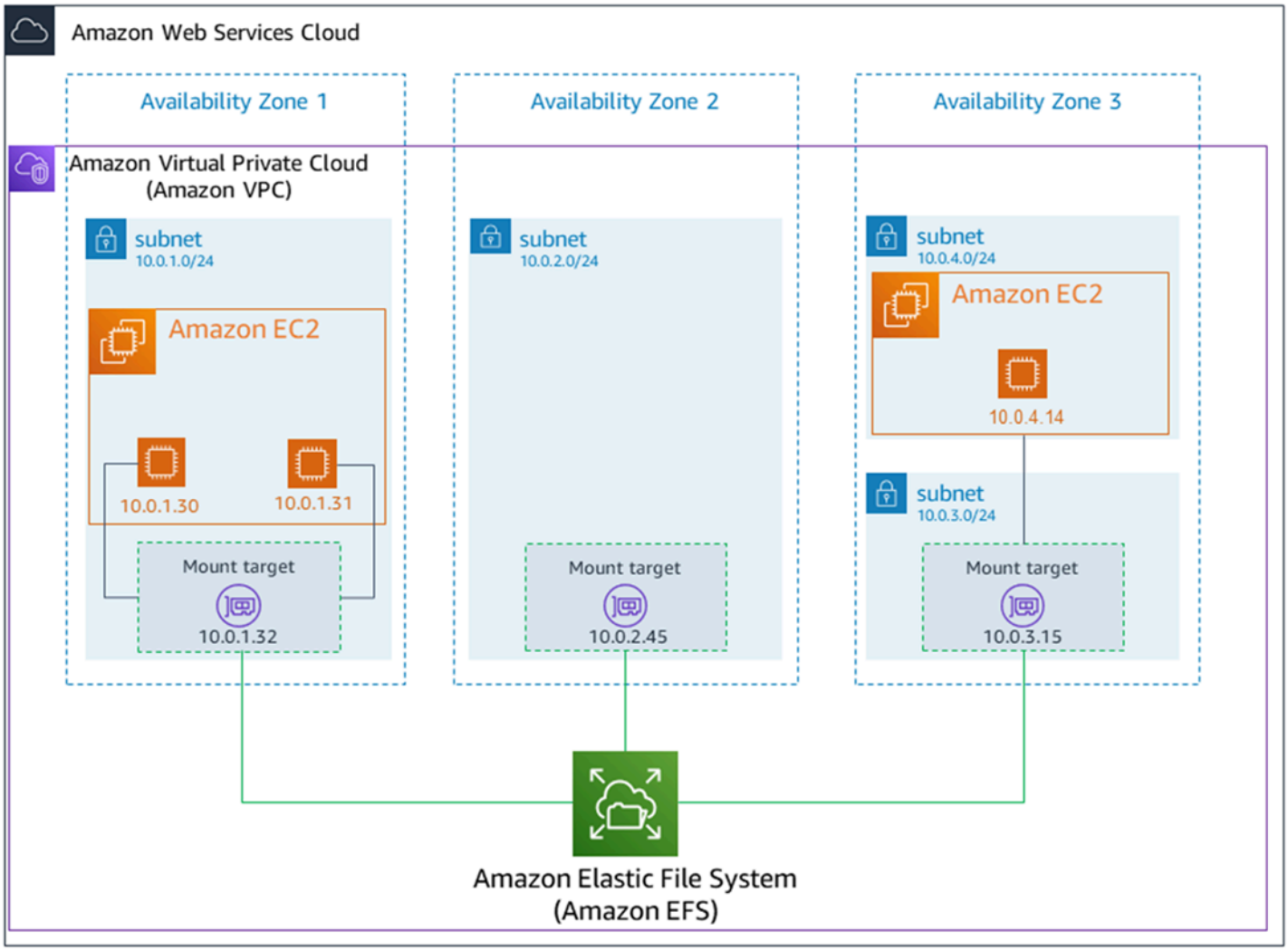
- Come funziona Amazon EFS con Amazon EC2
- Come funziona Amazon EFS con AWS Direct Connect e AWS Managed VPN
- Come funziona Amazon EFS con AWS Backup

Come funziona Amazon EFS con Amazon EC2

Questa sezione spiega come i file system Amazon EFS Regional e One Zone vengono montati su EC2 istanze in un Amazon VPC.

File system EFS regionali

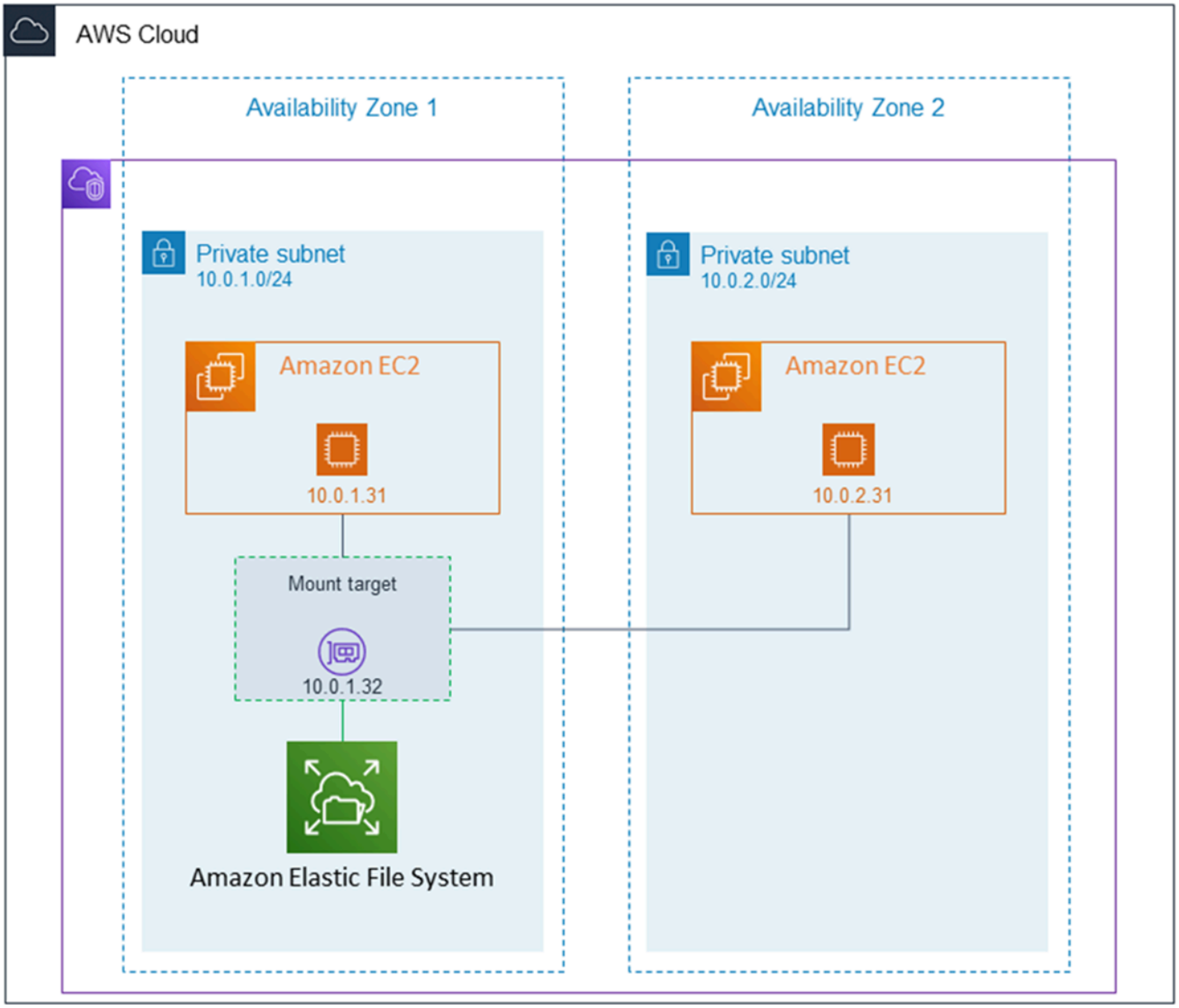
La seguente illustrazione mostra più EC2 istanze che accedono a un file system Amazon EFS configurato per più zone di disponibilità in un. Regione AWS



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 Montaggio dei file system EFS utilizzando l'helper di montaggio EFS.

File system EFS a zona singola

La seguente illustrazione mostra più EC2 istanze che accedono a un file system One Zone da diverse zone di disponibilità in un'unica istanza. 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, si consiglia di accedere al file system da una destinazione di montaggio nella stessa zona di disponibilità dell' EC2 istanza su cui lo si sta montando.

In questo esempio, l' EC2 istanza nella zona di disponibilità us-west-2c pagherà i costi di accesso ai EC2 dati 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 AWS Managed VPN

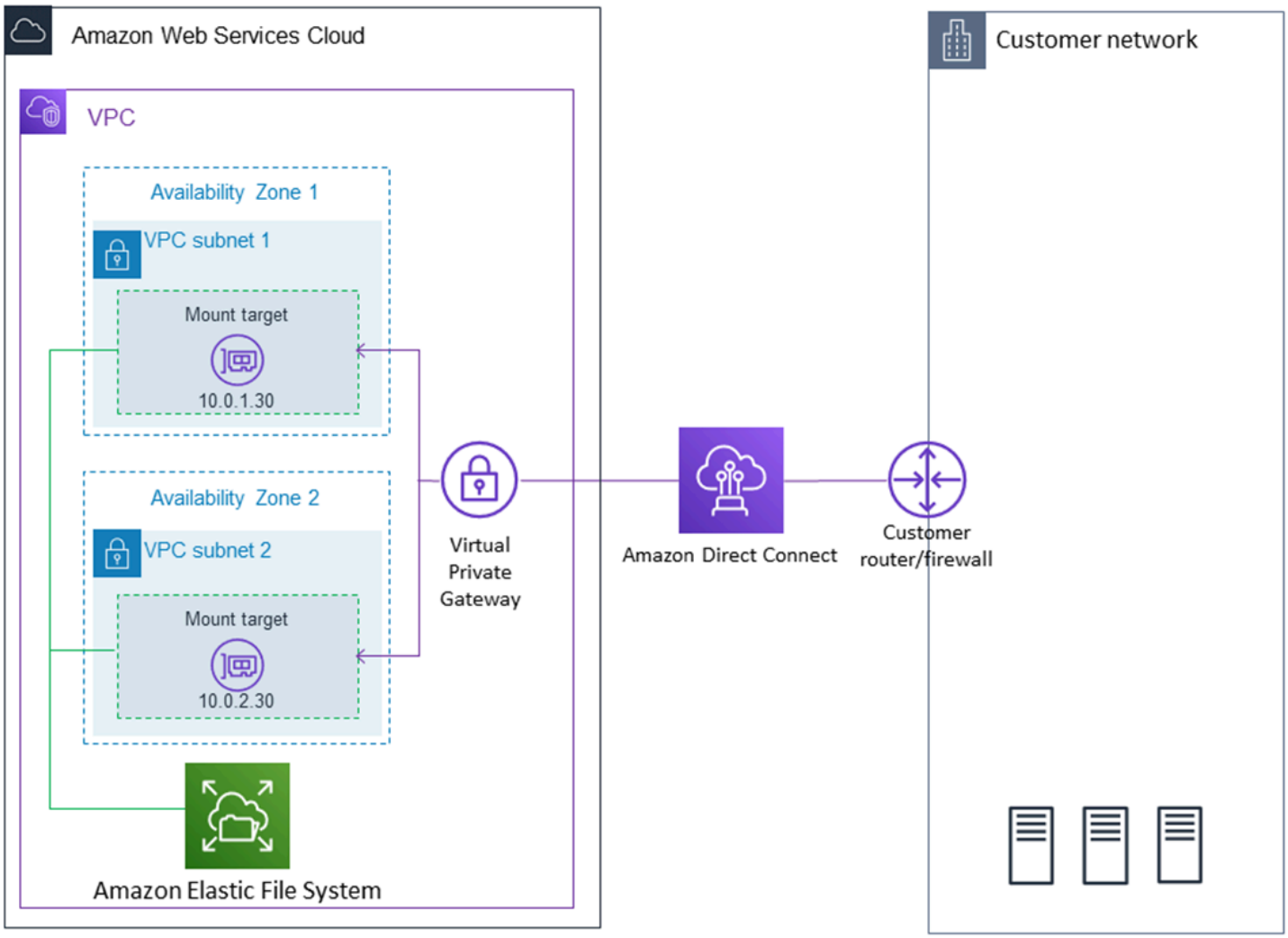
Utilizzando un file system Amazon EFS montato su un server locale, puoi migrare i dati locali verso quelli Cloud AWS ospitati in un file system Amazon EFS. È inoltre possibile usufruire del bursting. In altre parole, puoi spostare i dati dai tuoi server locali in Amazon EFS e analizzarli su una flotta di EC2 istanze Amazon nel tuo Amazon VPC. 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. Ti viene addebitato il costo della AWS Direct Connect connessione al tuo Amazon VPC. 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).



Puoi utilizzare qualsiasi target di montaggio nel tuo VPC se riesci a raggiungere la sottorete di tale destinazione di montaggio utilizzando una AWS Direct Connect connessione 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 Prerequisiti.

Come funziona Amazon EFS con AWS Backup

Per un'implementazione di backup completa per i tuoi file system, puoi utilizzare Amazon EFS con AWS Backup. AWS Backup è un servizio di backup completamente gestito che semplifica la centralizzazione e l'automazione del backup dei dati tra i AWS servizi nel cloud e in locale. Utilizzando AWS Backup, è possibile configurare centralmente le politiche di backup e monitorare l'attività di backup delle risorse. AWS 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, vedereBackup dei file system EFS.

Caratteristiche di Amazon EFS

Di seguito sono elencate le funzionalità di Amazon EFS.

Argomenti

- Autenticazione e controllo degli accessi
- Coerenza dei dati in Amazon EFS
- Disponibilità e durabilità dei file system EFS
- Replica

Autenticazione e controllo degli accessi

È necessario disporre di credenziali valide per utilizzare la console di gestione Amazon EFS e per effettuare richieste API Amazon EFS, ad esempio creare un file system. Inoltre, è necessario disporre delle autorizzazioni per creare o accedere ad altri EFS e AWS 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 delle identità e degli accessi per Amazon EFS.

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 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 read/write le operazioni 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.

Disponibilità e durabilità dei file system 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 della stessa. 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 un'unica zona di disponibilità. 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	99,999999999% (11 9 s)	99,99%	1	Non resiliente

Tipo di file system	Sviluppato per	Durabilità (in base alla progettazione)	Disponibilità	Zone di disponibilità	Altre considerazioni
	durabilità e disponibilità.				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. Nella tabella seguente sono elencati i file system One Zone Regione AWS e AZ IDs per ogni zona di disponibilità in cui è possibile utilizzare i file system One Zone. Per vedere la mappatura di AZ IDs alle zone di disponibilità nel tuo account, consulta la sezione Zona di disponibilità IDs 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	AZ supportato IDs
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

Regione AWS Nome	Regione AWS Codice	AZ supportato IDs
Asia Pacifico (Seul)	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
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

Regione AWS Nome	Regione AWS Codice	AZ supportato IDs
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.

Confronto delle classi di storage

La tabella seguente confronta le classi di storage. Per ulteriori dettagli sulle prestazioni di ogni classe di storage, vedi Specifiche prestazionali di 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	Durata di archiviazione minima
EFS Standard	Dati attivi che richiedono prestazioni di latenza inferiori al millisecondo	Meno di millisecondo	99,999999999% (11 anni e 9)	99,99% (regionale) 99,9% (una zona)	=>3 (regionale)	Non applicabile	Non applicabile
Accesso non frequente a EFS	Dati inattivi a cui si accede solo poche volte ogni trimestre.	Decine di millisecondi			1 (Una zona)	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

[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 alle 12:00 PT del 26 novembre 2023 inseriranno i file di dimensioni inferiori a 128 KB nella classe IA. Per ulteriori informazioni su come Amazon EFS contabilizza e fattura singoli file e metadati, consulta. In che modo Amazon EFS riporta le dimensioni dei file system e degli oggetti

Fatturazione per classi 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 archiviazione 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. In che modo Amazon EFS riporta le dimensioni dei file system e degli oggetti

Ulteriori considerazioni sulla fatturazione si applicano a seconda della modalità di throughput.

- Per i file system che utilizzano Elastic Throughput, viene fatturata la quantità totale mensile di metadati e dati trasferiti per i file system, indipendentemente dai costi di archiviazione.
- 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 su AWS Backup Amazon EFS, consultaBackup dei file system EFS.

Gestione del ciclo di vita

Per gestire i tuoi 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 del ciclo di vita dello storage.

Replica

Puoi creare una replica del tuo file system Amazon EFS nella modalità che Regione AWS preferisci utilizzando la replica. La replica replica in modo automatico e trasparente i dati e i metadati del file system EFS in un nuovo file system EFS di destinazione creato in un Regione AWS file system EFS di tua scelta. EFS mantiene automaticamente sincronizzati i file system di origine e destinazione. La replica è continua e progettata per fornire un obiettivo del punto di ripristino (RPO) 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 EFS.

Guida introduttiva ad Amazon EFS

Se utilizzi Amazon Elastic File System (Amazon EFS) per la prima volta, completa i seguenti passaggi per iniziare con il tuo primo file system EFS.

1. Rivedi i prerequisiti per iniziare
2. Crea il tuo file system EFS e avvia la tua EC2 istanza
3. Trasferisci i file sul tuo file system EFS utilizzando AWS DataSync
4. Pulisci le risorse e proteggi il tuo account AWS

Prerequisiti

Prima di completare la procedura introduttiva, assicurati di avere i seguenti requisiti:

- Sei configurato con Amazon EC2 e conosci bene le EC2 istanze di avvio. È necessario un Account AWS utente con accesso amministrativo, una key pair e un gruppo di sicurezza. Per ulteriori informazioni, consulta la sezione Guida introduttiva ad Amazon EC2 nella Amazon EC2 User Guide.
- Le tue risorse Amazon Virtual Private Cloud (Amazon VPC) ed EFS sono tutte uguali Regione AWS e hai un VPC predefinito nella regione. EC2 Se non disponi di un VPC predefinito o se desideri montare il tuo file system da un nuovo VPC con gruppi di sicurezza nuovi o esistenti, consulta. Utilizzo dei gruppi di sicurezza VPC
- Non è stata modificata la regola di autorizzazione in ingresso predefinita per il gruppo di sicurezza di predefinito.

Puoi anche eseguire un esercizio introduttivo simile utilizzando i comandi AWS Command Line Interface (AWS CLI) per effettuare chiamate all'API EFS. Per ulteriori informazioni, consulta Tutorial: creare un file system EFS e montarlo su un' EC2 istanza utilizzando il AWS CLI.

Crea il tuo file system EFS e avvia la tua EC2 istanza

Dopo esserti assicurato di disporre dei prerequisiti per questo esercizio introduttivo, puoi creare il file system EFS e avviare l' EC2 istanza. Il modo più rapido per completare tutti i passaggi necessari per iniziare a utilizzare il primo file system EFS consiste nell'utilizzare la EC2 nuova procedura guidata di avvio durante l'avvio dell'istanza.

> **Note**
>
> Non puoi usare Amazon EFS con istanze basate su Microsoft Windows EC2 .

Per creare il file system EFS e avviare l' EC2 istanza utilizzando la procedura guidata di EC2 avvio

Per istruzioni sulla creazione e il montaggio del file system EFS durante la creazione del lancio di un' EC2 istanza, consulta Use Amazon EFS with Amazon EC2 nella Amazon EC2 User Guide.

Di seguito sono riportati i passaggi da eseguire durante la creazione di un file system EFS durante l'avvio dell'istanza.

1. Crea un' EC2 istanza in esecuzione su un sistema operativo Linux utilizzando la coppia di key pair e le impostazioni di rete che scegli.
2. Crea un file system EFS condiviso con le impostazioni consigliate e montato automaticamente sull' EC2 istanza.
3. Avvia l' EC2 istanza in modo che il file system EFS sia immediatamente disponibile per i trasferimenti di file.

In alternativa, nella console Amazon EFS, puoi creare file system con impostazioni consigliate o impostazioni personalizzate. Puoi anche utilizzare la AWS CLI e l'API per creare file system. Per ulteriori informazioni su tutte le opzioni disponibili per la creazione di un file system, consultaCreazione di file system EFS.

Trasferisci i file sul tuo file system EFS utilizzando AWS DataSync

Dopo aver creato un file system EFS, è possibile trasferire file su di esso da un file system esistente utilizzando AWS DataSync. DataSync è un servizio di trasferimento dati che semplifica, automatizza e accelera lo spostamento e la replica dei dati tra sistemi di storage locali e servizi di archiviazione su AWS Internet o. AWS Direct Connect DataSync può trasferire i dati dei file e anche i metadati del file system come proprietà, timestamp e autorizzazioni di accesso.

Per ulteriori informazioni su DataSync, consulta AWS DataSync.

Prerequisiti

Prima di trasferire i file sul file system EFS, assicurati di 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. I file system di esempio includono quelli che si trovano in un data center locale, i file system in-cloud autogestiti e i file system EFS.
- Sei configurato per l'uso. DataSync Per ulteriori informazioni, consulta la sezione Guida introduttiva AWS DataSync nella Guida AWS DataSync per l'utente.

Per trasferire file sul file system EFS utilizzando AWS DataSync

Per istruzioni sull'utilizzo per DataSync trasferire file su un file system EFS, consulta Trasferimento dei dati con AWS DataSync nella Guida per l'AWS DataSync utente.

Di seguito sono riportati i passaggi da eseguire durante il trasferimento di file al file system EFS utilizzando DataSync.

1. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
2. Scarica, distribuisci e attiva un agente nel tuo ambiente.
3. Creare e configurare una posizione di origine e di destinazione.
4. Creare e configurare un'attività.
5. Eseguire l'attività per trasferire i file dall'origine alla destinazione.

Pulisci le risorse e proteggi il tuo account AWS

Al termine di questo esercizio introduttivo, esegui i seguenti passaggi per ripulire le risorse e proteggere le tue Account AWS.

Eliminazione delle risorse e protezione dell'account

1. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
2. Disinstalla il file system Amazon EFS con il seguente comando.

```
$ sudo umount efs
```

3. Apri la console Amazon Elastic File System all'indirizzo https://console.aws.amazon.com/efs/.
4. Eliminare il file system EFS creato nel primo passaggio dell'esercizio introduttivo.

a. Scegli il file system EFS che si desidera eliminare dall'elenco dei file system.
b. In Azioni, seleziona Elimina file system.
c. Nella finestra di dialogo Eliminazione definitiva del file system, immetti l'ID del file system Amazon EFS da eliminare e scegli Elimina file system.

5. Termina l' EC2 istanza che hai avviato per questo esercizio introduttivo. Per istruzioni, consulta Terminare le EC2 istanze Amazon nella Guida per l'AWS IAM Identity Center utente.
6. Se hai creato un gruppo di sicurezza per questo esercizio introduttivo, eliminalo. Per istruzioni, consulta Eliminare un gruppo di sicurezza nella Guida AWS IAM Identity Center per l'utente.

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

Installazione del client Amazon EFS

Ti consigliamo di installare il client Amazon EFS (`amazon-efs-utils`), una raccolta di strumenti open source per Amazon EFS. Il client Amazon EFS include un mount helper, un programma che aiuta a semplificare il montaggio dei file system EFS. Il client consente inoltre di utilizzare Amazon per CloudWatch monitorare lo stato di montaggio di un file system EFS e include strumenti che semplificano l'esecuzione della crittografia dei dati in transito per i file system Amazon EFS.

Puoi installare manualmente il client Amazon EFS su istanze Amazon EC2 (EC2) che eseguono distribuzioni supportate. Per alcuni sistemi operativi supportati, puoi in alternativa AWS Systems Manager configurare l'installazione o l'aggiornamento automatico del pacchetto. Per un elenco delle distribuzioni utilizzabili AWS Systems Manager, consultaSistemi operativi supportati da Systems Manager.

> **Important**
>
> Ti consigliamo di utilizzare sempre la versione più recente di `amazon-efs-utils` per garantire l'accesso a tutte le sue funzionalità. Ad esempio, il montaggio con IPv6 indirizzi è supportato nelle versioni 2.3 o successive, ma non nelle versioni precedenti.

Argomenti

- Dipendenze per gli strumenti EFS
- Distribuzioni supportate
- Installazione manuale del client Amazon EFS
- Installazione o aggiornamento automatico del client Amazon EFS tramite AWS Systems Manager
- Installazione e aggiornamento botocore
- Aggiornamento di stunnel
- Attivazione della modalità FIPS

Dipendenze per gli strumenti 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 si utilizza l'helper di montaggio EFS con Transport Layer Security (TLS), l'helper di montaggio impone il controllo del nome host del certificato. L'helper di montaggio EFS utilizza il `stunnel` programma 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 queste versioni di Linux, il montaggio di un file system EFS tramite TLS non riesce.

Dopo aver installato il `amazon-efs-utils` pacchetto, aggiorna stunnel. Consultare 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 EC2 istanze. Per ulteriori informazioni, consulta Installazione o aggiornamento automatico del client Amazon EFS tramite AWS Systems Manager.

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 (2AL2)	rpm	`systemd`

Distribuzione	Tipo di pacchetto	Sistema **`init`**
CentOS 8	rpm	`systemd`
Amazon Linux (1AL1) 2017.09 **Note** AL1 L'AMI ha raggiunto il 31 end-of-life dicembre 2023 e non è supportato per `amazon-efs-utils` i pacchetti rilasciati ad aprile 2024 o versioni successive (versione 2.0 e successive).	rpm	`upstart`
Debian 11	deb	`systemd`
Fedora 29-32	rpm	`systemd`
macOS Big Sur		`launchd`
macOS Monterey		`launchd`
macOS Ventura		`launchd`
macOS Sonoma		`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, 22.04 LTS	deb	`systemd`

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

Installazione manuale del client Amazon EFS

Puoi installare manualmente il client Amazon EFS su istanze Amazon EC2 (EC2) Linux e su istanze EC2 Mac che eseguono macOS Big Sur, macOS Monterey e macOS Ventura. Per un elenco delle distribuzioni che supportano il client Amazon EFS, consulta Distribuzioni supportate

Le procedure di installazione per i sistemi operativi supportati sono descritte nelle seguenti sezioni.

Argomenti

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

Installazione del client Amazon EFS su istanze Amazon EC2 Linux

Il `amazon-efs-utils` pacchetto per l'installazione su istanze Amazon EC2 Linux dalle seguenti posizioni:

- I repository di pacchetti Amazon Machine Images (AMI) per Amazon Linux. Le seguenti istruzioni riguardano l'installazione del `amazon-efs-utils` pacchetto dagli archivi dei pacchetti AMI.
- Il AWS efs-utils GitHub repository. Per ulteriori informazioni sull'installazione del `amazon-efs-utils` pacchetto da GitHub, vedereInstallazione del client Amazon EFS su altre distribuzioni Linux.

> **Note**
>
> - Se lo stai usando AWS Direct Connect, puoi trovare le istruzioni di installazione inPrerequisiti.
> - L'AMI Amazon Linux 1 (AL1) ha raggiunto il 31 end-of-life dicembre 2023 e non è supportata per `amazon-efs-utils` i pacchetti rilasciati ad aprile 2024 e versioni successive (versione 2.0 e successive). Ti consigliamo di aggiornare le applicazioni ad Amazon Linux 2023 (AL2023), che include supporto a lungo termine fino al 2028.

Per installare il **`amazon-efs-utils`** pacchetto dal repository di pacchetti AMI su istanze EC2 Linux

1. Assicurati di aver creato un' EC2 istanza AL2 023 o Amazon Linux 2 (AL2). Per informazioni su come eseguire questa operazione, consulta la Fase 1: Avvio di un'istanza.
2. Accedi al terminale dell'istanza utilizzando SSH (Secure Shell) e accedi con il nome utente opportuno. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
3. Per installare il pacchetto `amazon-efs-utils`, esegui il comando seguente.

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

Installazione del client Amazon EFS su altre distribuzioni Linux

Se non desideri scaricare il `amazon-efs-utils` pacchetto dagli archivi di pacchetti AMI di Amazon Linux, 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 AL2 023, Amazon Linux 2, Red Hat Linux, CentOS e simili.
- DEB - Questo tipo di pacchetto è supportato da Ubuntu, Debian e simili.

Per istruzioni sull'installazione del `amazon-efs-utils` pacchetto per altre distribuzioni Linux, consulta Su altre distribuzioni Linux nel README su Github. `amazon-efs-utils`

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

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

Per istruzioni sull'installazione del `amazon-efs-utils` pacchetto su istanze Mac, consulta Sulla distribuzione macOS Big Sur, macOS Monterey, macOS Sonoma e macOS Ventura nel README su Github. `amazon-efs-utils`

Passaggi successivi

Dopo l'installazione sull' EC2 istanza, procedi con i `amazon-efs-utils` 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 o aggiornamento automatico del client Amazon EFS tramite AWS Systems Manager

Puoi utilizzarlo AWS Systems Manager per semplificare la gestione del client Amazon EFS (`amazon-efs-utils`). AWS Systems Manager è un AWS servizio che puoi usare per visualizzare e controllare la tua infrastruttura AWS. Con AWS Systems Manager puoi automatizzare le attività richieste per installare o aggiornare il `amazon-efs-utils` pacchetto sulle tue istanze Amazon EC2 (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 di mantenimento delle EC2 istanze in uno stato definito.

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 tue EC2 istanze Amazon utilizzando Systems Manager, vengono eseguite le seguenti azioni:

- Viene installato il pacchetto `botocore` utilizzando gli stessi passaggi descritti in Installazione e aggiornamento `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 dei tentativi di montaggio riusciti e falliti.
- Per EC2 le istanze in esecuzione `RHEL7` o`CentOS7`, il client Amazon EFS si 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 da Systems Manager

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

Piattaforma	Versione della piattaforma	Architettura
Amazon Linux 2023 (AL2023)	AL2023	x86_64, arm64 (processori Graviton2 o successivi)
Amazon Linux (2AL2)	2.0	x86_64, arm64 (Amazon Linux 2, tipi di istanza A1)
Amazon Linux (1AL1)	2017.09, 2018.03	x86_64

> **Note**
>
> L'AMI Amazon Linux 1 (AL1) ha raggiunto il 31 end-of-life dicembre 2023 e non è supportata per `amazon-efs-utils` i pacchetti rilasciati ad aprile 2024 e versioni

Piattaforma	Versione della piattaforma	Architettura
successive (versione 2.0 e successive). Ti consigliamo di aggiornare le applicazioni ad Amazon Linux 2023 (AL2023), che include supporto a lungo termine fino al 2028.		
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)

Configurazione AWS Systems Manager per l'installazione del client EFS

Sono necessarie due configurazioni monouso per configurare Systems Manager in modo che installi o aggiorni 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 di istanza è un contenitore che trasmette le informazioni sul ruolo IAM a un'istanza Amazon EC2 (EC2) al momento del lancio.

Utilizza la politica 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 di istanza per avviare le EC2 istanze. Per ulteriori informazioni, consulta la pagina Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager.

Passaggio 2: Configurare un'associazione utilizzata da State Manager

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

Utilizzando State Manager, puoi installare o aggiornare il `amazon-efs-utils` pacchetto sulle EC2 istanze gestite immediatamente o in base a una pianificazione. Inoltre, puoi assicurarti che `amazon-efs-utils` venga installato automaticamente su nuove EC2 istanze. 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 Targets, l'impostazione consigliata è Scegli tutte le istanze per registrare tutte le EC2 istanze nuove ed esistenti come destinazioni per installare o aggiornare automaticamente Amazon.

EFSUtils 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 EC2 istanze con i tag per consentire a AWS Systems Manager di installare o aggiornare automaticamente il client Amazon EFS.

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

Per utilizzarli AWS Systems Manager per montare i file system EFS su più EC2 istanze, vedereMontaggio di EFS su più EC2 istanze .

Installazione e aggiornamento **`botocore`**

Il client Amazon EFS viene utilizzato `botocore` per interagire con altri AWS servizi. È necessario se si desidera monitorare il successo o il fallimento dei tentativi di montaggio per i file system EFS in CloudWatch Logs. Per ulteriori informazioni, consulta Monitoraggio dei tentativi di montaggio riusciti e falliti.

Per istruzioni sull'installazione e l'aggiornamento`botocore`, consulta Installazione `botocore` nel `amazon-efs-utils` README su Github.

Aggiornamento di **`stunnel`**

La crittografia dei dati in transito con l'helper di montaggio EFS richiede la `OpenSSL` versione 1.0.2 o successiva, e una versione `stunnel` che supporta sia l'Online Certificate Status Protocol (OCSP) che il controllo del nome host del certificato. L'helper di montaggio EFS utilizza il `stunnel` programma 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 queste distribuzioni Linux, il montaggio di un file system EFS tramite TLS non riesce.

Dopo aver installato l'EFS mount helper, puoi aggiornare la versione di stunnel del tuo 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. Sostituisci *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 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 in esecuzione. 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.

Risoluzione dei problemi con l'installazione di stunnel

Se non riesci a installare stunnel, prova a disabilitare il controllo del nome host del certificato. Inoltre, offri la massima sicurezza possibile abilitando l'Online Certificate Status Protocol (OCSP).

Argomenti

- Disabilitazione della verifica del certificato associato al nome dell'host
- Abilitazione di OCSP (Online Certificate Status Protocol)

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, Amazon EFS monitora continuamente lo stato dei certificati ed emette nuovi certificati per 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 EFS TLS venga revocato, Amazon pubblica un bollettino sulla sicurezza e rilascia una nuova versione di EFS mount helper 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
```

Attivazione della modalità FIPS

Se il tuo sistema operativo utilizza gli endpoint FIPS (Federal Information Processing Standards) durante il montaggio del file system, devi abilitare la modalità FIPS nel client Amazon EFS. L'attivazione della modalità FIPS comporta la modifica del `efs-utils.conf` file sul sistema operativo.

> **Note**
>
> La modalità FIPS richiede che la versione installata di OpenSSL sia compilata con FIPS. Per ulteriori informazioni su come configurare OpenSSL con FIPS, consulta OpenSSL FIPS README.

Per abilitare la modalità FIPS nel client Amazon EFS

1. Accedi al terminale per la tua EC2 istanza Amazon tramite Secure Shell (SSH) e accedi con il nome utente appropriato. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon Elastic Compute Cloud User Guide.
2. Utilizzando un editor di testo a scelta, aprire il file `/etc/amazon/efs/efs-utils.conf`.
3. Trova la riga contenente il testo seguente:

   ```
   "fips_mode_enabled = false"
   ```
4. Cambia il testo nel modo seguente:

   ```
   "fips_mode_enabled = true"
   ```
5. Salvare le modifiche.

Creazione e gestione di risorse 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 EC2 istanze Amazon. Il file system è accessibile anche da tutte le zone di disponibilità in Regione AWS cui è stato creato.

Puoi montare un file system Amazon EFS su EC2 istanze nel tuo cloud privato virtuale (VPC) basato su Amazon VPC utilizzando le versioni 4.0 e 4.1 del protocollo Network File System (). NFSv4 Per ulteriori informazioni, consulta Come funziona Amazon EFS.

Ad esempio, supponiamo di avere una o più EC2 istanze lanciate nel tuo 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 destinazioni di montaggio per il file system: per accedere al file system nel tuo VPC e montare il file system sulla tua EC2 istanza Amazon, devi creare destinazioni di montaggio nelle sottoreti VPC.
- Crea gruppi di sicurezza: sia un' EC2 istanza Amazon che un target di montaggio devono avere gruppi di sicurezza associati. 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 Mount Target che consenta l'accesso da un' EC2 istanza specifica. Quindi, puoi montare il file system solo su quell' EC2 istanza.

Argomenti

- Riepilogo dell'implementazione
- Risorsa IDs
- Token di creazione e idempotenza
- Creazione di file system EFS
- Eliminazione dei file system EFS
- Creazione di policy del file system

- Creazione di access point
- Eliminazione dei punti di accesso
- Etichettatura delle risorse EFS
- Tutorial: creazione di sottodirectory scrivibili per utente

Riepilogo dell'implementazione

In Amazon EFS, la risorsa principale è un file system. Ogni file system ha proprietà quali ID, token di creazione, ora di creazione, dimensione del file system in byte, numero di destinazioni di montaggio create per il file system e politiche del ciclo di vita del file system.

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 nel 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 Amazon EFS. Supponiamo che tu crei una `efs-mount-point` sottodirectory dalla tua home directory sull'istanza o sul server locale. EC2 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 Gestione dei target di montaggio.
- 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.

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 (CLI) di Amazon EFS - Per un esempio, consulta Tutorial: creare un file system EFS e montarlo su un' EC2 istanza utilizzando il AWS CLI.
- È inoltre possibile gestire queste risorse in modo programmatico come segue:
  - Usa AWS SDKs : AWS SDKs semplifica le tue attività di programmazione eseguendo il wrapping dell'API Amazon EFS 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.
  - Chiama l'API Amazon EFS direttamente dalla tua applicazione: se SDKs per qualche motivo non puoi utilizzarla, puoi effettuare chiamate all'API Amazon EFS direttamente dalla tua applicazione. Tuttavia, scegliendo questa opzione è necessario scrivere il codice di autenticazione delle richieste. Per ulteriori informazioni sull'API Amazon EFS, consulta API Amazon EFS.

Risorsa IDs

Amazon EFS assegna identificatori di risorsa univoci (IDs) a tutte le risorse EFS al momento della creazione. Tutte le risorse EFS IDs sono costituite da un identificatore di risorsa e da una combinazione di cifre da 0 a 9 e lettere minuscole a—f.

Prima di ottobre 2021, le risorse di destinazione IDs assegnate al file system e mount appena create utilizzavano 8 caratteri dopo il trattino (ad esempio,). `fs-12345678` Da maggio 2021 a ottobre 2021,

abbiamo modificato questi tipi IDs di risorse in modo da utilizzare 17 caratteri dopo il trattino (ad esempio,`fs-1234567890abcdef0`). A seconda di quando è stato creato il tuo account, potresti avere un file system e montare le risorse di destinazione con short IDs, ma tutte le nuove risorse di questo tipo riceveranno quelle più lunghe IDs. L'ID della risorsa non cambia mai.

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"
```

Creazione di file system EFS

È possibile creare un file system quando si crea una nuova istanza di EC2 avvio, come spiegato nell'esercizio Guida introduttiva. Tuttavia, puoi anche creare file system utilizzando la console Amazon EFS, AWS Command Line Interface (AWS CLI) o l'API Amazon EFS.

Quando crei il file system utilizzando la console Amazon EFS, hai diverse opzioni, a seconda che desideri che il file system utilizzi le impostazioni consigliate o se desideri personalizzare le impostazioni.

- Puoi utilizzare Quick create per creare rapidamente un file system con le seguenti impostazioni consigliate.
  - Disponibilità regionale
  - Criteri del ciclo di vita per la transizione del file system allo storage EFS Infrequent Access (IA) dopo 30 giorni, allo storage EFS Archive dopo 90 giorni e non alla transizione allo storage EFS Standard
  - La crittografia dei dati inattivi è abilitata
  - Modalità di trasmissione elastica
  - Modalità prestazionale per scopi generici
  - Monta le destinazioni configurate in ogni zona di disponibilità Regione AWS in cui viene creato il file system utilizzando una sottorete disponibile IPv4 sulla sottorete specificata
- È possibile utilizzare Personalizza per creare un file system con le impostazioni scelte.

Per una tabella che elenca le impostazioni del file system e i valori consigliati, vedereOpzioni di configurazione per i file system.

Autorizzazioni IAM richieste per la creazione di file system

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 delle identità e degli accessi per Amazon EFS.

Opzioni di configurazione per i file system

I file system EFS sono configurati con le impostazioni elencate nella tabella seguente.

- Se si utilizza la creazione rapida per creare il file system, il file system viene creato con il valore consigliato indicato per l'impostazione.
- Se si utilizza Personalizza per creare un file system personalizzato, è possibile modificare il valore consigliato per l'impostazione.

Dopo aver creato il file system, è possibile personalizzare le impostazioni del file system ad eccezione del tipo di file system, della crittografia e della modalità di prestazioni.

Impostazioni del file system EFS

Impostazione	Descrizione
Tipo di file system	Consigliato: regionale Il tipo di file system determina la disponibilità e la durabilità con cui un file system EFS archivia i dati all'interno di un file Regione AWS. • I file system regionali archiviano dati e metadati in modo ridondante in tutte le zone di disponibilità all'interno di un. Regione AWSÈ possibile creare inoltre target di montaggio per ogni zona di disponibilità in Regione AWS. Regionale offre i massimi livelli di disponibilità e durabilità. • I file system One Zone archiviano dati e metadati in modo ridondante all'interno di un'unica zona di disponibilità. I file system One Zone possono avere una sola destinazi one di montaggio. Questa destinazione di montaggio deve trovarsi nella stessa zona di disponibilità in cui viene creato il file system. **Note** I file system One Zone sono disponibi li solo per determinate zone di disponibilità. Per ulteriori informazioni sui tipi di file system, consulta Disponibilità e durabilità dei file system EFS.

Impostazione	Descrizione
Gestione del ciclo di vita	Consigliato: passaggio allo storage IA dopo 30 giorni e allo storage Archive dopo 90 giorni. Non passare allo storage Standard. La gestione del ciclo di vita utilizza le policy del ciclo di vita per spostare automaticamente i file da e verso la classe di storage Infrequen t 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. • Transizione all'archivio impostata su 90 giorni dall'ultimo accesso. • Transizione a standard impostato su Nessuno. Quando crei un file system utilizzando l' AWS CLI API Amazon EFS oppure AWS SDKs, non puoi impostare una policy del ciclo di vita contemporaneamente. 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 sulla gestione del ciclo di vita, consulta Gestione del ciclo di vita dello storage.

Impostazione	Descrizione
Crittografia dei dati inattivi	Consigliato: abilitato Amazon EFS utilizza la tua AWS Key Management Service chiave di servizio EFS (`aws/elasticfilesystem`) per crittografare i dati inattivi per impostazione predefinita.AWS KMS Con la crittografia, tutti i dati e i metadati memorizzati su di esso sono crittografati. 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. Per ulteriori informazioni sulla crittografia in Amazon EFS consulta Crittografia dei dati in Amazon EFS.

Impostazione	Descrizione
modalità Throughput	Consigliato: Elastic È possibile scegliere tra le seguenti modalità di throughput: • Elastico: fornisce un throughput scalabile automaticamente verso l'alto e verso il basso in tempo reale, per soddisfare le esigenze di prestazioni del carico di lavoro. • Provisioned: specifica la quantità di throughput desiderata, indipendentemente dalle dimensioni del file system. • Bursting: fornisce un throughput scalabile in base alla quantità di dati nello storage Standard. **Note** Alla modalità di Throughput Elastic e con provisioning sono associati dei costi aggiuntivi. Per ulteriori informazioni, consulta Prezzi di Amazon EFS. Per ulteriori informazioni sulle modalità di throughput, vedere. Modalità di velocità di trasmissione effettiva

Impostazione	Descrizione
Modalità Performance	Consigliato: uso generico La modalità di prestazioni General Purpose ha la latenza per operazione più bassa ed è consigliata per tutti 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 I/O modalità Max non è supportata per i file system One Zone o per i file system che utilizzano la velocità effettiva elastica. **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.

Impostazione	Descrizione
Accesso alla rete	Consigliato: monta la destinazione creata in ogni zona di disponibilità in cui è disponibile il file system Le impostazioni del target di montaggio sono le seguenti: • VPC: è possibile creare destinazioni di montaggio per il file system in un VPC alla volta. Per impostazione predefinita, viene selezionata la sottorete predefinita dell' EC2 istanza. Cambia il VPC se devi accedere al file system da un altro VPC. Se desideri modificare il VPC dopo aver creato il file system successivo, devi prima eliminare le destinazioni di montaggio dal VPC corrente. Per ulteriori informazioni, consulta Modifica del VPC di destinazione del montaggio. • Zona di disponibilità e ID di sottorete: è possibile modificare la zona di disponibilità o la sottorete per la destinazione di montaggio. • Tipo di indirizzo IP: per impostazione predefinita, Amazon EFS utilizza un IPv4 indirizzo in cui creare la destinazione di montaggio. In alternativa, puoi scegliere di supportare IPv6 solo IPv6 gli indirizzi o Dual-stack per supportare entrambi IPv4 gli indirizzi. IPv6 Note Il tipo di indirizzo IP deve corrispon dere al tipo IP della sottorete. Inoltre,

Impostazione	Descrizione
	il tipo di indirizzo IP ha la precedenza sull'attributo di indirizzo IP della sottorete. Ad esempio, se il tipo di indirizzo IP è IPv4 -only e l'attributo di IPv6 indirizzamento è abilitato per la sottorete, le interfacce di rete create nella sottorete ricevono un IPv4 indirizzo dall'intervallo della sottorete. Per ulteriori informazioni, consulta la sezione Modifica dell'attributo di assegnazione degli indirizzi IP della sottorete. • Indirizzo IP: per impostazione predefinita, Amazon EFS crea la destinazione di montaggio a un indirizzo disponibile nella sottorete specificata. In alternativa, puoi specificare l'indirizzo IP per la destinazione di montaggio. Non è possibile modificare l'indirizzo IP di un target di montaggio dopo che è stato creato. È necessario eliminare la destinazione di montaggio e crearne una nuova con il nuovo indirizzo. • Gruppo di sicurezza: il gruppo di sicurezza assegnato alla destinazione VPC viene utilizzato per impostazione predefinita. È possibile aggiungere o rimuovere gruppi di sicurezza. Per ulteriori informazioni sui gruppi di sicurezza, consulta Modifica dei gruppi di sicurezza di Mount Target. Quando crei un file system utilizzando l' AWS CLI API Amazon EFS oppure AWS

Impostazione	Descrizione
	SDKs, non puoi creare un target di montaggio contemporaneamente. È necessario attendere la creazione del file system e quindi utilizzare l'operazione CreateMountTarget API per creare le destinazioni di montaggio. Per ulteriori informazioni sugli obiettivi di montaggio, vedereGestione dei target di montaggio.

Creazione rapida utilizzando la console

Utilizza la console Amazon EFS per creare un file system Amazon EFS con le impostazioni consigliate. Se desideri creare un file system con una configurazione personalizzata, consulta Creazione personalizzata utilizzando la console.

Per creare rapidamente un file system Amazon EFS con le impostazioni consigliate

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. (Facoltativo) Immetti un Nome per il file system.
4. Per cloud privato virtuale (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:

   - Disponibilità regionale
   - Criteri del ciclo di vita per la transizione del file system allo storage EFS Infrequent Access (IA) dopo 30 giorni, allo storage EFS Archive dopo 90 giorni e non alla transizione allo storage EFS Standard
   - La crittografia dei dati inattivi è abilitata
   - Modalità di trasmissione elastica
   - Modalità prestazionale per scopi generici
   - Monta le destinazioni configurate in ogni zona di disponibilità Regione AWS in cui viene creato il file system, utilizzando una subnet disponibile IPv4 sulla sottorete specificata

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 Comprendere lo stato del file system.

Creazione personalizzata utilizzando la console

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 utilizzando le impostazioni consigliate, consultaCreazione rapida utilizzando la console.

La creazione di un file system EFS con impostazioni personalizzate utilizzando la console è un processo 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. 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 impostazione predefinita, per Tipo di file system, è selezionata l'opzione Regionale. Scegliete One Zone se desiderate creare un file system che memorizzi i dati e i metadati del file system in modo ridondante all'interno di un'unica zona di disponibilità. Se scegli Zona singola, seleziona la Zona di disponibilità in cui desideri creare il file system o mantieni il valore predefinito.

   c. Per la Gestione del ciclo di vita, modifica le policy 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 del ciclo di vita dello storage.

   d. Amazon EFS utilizza la tua AWS Key Management Service chiave di servizio EFS (`aws/elasticfilesystem`) per crittografare i dati inattivi 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.

      Non è possibile modificare l'impostazione di crittografia dopo la creazione del file system. Per ulteriori informazioni, consulta Crittografia dei dati in Amazon EFS.

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 throughput massimo in lettura appare come tre volte la quantità di velocità di throughput inserita.

- Per utilizzare il bursting throughput, scegliete Bursting.

Dopo aver scelto la modalità di 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 Crittografia dei dati in Amazon EFS.

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 EC2 le istanze si connettano al tuo file system. Per ulteriori informazioni, consulta Gestione dei target di montaggio.
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.
- Tipo di indirizzo IP: scegli IPv4 solo per supportare solo IPv4 gli indirizzi, solo per supportare IPv6solo IPv6 gli indirizzi o Dual-stack per supportare entrambi gli indirizzi. IPv4 IPv6
- IPv4 o IPv6 indirizzo: se conosci l'indirizzo IP su cui desideri posizionare la destinazione di montaggio, inseriscilo nella casella dell'indirizzo IP corrispondente al tipo di indirizzo IP. Se non specifichi un valore, Amazon EFS seleziona un indirizzo IP inutilizzato dalla sottorete specificata.
- Gruppi di sicurezza: per impostazione predefinita, Amazon EFS sceglie il gruppo di sicurezza predefinito per il VPC. Per modificare il gruppo di sicurezza, elimina il gruppo assegnato e scegli il gruppo dall'elenco Scegli i gruppi di sicurezza. È possibile specificare uno o più gruppi di sicurezza per il target di montaggio. Per ulteriori informazioni, consulta Utilizzo dei gruppi di sicurezza VPC.

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 file system.

1. 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.

2. Usa Grant additional permissions per concedere le autorizzazioni del file system a principali IAM aggiuntivi, incluso un altro. 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.
3. 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.
4. 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 file system per creare il tuo file system e torna 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.

Crea usando il AWS CLI

Quando utilizzi il AWS CLI, crei 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, consultate Prerequisiti per l'utilizzo di AWS CLI nella Guida per l'AWS Command Line Interface utente.

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

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

Ad esempio, il `create-file-system` comando seguente crea un file system utilizzando la velocità effettiva elastica in. `us-west-2`Regione AWS Il comando specifica `MyFirstFS` come token di creazione. Per un elenco delle aree Regioni AWS in cui è possibile creare un file system Amazon EFS, consulta Endpoint e quote Amazon EFS nel. Riferimenti generali di Amazon Web Services

```
aws efs create-file-system \
--creation-token MyFirstFS \
--backup \
--encrypted \
--performance-mode generalPurpose \
--throughput-mode elastic \
--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": "elastic",
    "Tags": [
      {
         "Key": "Name",
         "Value": "Test File System"
      }
   ]
}
```

- L'esempio seguente crea un file system che utilizza il throughput Bursting nella zona di `us-west-2a` 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.

Eliminazione dei file system 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 all'indirizzo https://console.aws.amazon.com/efs/.
2. Scegli il file system che desideri eliminare dalla pagina File system.
3. Scegliere Delete (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.

Usando il AWS 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: pulizia.

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 AWS SDKs 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 file system.

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

Utilizzo della console

1. Apri la console Amazon Elastic File System all'indirizzo 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.
4. Scegli Policy del file system, quindi scegli Modifica.
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 ad altri principali IAM, 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.

Utilizzando il AWS 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 di access point

Puoi creare ed eliminare punti di accesso Amazon EFS utilizzando AWS Management Console, the AWS Command Line Interface (AWS CLI) e l'API Amazon EFS e SDKs. Non è possibile modificare un punto di accesso dopo la sua creazione. Un file system può avere un massimo di 10.000 punti di accesso, a meno che tu non richieda un aumento.

> **Note**
>
> Se più richieste di creazione di punti di accesso sullo stesso file system vengono inviate in rapida successione e il file system si avvicina al limite dei punti di accesso, è possibile che si verifichi una limitazione della risposta a tali richieste. Ciò serve a garantire che il file system non superi il limite di punti di accesso dichiarato.

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

Utilizzo della console

1. Apri la console Amazon Elastic File System all'indirizzo 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.

   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 radice 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 Applicazione di un'identità utente mediante 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.
- Gruppo secondario IDs: inserisci un elenco opzionale separato da virgole di gruppi secondari. IDs

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 radice 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.

Utilizzando il AWS 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 si avvicina al limite dei punti di accesso, è possibile che si verifichi una limitazione della risposta a tali richieste. Ciò serve a garantire che il file system non superi il limite di punti di accesso dichiarato.

Eliminazione dei punti 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.

Utilizzo della console

1. Apri la console Amazon Elastic File System all'indirizzo 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.

Usando il AWS 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
```

Etichettatura delle risorse EFS

Per aiutarti a gestire le tue risorse EFS, puoi assegnare i tuoi metadati 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.

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'uso AWS . 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'uso dei tag per il controllo degli accessi basato su attributi (ABAC).

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.

Utilizzo della console

- 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.

Usando il AWS CLI

- 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

Tutorial: creazione di sottodirectory scrivibili per utente

Dopo aver creato un file system EFS e averlo montato localmente sulla tua istanza Amazon EC2 (EC2), espone una directory vuota chiamata. *`file system root`* Un caso d'uso comune di questa directory principale del file system consiste nel creare una sottodirectory «scrivibile» per ogni utente creato sull' EC2 istanza e montare la sottodirectory nella home directory dell'utente. Tutti i file e le sottodirectory che l'utente crea nella propria home directory vengono quindi creati nel file system EFS.

> **Note**
>
> Puoi seguire l'Nozioni di baseesercizio per creare e montare un file system EFS sulla tua EC2 istanza.

Nei passaggi seguenti, crei un utente, crei una sottodirectory per l'utente, renda l'utente il proprietario della sottodirectory e quindi monti la sottodirectory Amazon EFS nella home directory dell'utente.

1. Creazione dell'utente mike:

   - Accedi alla tua istanza. EC2 Utilizzando i privilegi di root (in questo caso, utilizzando il `sudo` comando), crea l'utente e assegna una password.

     Ad esempio, il comando seguente crea l'utente. `mike`

     ```
     $ sudo useradd -c "Mike Smith" mike
     $ sudo passwd mike
     ```

     Viene inoltre creata una home directory per l'utente. Ad esempio, `/home/mike`.

2. Crea una sottodirectory *`EFSroot`* per l'utente.

   Ad esempio, il comando seguente crea una sottodirectory `mike` in. *`EFSroot`*

   ```
   $  sudo mkdir /EFSroot/mike
   ```

   Dovrete sostituirlo *`EFSroot`* con il nome della directory locale.

3. L'utente root e il gruppo root sono i proprietari della sottodirectory (è possibile verificarlo utilizzando il `ls -l` comando). Per abilitare le autorizzazioni complete per l'utente in questa sottodirectory, concedi la proprietà della directory all'utente.

   Per esempio:

   ```
   $ sudo chown mike:mike /EFSroot/mike
   ```

4. Utilizzate il `mount` comando per montare la sottodirectory nella home directory dell'utente.

   Per esempio:

   ```
   $  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'*`mount-target-DNS`*indirizzo identifica la radice del file system EFS remoto.

Se smonti questo target di montaggio, l'utente non può accedere alla directory senza rimontarlo, il che richiede i permessi di root.

Montaggio dei file system EFS

Per montare i file system EFS, si consiglia di utilizzare l'helper di montaggio EFS. L'helper di montaggio EFS ti aiuta a montare i tuoi file system EFS su istanze EC2 Linux e Mac che eseguono le distribuzioni supportate. Il mount helper fa parte della raccolta di strumenti open source che viene installata quando installi il client Amazon EFS ()`amazon-efs-utils`. Per ulteriori informazioni sul client Amazon EFS e sulle distribuzioni supportate, consultaInstallazione del client Amazon EFS.

In alternativa, è possibile montare manualmente i file system EFS utilizzando il client Linux NFS standard. Amazon EFS supporta i protocolli Network File System versioni 4.0 e 4.1 (NFSv4) per il montaggio dei file system su EC2 istanze Amazon.

Inoltre, è possibile utilizzare EFS mount helper o NFS per configurare un' EC2 istanza in modo che monti automaticamente un file system EFS all'avvio dell'istanza.

Argomenti

- Considerazioni sul montaggio per Linux
- Montaggio dei file system EFS utilizzando l'helper di montaggio EFS
- Utilizzo del Network File System per montare i file system EFS
- Montaggio automatico dei file system EFS
- Smontaggio dei file system
- Tutorial: creare un file system EFS e montarlo su un' EC2 istanza utilizzando il AWS CLI
- Tutorial: montaggio con client Linux locali
- Tutorial: monta un file system da un altro VPC
- Risoluzione dei problemi con il montaggio

Considerazioni sul montaggio per Linux

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 nell'indirizzo IP del target di montaggio EFS nella stessa zona di disponibilità dell' EC2 istanza Amazon senza chiamare risorse esterne. Se utilizzi un target di montaggio in una zona di disponibilità diversa da quella dell' EC2 istanza, dovrai sostenere EC2 costi standard per i dati inviati tra le zone di disponibilità. Potresti anche osservare un aumento delle latenze per le operazioni del file system.
- Per ulteriori opzioni di montaggio e spiegazioni dettagliate delle impostazioni predefinite, consulta la documentazione di Linux.

> **Note**
>
> Se l' EC2 istanza deve essere avviata indipendentemente dallo stato del file system EFS montato, aggiungete l'`nofail`opzione alla voce del file system nel `/etc/fstab` file.

Montaggio dei file system EFS utilizzando l'helper di montaggio EFS

Dopo aver installato il client Amazon EFS (`amazon-efs-utils`), puoi utilizzare l'helper di montaggio EFS per montare i file system EFS sulle tue istanze EC2 Linux e Mac che eseguono distribuzioni supportate. Amazon EFS non supporta il montaggio da istanze EC2 Windows.

> **Important**
>
> Ti consigliamo di utilizzare sempre la versione più recente di `amazon-efs-utils` per garantire il corretto montaggio. Ad esempio, le versioni `amazon-efs-utils` precedenti alla 2.3 non supportano il montaggio con IPv6 indirizzi.

Quando si monta un file system, il mount helper definisce un nuovo tipo di file system di rete, chiamato`efs`, che è completamente compatibile con il `mount` comando standard di Linux. Il mount helper supporta anche il montaggio automatico di un file system EFS all'avvio dell'istanza utilizzando le voci nel file di `/etc/fstab` configurazione sulle 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` manca, l' EC2istanza 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 interfaccia di rete elastica (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 la crittografia dei dati in transito viene dichiarata come opzione di montaggio per il file system EFS, l'helper di montaggio inizializza un `stunnel` processo client e viene chiamato un processo supervisore. `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 `systemd` a seconda della distribuzione 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.

Argomenti

- Impostazioni di montaggio utilizzate dall'helper di montaggio EFS
- Ottenimento dei log per il supporto
- Prerequisiti per l'utilizzo dell'helper di montaggio EFS
- Montaggio su istanze EC2 Linux utilizzando l'helper di montaggio EFS
- Montaggio su istanze EC2 Mac utilizzando l'helper di montaggio EFS
- Montaggio di file system EFS da un altro Regione AWS
- Montaggio dei file system a zona singola
- Montaggio con autorizzazione IAM
- Montaggio con punti di accesso EFS
- Montaggio di EFS su più EC2 istanze
- Montaggio di file system EFS da un altro Account AWS o da un VPC

Impostazioni di montaggio utilizzate dall'helper di montaggio 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 EC2 Mac 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 EC2 Mac che eseguono macOS Big Sur, Monterey e Ventura.

Ottenimento dei log per il supporto

L'EFS mount helper dispone di una registrazione integrata per il file system 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 `amazon-efs-mount-watchdog` processo assicura che il processo stunnel di ogni montaggio sia in esecuzione e interrompe il processo di stunnel quando il file system 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

Puoi montare un file system EFS su un' EC2 istanza Amazon 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 interfaccia di rete elastica (ENI) del target di montaggio senza richiamare risorse esterne.
- Un target di montaggio EFS: crei target di montaggio nel tuo cloud privato virtuale (VPC). 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 Gestione dei target di montaggio.

  > **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 si utilizza un mount target in una zona di disponibilità diversa da quella dell' EC2istanza, vengono EC2 addebitati costi standard per i dati inviati tra le 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:
  - Il nome della zona di disponibilità del file system: se si sta montando un file system EFS One Zone che si trova in una zona di disponibilità diversa rispetto all' EC2 istanza.
  - Nome DNS del target di montaggio: in alternativa, puoi specificare il nome DNS del target di montaggio anziché la zona di disponibilità.

- Un' EC2 istanza che esegue una delle distribuzioni Linux o macOS supportate: le distribuzioni supportate per il montaggio del file system con il mount helper sono le seguenti:
  - Amazon Linux 2
  - Amazon Linux 2023
  - 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**
  >
  > EC2 Le istanze Mac che eseguono macOS Big Sur supportano solo NFS 4.0.

- L'EFS mount helper è installato sull' EC2istanza: il mount helper è uno strumento `amazon-efs-utils` incluso nel pacchetto di utilità. Per informazioni sull'installazione`amazon-efs-utils`, vedere. Installazione del client Amazon EFS
- L' EC2 istanza è in un VPC: l' EC2 istanza di connessione deve trovarsi in un cloud privato virtuale (VPC) basato sul servizio Amazon VPC. Inoltre, deve essere configurata per utilizzare il server DNS fornito da. AWS Per informazioni sul server Amazon DNS, consulta i set di opzioni DHCP in Amazon VPC nella Amazon VPC User Guide.
- Il VPC ha nomi host DNS abilitati: il VPC dell' EC2 istanza di connessione deve avere nomi host DNS abilitati. Per ulteriori informazioni, consulta gli attributi DNS per il tuo VPC nella Amazon VPC User Guide.
- Per EC2 istanze e file system diversi Regioni AWS: se l' EC2 istanza 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 EFS da un altro Regione AWS.

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

Questo processo richiede i seguenti elementi:

- Hai installato il `amazon-efs-utils` pacchetto sull' EC2istanza Amazon. Per ulteriori informazioni, consulta Installazione manuale del client Amazon EFS.

- Sono stati creati dei target di montaggio per il file system. Per ulteriori informazioni, consulta Gestione dei target di montaggio.

Per montare il file system EFS utilizzando il mount helper su istanze EC2 Linux

1. Apri una finestra di terminale sull' EC2 istanza tramite Secure Shell (SSH) e accedi con il nome utente appropriato. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
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' EC2 istanza e il file system che stai montando si trovano in sistemi diversi Regione AWS, consulta Montaggio di file system EFS da un altro Regione AWS per modificare la `region` proprietà nel `efs-utils.conf` file.

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

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

Utilizzate l'ID del file system che state montando al posto di *`file-system-id`* e `efs` al posto 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 del target di montaggio nella zona di disponibilità selezionata con un client NFS.

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

Questo processo richiede i seguenti elementi:

- Hai installato il `amazon-efs-utils` pacchetto sull'istanza Amazon EC2 Mac. Per ulteriori informazioni, consulta Installazione del client Amazon EFS su istanze EC2 Mac che eseguono macOS Big Sur, macOS Monterey o macOS Ventura.

- Sono stati creati dei target di montaggio per il file system. È possibile creare target di montaggio al momento della creazione del file system e aggiungerli ai file system esistenti. Per ulteriori informazioni, consulta Gestione dei target di montaggio.
- 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 che eseguono macOS Big Sur, Monterey e Ventura. Altre versioni di macOS non sono supportate per l'uso con Amazon EFS.

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

1. Apri una finestra di terminale sull'istanza EC2 Mac tramite Secure Shell (SSH) e accedi con il nome utente appropriato. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
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 EC2 Mac, indipendentemente dal fatto che si utilizzi o meno l'`tls`opzione nel comando mount.

   ```
   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, utilizzate l'`notls`opzione, come illustrato 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 EFS da un altro Regione AWS

Per montare il file system EFS da un' EC2 istanza che si trova in un'istanza Regione AWS diversa dal file system, è necessario modificare il valore della `region` proprietà nel `efs-utils.conf` file.

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

1. Accedi al terminale dell' EC2 istanza tramite Secure Shell (SSH) e accedi con il nome utente appropriato. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
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 Fase 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 EFS One Zone supportano solo una singola destinazione 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 EC2 calcolo Amazon che si trova nella stessa zona di disponibilità di quella della destinazione di montaggio del file system.

Questa sezione contiene le procedure seguenti:

- L'hai installato `amazon-efs-utils package` sull' EC2istanza. Per ulteriori informazioni, consulta Installazione del client Amazon EFS.
- Il target di montaggio del file system è stato creato. Per ulteriori informazioni, consulta Gestione dei target di montaggio.

Montaggio dei file system One Zone EC2 in una zona di disponibilità diversa

Se stai montando un file system One Zone su un' EC2 istanza Amazon che si trova in una zona di disponibilità diversa, devi specificare il nome della zona di disponibilità del file system o il nome DNS della destinazione di montaggio del file system nel comando mount helper mount.

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 One Zone su un' EC2 istanza 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 della destinazione di montaggio del file system nella `/etc/fstab` voce.

```
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' EC2 istanza 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.

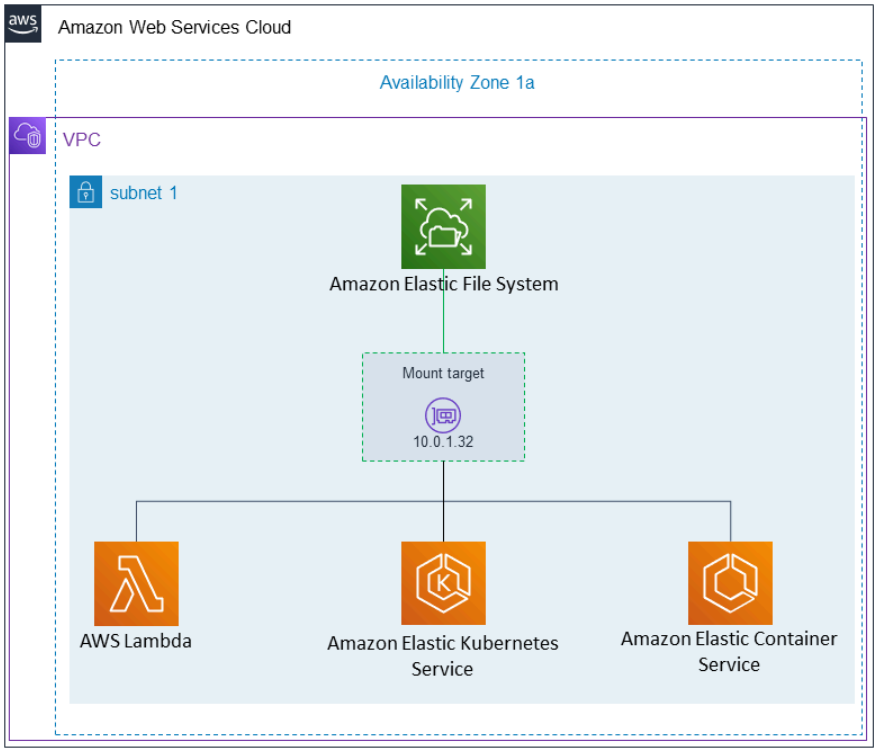
```
availability-zone-name.file-system-id.efs.aws-region.amazonaws.com:/ efs-mount-point
 nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0
```

```
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 Montaggio automatico dei file system EFS.

Montaggio dei file system con il file system One Zone su altre istanze di AWS 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 EFS con Amazon ECS per condividere i dati del file system nella tua flotta di istanze di container in modo che le tue attività abbiano accesso allo stesso storage persistente, indipendentemente dall'istanza su cui atterrano. Per utilizzare i file system EFS One Zone 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 One Zone da Amazon EKS, puoi utilizzare il driver Amazon EFS Container Storage Interface (CSI), che supporta i punti di accesso EFS, per condividere un file system tra più pod in un cluster Amazon EKS o Kubernetes autogestito. Il driver CSI Amazon EFS è installato nello stack Fargate. Quando utilizzi il driver CSI Amazon EFS con i file system EFS One Zone, puoi utilizzare l'`nodeSelector`opzione 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 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 invocazioni solo nelle sottoreti che si trovano nella stessa zona di disponibilità del file system.

Montaggio con autorizzazione IAM

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

È necessario creare una directory da utilizzare come punto di montaggio del file system nelle sezioni seguenti. 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 di EC2 istanza

Se esegui il montaggio con l'autorizzazione IAM su un' EC2 istanza Amazon con un profilo di istanza, utilizza le opzioni `tls` e `iam` mount, illustrate di seguito.

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

Per eseguire il montaggio automatico con l'autorizzazione IAM su un' EC2 istanza con un profilo di istanza, aggiungi la riga seguente al `/etc/fstab` file sull' EC2 istanza.

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

Montaggio con IAM utilizzando un profilo denominato

È possibile eseguire il montaggio con l'autorizzazione IAM utilizzando le credenziali IAM presenti nel file delle AWS CLI credenziali o nel AWS CLI file `~/.aws/credentials` di configurazione. `~/.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 il montaggio automatico con l'autorizzazione IAM su un'istanza Linux utilizzando un file di credenziali, aggiungi la riga seguente al `/etc/fstab` file sull'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 montare automaticamente un file system utilizzando un punto di accesso, aggiungete la riga seguente al `/etc/fstab` file sull' EC2 istanza.

```
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.

Montaggio di EFS su più EC2 istanze

Puoi montare i file system EFS su più EC2 istanze Amazon in remoto e in modo sicuro senza dover accedere alle istanze utilizzando il comando Run. AWS Systems Manager 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 EC2 istanze vengono avviate con un profilo di istanza che include la politica delle `AmazonElasticFileSystemsUtils` 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 EC2 istanze. È possibile utilizzare AWS Systems Manager per installare automaticamente il pacchetto sulle istanze. Per ulteriori informazioni, consulta Passaggio 2: Configurare un'associazione utilizzata da State Manager.

Per montare più file system EFS su più EC2 istanze utilizzando la console

1. Apri 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 EC2 Linux utilizzando l'helper di montaggio EFS o Montaggio su istanze EC2 Mac utilizzando l'helper di montaggio EFS.
7. Seleziona le EC2 istanze 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 EFS utilizzando l'autorizzazione IAM per client NFS e punti di accesso EFS utilizzando 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.

Argomenti

- Montaggio di file system EFS da un altro Account AWS
- Montaggio di file system EFS da un altro VPC

Montaggio di file system EFS da un altro Account AWS

Utilizzando shared VPCs, puoi montare un file system EFS di proprietà di una Account AWS EC2 istanza Amazon appartenente a un'altra Account AWS istanza Amazon. Per ulteriori informazioni sulla configurazione di un VPC condiviso, consulta Condividi il tuo VPC con altri account nella Amazon VPC Peering Guide.

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

Montaggio di file system EFS da un altro VPC

Quando utilizzi una connessione peering VPC o un gateway di transito per connetterti, EC2 le istanze VPCs Amazon che si trovano in un VPC possono accedere ai file system EFS in un altro VPC, anche se appartengono a account diversi. VPCs

Non è possibile utilizzare la risoluzione dei nomi DNS per i punti di montaggio EFS in un altro VPC. Per montare il file system EFS, utilizzare l'indirizzo IP dei punti di montaggio nella zona di disponibilità corrispondente.

In alternativa, puoi utilizzare Amazon Route 53 come servizio DNS. In Route 53, è possibile risolvere gli indirizzi IP di destinazione del mount EFS da un altro VPC creando una zona ospitata privata e

un set di record di risorse. Per ulteriori informazioni su come eseguire questa operazione, consulta Working with private hosted zones nella Amazon Route 53 Developer Guide.

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 Installazione del client Amazon EFS.
- Consenti l'azione `ec2:DescribeAvailabilityZones` nella policy IAM per il ruolo IAM che hai associato all'istanza. Ti consigliamo di collegare 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:root"},
            "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 utilizzi una connessione peering VPC o un gateway di transito per connetterti, EC2 le istanze VPCs Amazon che si trovano in un VPC possono accedere ai file system EFS in un altro VPC, anche se appartengono a account diversi. VPCs

  Un gateway di transito è un hub di transito di rete che puoi utilizzare per interconnettere le tue reti e quelle locali. VPCs 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 peering VPC è una connessione di rete tra due. VPCs Questo tipo di connessione consente di instradare il traffico tra di essi utilizzando indirizzi privati del protocollo Internet versione 4 (IPv4) o del protocollo Internet versione 6 (IPv6). Puoi utilizzare il peering VPC per connetterti VPCs all'interno dello stesso Regione AWS o tra di essi. Regioni 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. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
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 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.

Montaggio di file system 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`.

Utilizzo del Network File System per montare i file system EFS

Di seguito, scopri come installare il client Network File System (NFS) e come montare il tuo file system Amazon EFS su un' EC2 istanza Amazon. 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**
>
> 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 Installazione del client Amazon EFS.

Argomenti

- Prerequisiti

- Supporto per NFS
- Installazione del client NFS
- Impostazioni di montaggio NFS consigliate
- Montaggio su Amazon EC2 con un nome DNS
- Montaggio con un indirizzo IP

Prerequisiti

Prima di montare un file system, assicuratevi di soddisfare i seguenti requisiti:

- Crea, configura e avvia le AWS risorse correlate. Per istruzioni, consultare Guida introduttiva ad Amazon EFS.
- Crea gruppi di sicurezza VPC per le tue EC2 istanze Amazon e monta obiettivi con l'accesso in entrata e in uscita richiesto. Per ulteriori informazioni, consulta Utilizzo dei gruppi di sicurezza VPC.

Supporto per NFS

Amazon EFS supporta i protocolli Network File System versioni 4.0 e 4.1 (NFSv4) per il montaggio dei file system su EC2 istanze Amazon. Sebbene NFSv4 .0 sia supportato, ti consigliamo di utilizzare NFSv4 .1. Il montaggio del file system Amazon EFS sull' EC2 istanza Amazon richiede anche un client NFS che supporti il NFSv4 protocollo 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. Per risolvere i problemi relativi a determinate versioni di AMI o kernel quando si utilizza Amazon EFS da un' EC2 istanza, consulta. Risoluzione dei problemi di AMI e kernel

> **Note**
>
> Il montaggio di file system EFS con EC2 istanze Amazon che eseguono Microsoft Windows non è supportato.

Installazione del client NFS

Per montare il file system EFS sulla tua EC2 istanza Amazon, devi prima installare un client NFS. Per connetterti alla tua EC2 istanza e installare un client NFS, hai bisogno del nome DNS pubblico dell' EC2 istanza e di un nome utente per accedere. Il nome utente per l'istanza è generalmente `ec2-user`.

Per connettere l' EC2 istanza e installare il client NFS

1. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.

   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 Creare una coppia di key pair per la tua EC2 istanza Amazon.
2. (Facoltativo) Scaricare gli aggiornamenti e riavviare.

   ```
   $ sudo yum -y update
              $  sudo reboot
   ```
3. Dopo il riavvio, riconnettiti all'istanza. EC2
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 utilizzi un Amazon EC2 AMI Ubuntu, installa il client NFS con il seguente comando.

```
$ 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 (ovvero se si crea un'AMI personalizzata), è necessario includere almeno il modulo kernel client NFSv4 .1 e l'helper di montaggio dello spazio NFS4 utente corretto.

> **Note**
>
> Se scegli Amazon Linux AMI 2016.03.0 o Amazon Linux AMI 2016.09.0 all'avvio dell'istanza EC2 Amazon, non è necessario `nfs-utils` installarla perché è già inclusa nell'AMI per impostazione predefinita.

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 dei file system EFS

Impostazioni 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' EC2 istanza deve essere avviata indipendentemente dallo stato del file system EFS montato, aggiungete l'`nofail`opzione alla voce del file system nel `/etc/fstab` file.

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 viene risolto nell'indirizzo IP del target di montaggio di 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 della tua EC2 istanza Amazon, dovrai sostenere EC2 costi standard per i dati inviati tra le zone di disponibilità. Potresti anche osservare un aumento delle latenze per le operazioni del file system.
- Per ulteriori opzioni di montaggio e spiegazioni dettagliate delle impostazioni predefinite, consulta la documentazione di Linux.

Montaggio su Amazon EC2 con un nome DNS

> **Note**
>
> Prima di montare il file system, è necessario aggiungere una regola al gruppo di sicurezza Mount Target che consenta l'accesso NFS in entrata dal EC2 gruppo di sicurezza. Per ulteriori informazioni, consulta Utilizzo dei gruppi di sicurezza VPC.

- 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 si risolve automaticamente nell'indirizzo IP del target di montaggio nella zona di disponibilità dell'istanza Amazon connessa. EC2 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, 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 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 Amazon EC2 Mac 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 file-system-id.efs.aws-region.amazonaws.com:/ /efs
```

> **Important**
>
> È necessario utilizzare `mountport=2049` per connettersi correttamente al file system EFS durante il montaggio su istanze EC2 Mac 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' EC2 istanza di connessione deve trovarsi all'interno di un VPC e deve essere configurata per utilizzare il server DNS fornito da Amazon. Per informazioni sul server Amazon DNS, consulta i set di opzioni DHCP in Amazon VPC nella Amazon VPC User Guide.
- Il VPC dell' EC2 istanza di connessione deve avere sia la risoluzione DNS che i nomi host DNS abilitati. Per ulteriori informazioni, consulta gli attributi DNS per il tuo VPC nella Amazon VPC User Guide.

- L' EC2 istanza di connessione 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 Prerequisiti e Tutorial: monta un file system da un altro VPC .

> **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 con il nome DNS, EC2 le istanze Amazon possono montare un file system utilizzando l'indirizzo IP di una destinazione di montaggio. Il montaggio per indirizzo IP funziona in ambienti in cui il DNS è disabilitato, ad esempio VPCs con i nomi host 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 ci si connette a un indirizzo IP di destinazione di montaggio, EC2 le istanze devono essere montate utilizzando l'indirizzo IP di destinazione di montaggio nella stessa zona di disponibilità dell'istanza di connessione.

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, è necessario aggiungere una regola per il gruppo di sicurezza di destinazione di montaggio per consentire l'accesso NFS in entrata dal EC2 gruppo di sicurezza. Per ulteriori informazioni, consulta Utilizzo dei gruppi di sicurezza VPC.

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 all'indirizzo 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 una destinazione di montaggio nel `mount` comando, 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 una destinazione di montaggio nel `mount` comando, 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 utilizzare `mountport=2049` per connettersi correttamente al file system EFS durante il montaggio su istanze EC2 Mac 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

Montaggio automatico dei file system EFS

Puoi utilizzare EFS mount helper o NFS per configurare EC2 un'istanza Amazon per montare automaticamente un file system EFS all'avvio dell'istanza.

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

> **Note**
>
> L'helper di montaggio EFS non supporta il montaggio automatico su istanze EC2 Mac che eseguono macOS Big Sur o Monterey. È invece possibile utilizzare NFS per configurare il file /etc/fstab su un'istanza EC2 Mac per montare automaticamente un file system EFS.

Argomenti

- Attivazione del montaggio automatico su nuove istanze Linux EC2
- Abilitazione del montaggio automatico su istanze Linux esistenti EC2
- Abilitazione del montaggio automatico su istanze EC2 Linux o Mac tramite NFS

Attivazione del montaggio automatico su nuove istanze Linux EC2

Quando crei una nuova istanza EC2 Linux utilizzando l'Amazon EC2 Launch Instance Wizard, puoi configurarla per montare automaticamente il tuo file system Amazon EFS. L' EC2 istanza monta automaticamente il file system al primo avvio dell'istanza e anche ogni volta che viene riavviata.

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`.

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

> **Note**
>
> Non puoi usare Amazon EFS con istanze basate su Microsoft Windows EC2.

Prima di poter avviare e connettersi a un' EC2 istanza, è necessario creare una key pair. Per ulteriori informazioni, consulta le coppie di EC2 chiavi Amazon e EC2 le istanze Amazon nella Amazon EC2 User Guide per creare una coppia di chiavi.

Per configurare l' EC2 istanza per montare automaticamente un file system EFS all'avvio

1. Apri la EC2 console Amazon 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 l' EC2 istanza utilizzerà, che puoi 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 puoi accedere all' EC2 istanza 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' EC2 istanza è ora configurata per montare il file system EFS all'avvio e ogni volta che viene riavviato.

Abilitazione del montaggio automatico su istanze Linux esistenti EC2

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 l'istanza `/etc/fstab` su un'istanza Amazon 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 EFS non supportano il montaggio automatico utilizzando l'helper `/etc/fstab` di montaggio EFS su istanze EC2 Mac che eseguono macOS Big Sur o Monterey. Invece, puoi usare NFS con `/etc/fstab` per montare automaticamente il tuo file system su istanze EC2 Mac 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 `amazon-efs-utils` strumenti sono disponibili per l'installazione su Amazon Linux e Amazon Linux 2 Amazon Machine Images (AMIs). Per ulteriori informazioni su `amazon-efs-utils`, consulta Installazione del client Amazon EFS. 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 EFS che desideri venga rimontato automaticamente. Per ulteriori informazioni, consulta Creazione rapida utilizzando la console.
- 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 Installazione del client Amazon EFS.

Aggiornare il file /etc/fstab

Eseguire i passaggi seguenti per aggiornare /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.

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

1. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
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 il montaggio automatico con l'autorizzazione IAM su un' EC2 istanza con un profilo di istanza, aggiungi la riga seguente al `/etc/fstab` file.

     ```
     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,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` manca, l' EC2 istanza 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.

> **Note**
>
> In alcuni casi, potrebbe essere necessario avviare l' EC2 istanza indipendentemente dallo stato del file system 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 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 per il file system EFS sull' EC2istanza.
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: • _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. • 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. • tls: abilita la crittografia dei dati in transito. • iam— Utilizzate questa opzione per eseguire il montaggio con l'autorizzazione IAM su un' EC2istanza 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 file system. • 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 file system. • accesspoint= *access-point-id* : utilizza questa opzione con l'opzione tls per montare utilizzando un punto di accesso EFS. Per

Campo	Descrizione
	ulteriori informazioni sui punti di accesso EFS, consulta Utilizzo dei punti di accesso.
`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.

Abilitazione del montaggio automatico su istanze EC2 Linux o Mac tramite NFS

Utilizzo di NFS senza l'helper di montaggio EFS per aggiornare EC2 `/etc/fstab` il file Amazon, per istanze EC2 Linux e Mac.

Per aggiornare il **`/etc/fstab`** file sulla tua istanza EC2

1. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
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 Regione AWS quello del 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 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 per il file system EFS sull' EC2istanza.
nfs4	Specifica il tipo di file system.
mount options	L'elenco separato da virgole delle opzioni di montaggio per il file system: • nfsvers=4.1 : specifica l'utilizzo di NFS v4.1. • 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. • 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. • 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. • 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.

Campo	Descrizione
	• `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`: 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.

Smontaggio dei file system

Prima di eliminare un file system, ti consigliamo di smontarlo da ogni EC2 istanza Amazon a cui è connesso. Puoi smontare un file system sulla tua EC2 istanza Amazon eseguendo il `umount` comando sull'istanza stessa. Non è possibile smontare un file system EFS tramite AWS CLI AWS Management Console, il o tramite uno qualsiasi dei AWS SDKs. Per smontare un file system EFS connesso a un' EC2 istanza che esegue Linux, usa il `umount` comando 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 EFS sia stato smontato eseguendo il `df` comando. Questo comando visualizza le statistiche sull'utilizzo del disco per i file system attualmente montati sulla tua istanza Amazon EC2 basata su Linux. Se il file system EFS che si desidera smontare non è elencato nell'output del `df` comando, significa che il file system è smontato.

Example — Identifica lo stato di montaggio di un file system EFS e lo smonta

```
$ 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% /
```

Tutorial: creare un file system EFS e montarlo su un' EC2 istanza utilizzando il AWS CLI

Crea un file system EFS crittografato, montalo su un' EC2 istanza nel tuo VPC e verifica la configurazione utilizzando. AWS CLI

> **Note**
>
> Nel Nozioni di base tutorial, usi la console per creare risorse Amazon EC2 ed EFS. In questo tutorial, userai AWS CLI per fare lo stesso, principalmente per familiarizzare con l'API Amazon EFS.

In questo tutorial, crei le seguenti AWS risorse nel tuo account:

- EC2 Risorse Amazon:
  - Due gruppi di sicurezza (per l' EC2 istanza e il file system EFS).

    È possibile aggiungere regole a questi gruppi di sicurezza per autorizzare un accesso in ingresso e in uscita appropriato. In questo modo è possibile EC2instance connettersi al file system tramite la destinazione di montaggio utilizzando una porta TCP standard NFSv4 1.1.
  - Un' EC2 istanza nel tuo VPC.

- Risorse Amazon EFS:
  - Un file system.
  - Una destinazione di montaggio per il file system.

    Per montare il file system su un' EC2 istanza devi creare una destinazione di montaggio nel tuo VPC. È possibile creare una destinazione di montaggio in ogni zona di disponibilità nella propria VPC. Per ulteriori informazioni, consulta Come funziona Amazon EFS.

Quindi, testate il file system sulla vostra EC2 istanza. La fase di pulizia alla fine del tutorial fornisce informazioni per rimuovere queste risorse.

Il tutorial crea tutte queste risorse nella regione degli Stati Uniti occidentali (Oregon) (`us-west-2`). Qualunque cosa Regione AWS tu usi, assicurati di usarla in modo coerente. Tutte le tue risorse (VPC, EC2 risorse e risorse EFS) devono trovarsi nella stessa unità. Regione AWS

Argomenti

- Prerequisiti
- Configurazione del AWS CLI
- Fase 1: Creare risorse EC2
- Fase 2: Creare risorse EFS
- Passaggio 3: Montare il file system sull' EC2 istanza ed eseguire il test
- Fase 4: pulizia

Prerequisiti

- Puoi utilizzare le tue credenziali root Account AWS per accedere alla console e provare l'esercizio introduttivo. Tuttavia, AWS Identity and Access Management (IAM) consiglia 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. 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 Assegnare Account AWS l'accesso a un utente IAM Identity Center nella Guida per l'AWS IAM Identity Center utente.
- È possibile usare un VPC di default o una VPC personalizzata creata all'interno dell'account. Per questo scenario, va bene la configurazione di default del VPC. Tuttavia, se si utilizza un VPC personalizzata, verificare quanto segue:

  - I nomi host DNS sono abilitati. Per ulteriori informazioni, consulta Attributi DNS per VPC nella Guida per l'utente di Amazon VPC.
  - Il gateway Internet è connesso alla VPC. Per ulteriori informazioni, consulta Collegamento delle sottoreti a Internet tramite un 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, consulta la sezione Indirizzamento IP per le tue sottoreti VPCs e subnet nella Amazon VPC User Guide.
  - La tabella di routing della VPC include una regola per l'invio di tutto il traffico Internet-verso il gateway Internet.
- È necessario configurare AWS CLI e aggiungere il profilo adminuser.

Configurazione del AWS CLI

Utilizzare le seguenti istruzioni per configurare il profilo utente AWS CLI and.

Per configurare il AWS CLI

1. Scarica e configura la AWS CLI. Per istruzioni, consulta la Guida introduttiva AWS CLI alla Guida AWS Command Line Interface per l'utente.
2. Impostazione dei profili.

   Le credenziali utente vengono memorizzate nel AWS CLI `config` file. I comandi CLI di esempio in questo tutorial 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
   ```

Il profilo precedente imposta anche il valore predefinito. Regione AWS Se non si specifica una regione nel comando CLI, viene utilizzata la 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
     ```

Fase 1: Creare risorse 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.
- Avvia un' EC2 istanza. Il passaggio successivo prevede la creazione e il montaggio di un file system EFS su questa istanza.

Fase 1.1. Creazione di due gruppi di sicurezza

In questa sezione, crei gruppi di sicurezza nel tuo VPC per l' EC2 istanza e il target di montaggio EFS. Più avanti nel tutorial, assegnerai questi gruppi di sicurezza a un' EC2 istanza e a un target di montaggio EFS. Per informazioni sui gruppi di sicurezza, consulta Gruppi EC2 di sicurezza Amazon per istanze Linux.

Per creare i gruppi di sicurezza

1. Creare due gruppi di sicurezza tramite il comando CLI `create-security-group`:

a. Crea un gruppo di sicurezza (`efs-walkthrough1-ec2-sg`) per la tua EC2 istanza e fornisci il tuo 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. Crea un gruppo di sicurezza (`efs-walkthrough1-mt-sg`) per il tuo target di montaggio 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:

- Ti consente di connetterti alla tua EC2 istanza.
- Abilita il traffico tra un' EC2 istanza e un target di montaggio EFS (a cui assocerai questi gruppi di sicurezza più avanti in questo tutorial).

Fase 1.2: Aggiungere le regole ai gruppi di sicurezza per autorizzare un 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. Autorizza le connessioni Secure Shell (SSH) in entrata al gruppo di sicurezza dell' EC2 istanza (`efs-walkthrough1-ec2-sg`) in modo da poterti connettere all' EC2 istanza 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. Autorizza l'accesso in entrata al gruppo di sicurezza per il mount target EFS ()`efs-walkthrough1-mt-sg`.

   Al prompt dei comandi, esegui il AWS CLI `authorize-security-group-ingress` comando seguente utilizzando il profilo adminuser per aggiungere la regola in entrata.

```
$ 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
```

Passaggio 1.3: Avviare un'istanza EC2

In questo passaggio, si avvia un' EC2 istanza.

Per avviare un' EC2 istanza

1. Raccogli le seguenti informazioni che devi fornire all'avvio di un' EC2 istanza:

   - Nome della coppia di chiavi. Per istruzioni su come creare una coppia di chiavi, consulta Create a key pair for your Amazon EC2 istance nella Amazon EC2 User Guide.
   - L'ID dell'Amazon Machine Image (AMI) che si desidera avviare.

     Il AWS CLI comando che usi per avviare un' EC2 istanza richiede l'ID dell'Amazon Machine Image (AMI) che desideri distribuire come parametro. L'esercitazione utilizza l'AMI Amazon Linux HVM.

> **Note**
>
> Puoi utilizzare la maggior parte dei sistemi basati su Linux AMIs per scopi generici. 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 l'AMI Amazon Linux HVM, puoi trovare le ultime novità IDs su Amazon Linux AMI. Scegli il valore ID dalla IDs tabella AMI Amazon Linux come segue:

- 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 che hai creato per un' EC2 istanza.
- 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 sottorete - Questo valore è necessario per la creazione della destinazione di montaggio. In questo esercizio, creerete un target di montaggio nella stessa sottorete in cui lanciate un' EC2 istanza.
- Zona di disponibilità della sottorete: questo valore è necessario per creare il nome DNS della destinazione di montaggio, da utilizzare per montare un file system sull'istanza. EC2

2. Esegui il AWS CLI `run-instances` comando seguente 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' EC2 istanza che hai creato deve avere un nome DNS pubblico che usi per connetterti all' EC2 istanza 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 trovi il nome DNS pubblico, controlla la configurazione del VPC in cui hai avviato EC2 l'istanza. Per ulteriori informazioni, consulta Prerequisiti.
5. (Facoltativo) Assegna un nome all' EC2 istanza che hai creato. 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, eseguite il AWS CLI `create-tags` comando seguente.

   ```
   $  aws ec2 create-tags \
   --resources  EC2-instance-ID \
   --tags Key=Name,Value=Provide-instance-name  \
   --region us-west-2 \
   --profile adminuser
   ```

Fase 2: Creare risorse EFS

In questa fase si effettuano le operazioni seguenti:

- Crea un file system EFS crittografato.
- Abilitare la gestione del ciclo di vita.
- Crea un target di montaggio nella zona di disponibilità in cui è stata lanciata l'istanza EFS.

Fase 2.1: Creare un file system EFS

In questo passaggio, si crea un file system 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. Al prompt dei comandi, esegui il seguente comando AWS `create-file-system` CLI.

  ```
  $  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: creazione di una destinazione di montaggio.

Fase 2.2: abilitare la gestione del ciclo di vita

In questa fase, si abilita la gestione del ciclo di vita sul file system per utilizzare la classe di storage EFS Infrequent Access (IA). Per ulteriori informazioni, consultare Gestione del ciclo di vita dello storage e Classi di storage EFS.

Come abilitare la gestione del ciclo di vita

- Al prompt dei comandi, esegui il comando seguente. 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: creazione di una destinazione di montaggio

In questo passaggio, crei una destinazione di montaggio per il file system nella zona di disponibilità in cui è stata lanciata l' EC2 istanza.

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.
   - ID di sottorete VPC in cui è stata avviata l' EC2 istanza. Fase 1: Creare risorse EC2

     Per questo tutorial, si crea il target di montaggio nella stessa sottorete in cui è stata avviata l' EC2 istanza, quindi è necessario l'ID di sottorete (ad esempio,). `subnet-example`
   - L'ID del gruppo di sicurezza creato per la destinazione di montaggio nella fase precedente.
2. Al prompt dei comandi, esegui il comando seguente. 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
```

Passaggio 3: Montare il file system sull' EC2 istanza ed eseguire il test

In questa fase si effettuano le operazioni seguenti:

- Raccogli le informazioni richieste.
- Installa il client NFS sulla tua EC2 istanza.
- Installa il file system sull' EC2 istanza ed esegui il test.

Argomenti

- Fase 3.1: raccolta delle informazioni
- Passaggio 3.2: installa il client NFS sulla tua istanza EC2
- Passaggio 3.3: installa il file system sull'istanza ed esegui il test EC2

Fase 3.1: raccolta delle informazioni

Assicurarsi di disporre delle seguenti informazioni per procedere con le fasi di questa sezione:

- Nome DNS pubblico dell' EC2 istanza nel seguente formato:

```
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' EC2 istanza su cui si monta il file system utilizzando la destinazione di montaggio può risolvere il nome DNS del file system nell'indirizzo IP della destinazione di montaggio.

> **Note**
>
> Amazon EFS non richiede che l' EC2 istanza abbia un indirizzo IP pubblico o 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.

Passaggio 3.2: installa il client NFS sulla tua istanza EC2

Puoi connetterti alla tua EC2 istanza da Windows o da un computer che esegue Linux, macOS X o qualsiasi altra variante di Unix.

Per installare un client NFS

1. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
2. Esegui i seguenti comandi sull' EC2 istanza utilizzando la sessione SSH:

   a. (Facoltativo) Scaricare gli aggiornamenti e riavviare.

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

   Dopo il riavvio, riconnettiti all'istanza. EC2

   b. Installare il client NFS.

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

   > **Note**
   >
   > Se scegli l'AMI Amazon Linux 2016.03.0 Amazon Linux all'avvio EC2 dell'istanza, non è necessario `nfs-utils` installarla perché è già inclusa nell'AMI per impostazione predefinita.

Passaggio 3.3: installa il file system sull'istanza ed esegui il test EC2

Ora monti il file system sulla tua EC2 istanza.

1. Crea una directory (» efs-mount-point «).

```
$ mkdir ~/efs-mount-point
```

2. Montare il file system 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' EC2 istanza può risolvere il nome DNS del target di montaggio nell'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. Ora che hai il file system EFS montato sulla tua EC2 istanza, puoi creare 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
```

Ora hai creato e montato con successo un file system EFS sulla tua EC2 istanza nel tuo VPC.

Il file system montato non rimane persistente in caso di riavvio. Per rimontare automaticamente la directory, è possibile utilizzare il file `fstab`. Se utilizzi un gruppo Auto Scaling per avviare EC2 le istanze, puoi anche impostare gli script in una configurazione di avvio.

Fase 4: pulizia

Se le risorse create non sono più necessarie, dovrebbero essere eliminate. È possibile farlo tramite la CLI.

- Rimuovi EC2 le risorse (l' EC2 istanza e i due gruppi di sicurezza). Quando si elimina la destinazione di montaggio, Amazon EFS elimina l'interfaccia di rete.
- Rimuovi le risorse EFS (file system, destinazione di montaggio).

Per eliminare AWS le risorse create in questa procedura dettagliata

1. Termina l' EC2 istanza che hai creato per questo tutorial.

```
$ aws ec2 terminate-instances \
--instance-ids instance-id \
```

```
--profile adminuser
```

Puoi anche eliminare EC2 le risorse utilizzando la console. Per le istruzioni, consulta Arresto di un'istanza.

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.

   È necessario eliminare prima il gruppo di sicurezza del target di montaggio, prima di eliminare il gruppo di sicurezza dell' EC2 istanza. Il gruppo di sicurezza del target di montaggio ha una regola che fa riferimento al gruppo EC2 di sicurezza. Pertanto, non è possibile eliminare prima il gruppo di sicurezza dell' EC2 istanza.

   Per istruzioni, consulta Elimina il tuo gruppo di sicurezza nella Amazon EC2 User Guide.

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.

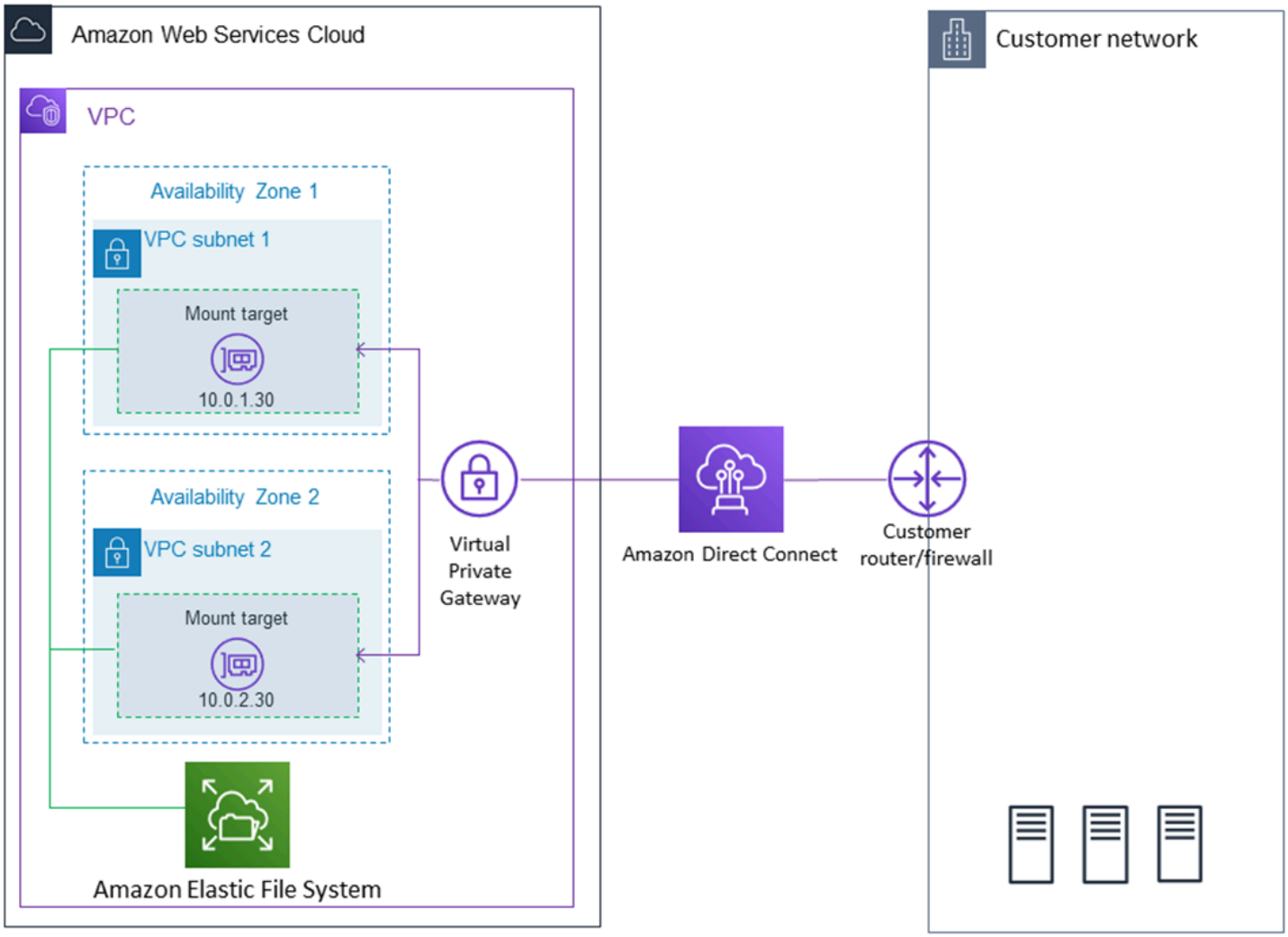
   ```
   aws efs describe-file-systems \
   --profile adminuser \
   --region aws-region
   ```

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
```

Tutorial: montaggio con client Linux locali

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.



> **Note**
>
> L'utilizzo di Amazon EFS con client basati su Microsoft Windows non è supportato.

Argomenti

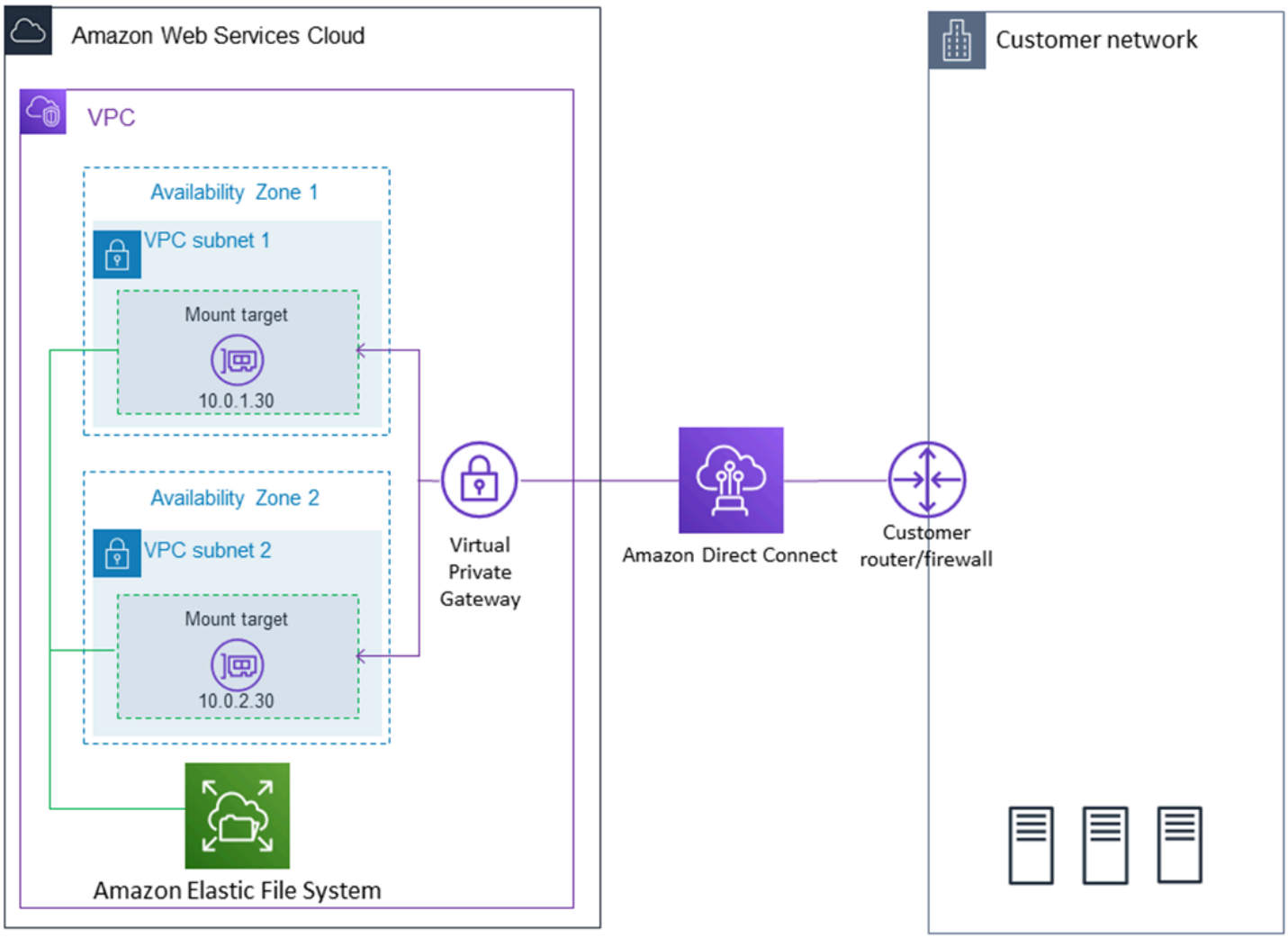
- Prerequisiti
- Fase 1: Crea le tue risorse EFS
- Fase 2: installare il client NFS
- Fase 3: Montare il file system Amazon EFS File System sul client on-premise
- Fase 4: Eliminazione delle risorse e protezione dell'account AWS
- Opzionale: crittografia dei dati in transito

Prerequisiti

Assicurati di disporre già di una connessione AWS Direct Connect o VPN. Per ulteriori informazioni su AWS Direct Connect, consulta la Guida per l'utente di AWS Direct Connect. Per ulteriori informazioni sulla configurazione di una connessione VPN, consulta Connetti il tuo VPC a reti remote utilizzando AWS Virtual Private Network la Amazon VPC User Guide.

Dopo aver stabilito una connessione AWS Direct Connect o VPN, crea un file system 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.

Tutte le risorse dello scenario sono create nella regione 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, la tua destinazione 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, si consiglia di avere due client locali collegati al file system tramite diverse zone di disponibilità (AZs) per una maggiore disponibilità.

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 la sezione Accesso Single Sign-on a Account AWS nella Guida per l'AWS IAM Identity Center utente.

È possibile usare un VPC di default o una VPC personalizzata creata all'interno dell'account. Per questo scenario, va bene la configurazione di default del VPC. Tuttavia, se si utilizza un VPC personalizzata, verificare quanto segue:

- Il gateway Internet è connesso alla VPC. Per ulteriori informazioni, consulta Abilitare l'accesso a Internet per un VPC utilizzando un gateway Internet nella Amazon VPC User Guide.
- 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 EFS

In questo passaggio, creerai il tuo file system EFS e monterai le destinazioni.

Per creare il file system EFS

1. Apri la console Amazon Elastic File System 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. Seleziona 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 Gestione dei target di montaggio.
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 si indica un gruppo di sicurezza durante la creazione di una destinazione di

montaggio, Amazon EFS associa ad essa il gruppo di sicurezza predefinito del VPC. 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). Puoi usare il AWS Management Console per aggiungere la regola ai gruppi di sicurezza del tuo target di montaggio nel tuo VPC.

Per permettere al traffico in entrata di raggiungere la porta NFS

1. Accedi a AWS Management Console e apri la EC2 console Amazon 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 EFS.
4. Nel riquadro a schede visualizzato sotto l'elenco dei gruppi di sicurezza, scegliere la scheda Inbound (In ingresso).
5. Scegli 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.

Fase 2: installare 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: Montare il file system Amazon EFS File System sul client on-premise

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. A tale scopo, utilizza uno strumento basato su

terminali, ad esempio `ping` confrontando l'indirizzo IP delle EC2 istanze in diverse zone di disponibilità, per trovare quella con la latenza più bassa.

- 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 il file system Amazon EFS è stato montato, è possibile testarlo con la procedura seguente.

Per verificare la connessione del file system Amazon EFS

1. Spostarsi nella nuova cartella appena creata con il seguente comando.

```
$ cd ~/efs
```

2. Crea una sottodirectory e trasferisci la proprietà di quella sottodirectory all'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
```

> **Warning**
>
> In caso di montaggio automatico del file system, utilizzare l'opzione `_netdev`, usata per identificare i file system di rete. Se `_netdev` manca, l' EC2istanza 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: Eliminazione delle risorse e protezione dell'account AWS

Al completamento di questo scenario, oppure qualora non si desideri esplorare gli scenari aggiuntivi, è necessario seguire questi passaggi per eliminare le risorse e proteggere l'account AWS .

Per ripulire le risorse e proteggere le Account AWS

1. Smontare il file system Amazon EFS con il seguente comando.

   ```
   $ sudo umount ~/efs
   ```

2. Apri la console Amazon EFS nella console Amazon EFS.
3. Scegli il file system EFS che si desidera eliminare dall'elenco dei file system.
4. In Azioni, seleziona Elimina file system.
5. Nella finestra di dialogo Elimina definitivamente il file system, immettere il file system ID del file system Amazon EFS da eliminare e scegliere Elimina il file system.
6. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
7. Fai clic su Security Groups (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 del 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).

Opzionale: 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 pacchetto amazon-efs-utils è una collezione di strumenti open source per 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 Installazione del client Amazon EFS. Questo pacchetto è disponibile come download gratuito da GitHub, che puoi ottenere clonando l'archivio del pacchetto.

Per 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. Installa 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. Installa 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. Modificare *`{region}`* con l'ID della propria regione AWS , per esempio `us-west-2`.

Per montare il file system EFS sul client locale, aprire un terminale sul client Linux locale. Per montare il file system, è necessario disporre dell'ID del file system, dell'indirizzo IP della destinazione di montaggio per una delle destinazioni di montaggio e della regione Regione AWS del file system.

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. A tale scopo, utilizza uno strumento basato su terminali, ad esempio `ping` confrontando l'indirizzo IP delle EC2 istanze in diverse zone di disponibilità, per trovare quella con la latenza più bassa.

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
```

Tutorial: monta un file system da un altro VPC

In questo tutorial, configurerai un' EC2 istanza per montare un file system EFS che si trova in un altro cloud privato virtuale (VPC). 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 Installazione del client Amazon EFS.

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 si utilizza una connessione peering VPC o un gateway di transito per la connessione VPCs, EC2 le istanze che si trovano in un VPC possono accedere ai file system EFS in un altro VPC, anche se appartengono a account diversi. VPCs

> **Note**
>
> L'utilizzo di Amazon EFS con client basati su Microsoft Windows non è supportato.

Argomenti

- Prerequisiti
- Fase 1: Determinare l'ID della zona di disponibilità del target di montaggio
- Fase 2: Determinare l'indirizzo IP di destinazione del montaggio
- Fase 3: Aggiungere una voce host per la destinazione di montaggio
- Fase 4: Montare il file system utilizzando l'helper di montaggio EFS
- Passaggio 5: ripulisci le risorse e proteggi le Account AWS

Prerequisiti

Per completare questo tutorial, è necessario disporre di quanto segue:

- Il `amazon-efs-utils` set di strumenti viene installato sull' EC2 istanza prima di utilizzare questa procedura. Per istruzioni sull'installazione di `amazon-efs-utils`, vedere Installazione del client Amazon EFS.
- Una delle seguenti:
  - Una connessione peering VPC tra il VPC in cui risiede il file system EFS e il VPC in cui risiede l'istanza. EC2 Una connessione peering VPC è una connessione di rete tra due. VPCs Questo tipo di connessione consente di instradare il traffico tra di essi utilizzando indirizzi privati del protocollo Internet versione 4 (IPv4) o del protocollo Internet versione 6 (IPv6). Puoi utilizzare il peering VPC per connetterti VPCs all'interno dello stesso Regione AWS o tra di essi. Regioni AWS Per ulteriori informazioni, consulta Creazione e accettazione di una connessione peering VPC nella Guida al peering Amazon VPC.
  - Un gateway di transito che collega il VPC in cui risiede il file system EFS e il VPC in cui risiede l'istanza. EC2 Un gateway di transito è un hub di transito di rete che puoi utilizzare per interconnettere le tue reti e quelle locali. VPCs Per ulteriori informazioni, consulta la sezione Guida introduttiva all'uso di Amazon VPC Transit Gateways nella Amazon VPC Transit Gateways Guide.

Fase 1: Determinare l'ID della zona di disponibilità del target di montaggio

Per garantire un'elevata disponibilità del file system, si consiglia di utilizzare sempre un indirizzo IP di destinazione di EC2 montaggio che si trovi nella stessa zona di disponibilità del client NFS. Se si sta montando un file system EFS in un altro account, assicurarsi 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 della zona di disponibilità possono differire da un account all'altro.

Per determinare l'ID della zona di disponibilità dell'istanza EC2

1. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.
2. Determina l'ID della zona di disponibilità in cui si trova l' EC2 istanza 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 proprietà `ZoneId`, `use2-az2`.

Fase 2: Determinare l'indirizzo IP di destinazione del montaggio

Ora che conosci l'ID della zona di disponibilità dell' EC2 istanza, puoi 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 di disponibilità `use2-az2` ha un indirizzo IP 10.0.2.153.

Fase 3: Aggiungere una voce host per la destinazione di montaggio

È ora possibile inserire una voce nel `/etc/hosts` file sull' EC2 istanza che mappa 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. Aggiungi una riga per l'indirizzo IP della destinazione di montaggio al `/etc/hosts` file dell' EC2 istanza. La voce utilizza il formato `mount-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' EC2 istanza e la destinazione di montaggio dispongano di regole che consentano l'accesso al file system EFS, se necessario. Per ulteriori informazioni, consulta Utilizzo dei gruppi di sicurezza VPC.

Fase 4: Montare il file system utilizzando l'helper di montaggio EFS

Per montare il file system EFS, devi prima creare una directory di montaggio sull' EC2 istanza. Quindi, utilizzando l'helper di montaggio EFS, è possibile montare il file system con l'autorizzazione AWS Identity and Access Management (IAM) o con un punto di accesso EFS. Per ulteriori

informazioni, consultare Utilizzo di IAM per controllare l'accesso ai file system e Utilizzo dei punti di accesso.

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 avete montato il file system EFS, potete testarlo con la procedura seguente.

Per testare la connessione del file system EFS

1. Spostarsi nella nuova cartella appena creata con il seguente comando.

```
$ cd ~/mnt/efs
```

2. Crea una sottodirectory e trasferisci la proprietà di quella sottodirectory all'utente dell' EC2istanza. 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 Abilitazione del montaggio automatico su istanze Linux esistenti EC2 .

> **Warning**
>
> In caso di montaggio automatico del file system, utilizzare l'opzione `_netdev`, usata per identificare i file system di rete. Se `_netdev` manca, l' EC2istanza 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 le Account AWS

Dopo aver terminato questo tutorial, esegui i seguenti passaggi per ripulire le tue risorse e proteggere le tue Account AWS.

Per ripulire le risorse e proteggere i tuoi Account AWS

1. Disinstalla il file system Amazon EFS con il seguente comando.

```
$ sudo umount ~/efs
```

2. Apri la console Amazon Elastic File System all'indirizzo https://console.aws.amazon.com/efs/.
3. Scegli il file system EFS che si desidera eliminare dall'elenco dei file system.
4. In Azioni, seleziona Elimina file system.

5. Nella finestra di dialogo Eliminazione definitiva del file system, immetti l'ID del file system Amazon EFS da eliminare e scegli Elimina file system.
6. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
7. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
8. Seleziona il nome del gruppo di sicurezza a cui hai aggiunto la regola per questo tutorial.

   > **Warning**
   >
   > Non eliminare il gruppo di sicurezza predefinito del 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).

Risoluzione dei problemi con il montaggio

Di seguito, sono disponibili informazioni sulla risoluzione dei problemi di montaggio del file system EFS.

Montaggio fallito del file system su un'istanza Windows

Un montaggio del file system su un' EC2 istanza Amazon su Microsoft Windows non riesce.

Operazione da eseguire

Non utilizzare Amazon EFS con EC2 istanze Windows, che non è supportata.

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 stai tentando di montare il file system utilizzando IAM, assicurati di utilizzare l'opzione `-o iam` o -o tls nel comando mount. 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 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` manca, l' EC2 istanza 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 state montando manualmente i file system, il `ExecStart` comando 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 `ExecStart` comando deve puntare a EFS anziché NFS4 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 riavvia l' EC2 istanza Amazon. 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 indica che la tua distribuzione Linux non supporta le versioni di 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 viene restituito il comando precedente`# CONFIG_NFS_V4_1 is not set`, NFSv4 .1 non è supportato nella distribuzione Linux in uso. Per un elenco delle Amazon Machine Images (AMIs) per Amazon Elastic Compute Cloud (Amazon EC2) che supportano la tecnologia NFSv4 1.1, 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.

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 codice, 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 l' EC2 istanza Amazon o i gruppi di sicurezza Mount Target non sono configurati correttamente. Assicurati che il gruppo di sicurezza Mount Target disponga di una regola in entrata che consenta l'accesso NFS dal gruppo EC2 di sicurezza. Per ulteriori informazioni, consulta Utilizzo dei gruppi di sicurezza VPC.

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, è necessario effettuare le seguenti operazioni:

- Assicurati che ci sia un target di montaggio Amazon EFS nella stessa zona di disponibilità dell' EC2 istanza Amazon.
- Assicurati che ci sia un target 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.
- Collega la tua EC2 istanza Amazon all'interno di un Amazon VPC configurato per 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.
- Assicurati che l'Amazon VPC dell' EC2 istanza Amazon connessa abbia i nomi host 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 del sistema dei nomi di dominio (DNS) 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 DNS `efs.<region>.amazonaws.com` 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 Gestione dei target di montaggio.

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 Installazione del client Amazon EFS.

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 Impostazioni 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' EC2 istanza Amazon è stata connessa a un file system e a una destinazione di montaggio con un indirizzo IP specificato e quindi il file system e la destinazione di montaggio sono stati eliminati. Se crei un nuovo file system e monti una destinazione per connetterti a quell' EC2 istanza Amazon con lo stesso indirizzo IP di destinazione di montaggio, questo problema può verificarsi.

Operazione da eseguire

Puoi risolvere questo errore smontando il file system e quindi rimontando il file system 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.

Trasferimento di dati da e verso Amazon EFS

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

AWS Transfer Family è un AWS servizio completamente gestito che puoi utilizzare per trasferire file da e verso i file system Amazon EFS tramite il protocollo 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, consulta Utilizzo AWS Transfer Family per trasferire dati.

Argomenti

- Utilizzo per trasferire dati AWS DataSync
- Utilizzo AWS Transfer Family per trasferire dati

Utilizzo per trasferire dati AWS DataSync

AWS DataSync è un servizio di trasferimento dati online che semplifica, automatizza e accelera lo spostamento e la replica dei dati tra i sistemi di storage locali e anche tra i servizi di archiviazione. AWS DataSync può copiare dati tra Network File System (NFS), file server Message Block (SMB), storage di oggetti autogestito, bucket Amazon AWS Snowball Edge S3, file system EFS FSx e file system Windows File Server.

È inoltre possibile utilizzare DataSync per trasferire file tra due file system Regione AWS EFS, inclusi file system in diversi file system e file system di proprietà di Account AWS s diversi. Utilizzando DataSync per copiare i dati tra i file system EFS, è possibile eseguire migrazioni di dati una tantum, inserire dati periodici per carichi di lavoro distribuiti e automatizzare la replica per la protezione e il ripristino dei dati.

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

Utilizzo AWS Transfer Family per trasferire dati

AWS Transfer Family è un AWS servizio 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 Amazon EFS.

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

> **Note**
>
> L'uso di Transfer Family con Amazon Account AWS EFS è disabilitato per impostazione predefinita per i file system Amazon 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 Supporto.

Argomenti

- Prerequisiti per l'utilizzo AWS Transfer Family con Amazon EFS
- Configurazione del file system EFS per AWS Transfer Family

Prerequisiti per l'utilizzo 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 ai file system EFS.
  - 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 EFS per 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 dei POSIX assegnati IDs agli utenti di Transfer Family.
- Fase 2. Assicurati che le directory del tuo file system siano accessibili agli utenti di Transfer Family utilizzando il POSIX IDs assegnato 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 POSIX IDs assegnato agli utenti Transfer Family. In questo esempio, un utente crea una directory denominata `transferFam` sotto il punto di montaggio di Amazon 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. Connect alla tua EC2 istanza Amazon. Amazon EFS supporta solo il montaggio tramite istanze basate su Linux EC2 .
2. Monta il tuo file system EFS se non è già montato sull' EC2 istanza. 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 IAM `EFS-role-for-transfer`.

```
{
    "Version": "2012-10-17",
    "Id": "efs-policy-wizard-8698b356-4212-4d30-901e-ad2030b57762",
    "Statement": [
```

```
        {
            "Sid": "Grant-transfer-role-access",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/EFS-role-for-transfer"
            },
            "Action": [
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ]
        }
    ]
}
```

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 ai file system EFS.

È possibile concedere un Account AWS accesso diverso al file system nella politica del file system. Nella console Amazon EFS, utilizza la sezione Concedi autorizzazioni aggiuntive dell'editor delle politiche del file system per specificare il 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 su ARNs, consulta IAM ARNs nella IAM User Guide.

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 concede solo privilegi di lettura e scrittura all'account Account AWS 111122223333, che è l'account proprietario del server Transfer Family che necessita dell'accesso a questo file system EFS nel tuo account. `Grant-cross-account-access`

```
{
    "Statement": [
        {
            "Sid": "NFS-client-read-write-via-fsmt",
            "Effect": "Allow",
            "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",
            "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 EFS

Le attività di gestione del file system comprendono la gestione dell'accessibilità di rete di un file system con destinazioni di montaggio, la modifica della modalità di throughput, l'aggiornamento delle politiche relative al ciclo di vita e la gestione della crittografia.

È possibile eseguire queste attività di gestione del file system utilizzando o utilizzando a livello di codice AWS Command Line Interface (AWS CLI) o l'API, come illustrato nelle sezioni seguenti. AWS Management Console

Argomenti

- Comprendere lo stato del file system
- Gestione dei target di montaggio
- Gestione della velocità di trasmissione effettiva del file system
- Gestione del ciclo di vita dello storage
- Gestione dell'accesso ai file system crittografati

Comprendere lo 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.
ELIMINAZIONE IN CORSO	Amazon EFS sta eliminando il file system in risposta a una richiesta di eliminazione avviata dall'utente. Per ulteriori informazioni, consulta Eliminazione dei file system EFS.

Stato del file system	Descrizione
ELIMINATO	Amazon EFS ha eliminato il file system in risposta a una richiesta di eliminazione avviata dall'utente. Per ulteriori informazioni, consulta Eliminazione dei file system 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. 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, consulta Backup e replica dei dati in Amazon EFS

Gestione dei target di montaggio

Monti il tuo file system su Amazon EC2 o un'altra istanza di AWS calcolo nel tuo cloud privato virtuale (VPC) utilizzando uno o più target di montaggio che crei per il file system. Puoi creare la destinazione di montaggio quando crei il file system o dopo aver creato il file system.

Dopo aver creato una destinazione di montaggio per un file system, è possibile creare destinazioni di montaggio aggiuntive, eliminare destinazioni di montaggio e modificare i gruppi di sicurezza per le destinazioni di montaggio. Se desideri modificare il VPC per le destinazioni di montaggio, devi prima eliminare le destinazioni di montaggio esistenti.

> **Note**
>
> Non è possibile modificare l'indirizzo IP di un target di montaggio esistente. Per modificare un indirizzo IP, è necessario eliminare il target di montaggio e crearne uno nuovo con il nuovo indirizzo.

Argomenti

- Monta obiettivi e zone di disponibilità
- Creazione di destinazioni di montaggio
- Eliminazione degli obiettivi di montaggio
- Modifica del VPC di destinazione del montaggio
- Modifica dei gruppi di sicurezza di Mount Target

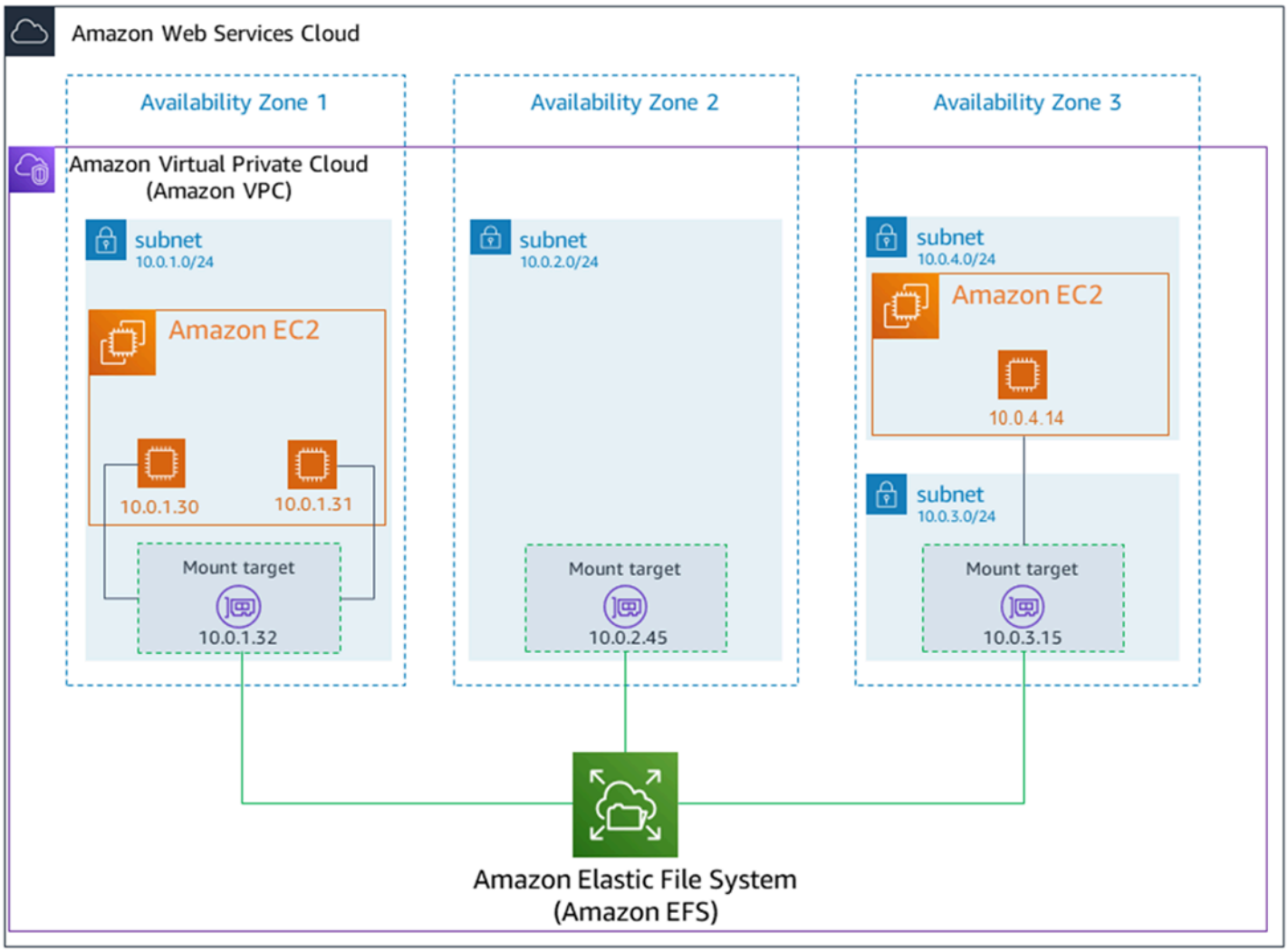
Monta obiettivi e zone di disponibilità

Per i file system EFS che utilizzano classi di storage regionali, è possibile creare un target di montaggio in ogni zona di disponibilità in un Regione AWS.

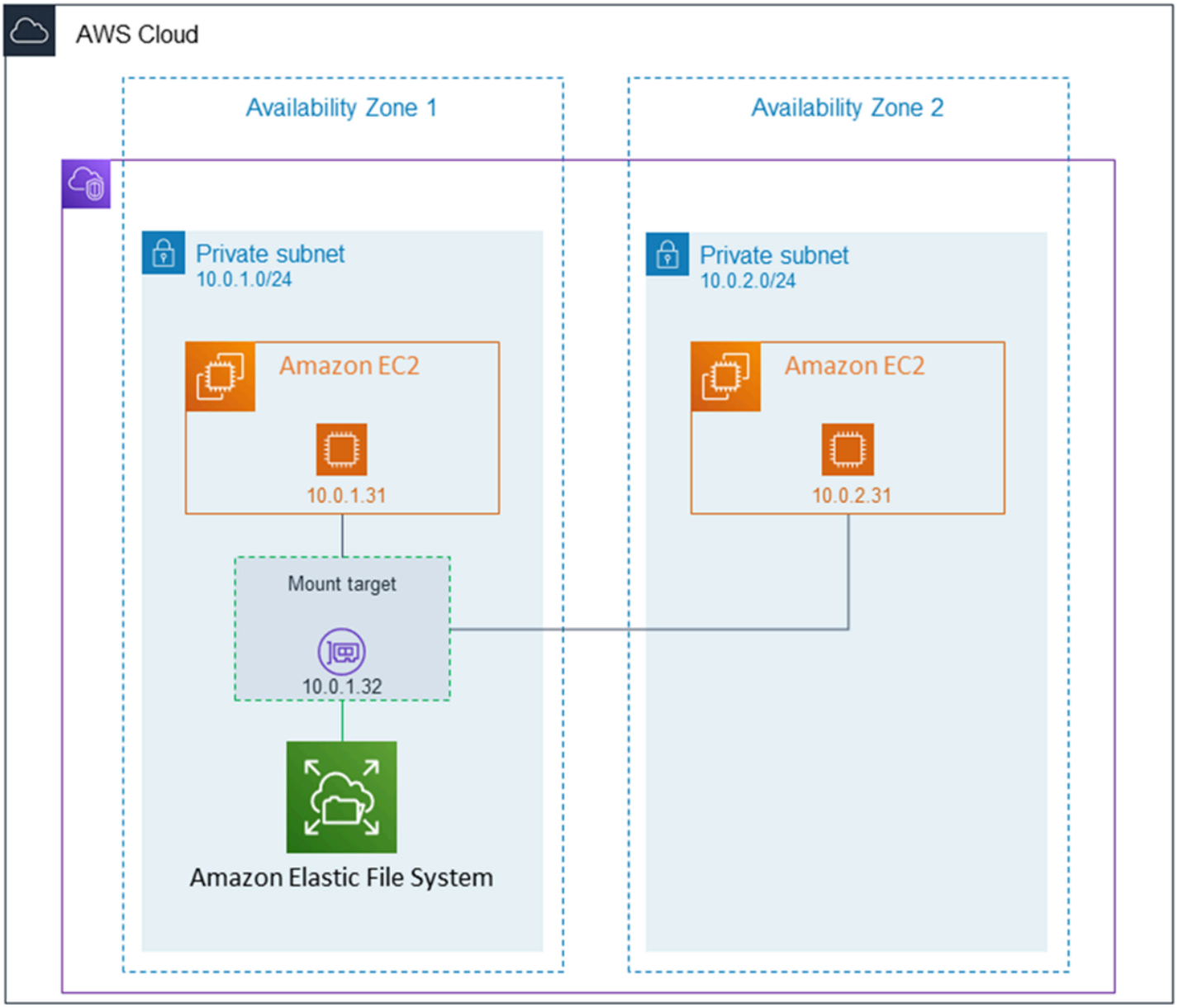
Per i file system a zona singola, è possibile creare un solo target di montaggio nella stessa zona di disponibilità del file system. Quindi puoi montare il file system su istanze di calcolo, tra cui Amazon, EC2 Amazon ECS e AWS Lambda nel tuo cloud privato virtuale (VPC).

Il diagramma seguente mostra un file system regionale con destinazioni di montaggio create in tutte le zone di disponibilità del VPC. L'illustrazione mostra tre EC2 istanze avviate in diverse sottoreti VPC che accedono a un file system 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. Finché è presente un target di montaggio in una zona di disponibilità, EC2 le istanze avviate in una qualsiasi delle relative sottoreti possono condividere lo stesso target di montaggio.



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' EC2 istanza nella zona di `us-west2c` disponibilità comporta costi di accesso ai dati perché l'istanza si trova in una zona di disponibilità diversa rispetto alla destinazione 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' EC2 istanza Amazon 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 Utenti, gruppi e autorizzazioni a livello di Network File System (NFS).

Creazione di destinazioni di montaggio

Per accedere a un file system EFS in un VPC, è necessario creare destinazioni di montaggio per il file system.

Per un file system EFS, vale quanto segue:

- È possibile creare destinazioni di montaggio per il file system in un VPC alla volta. Se desideri accedere al file system da un altro VPC, devi eliminare le destinazioni di montaggio dal VPC corrente e quindi creare nuove destinazioni di montaggio nell'altro VPC. Per ulteriori informazioni, consulta Modifica del VPC di destinazione del montaggio.
- 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 EC2 istanze nella zona di disponibilità possono condividere il singolo target di montaggio.
- Come minimo, è necessario creare un target di montaggio in ogni zona di disponibilità da cui si desidera accedere al file system.

> **Note**
>
> Esistono considerazioni relative ai costi per il montaggio di un file system su un' EC2 istanza in una zona di disponibilità tramite un target di montaggio creato in un'altra zona di disponibilità. Per ulteriori informazioni, consulta la pagina dei prezzi di 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.

Puoi creare destinazioni di montaggio per un file system utilizzando o a livello di codice utilizzando. AWS Management Console AWS CLI AWS SDKs Nella console, è possibile creare destinazioni di montaggio quando si crea il file system o dopo la creazione del file system. Per istruzioni sulla creazione di destinazioni di montaggio durante la creazione di un file system, consultaCreazione personalizzata utilizzando la console.

Utilizzo della console

Utilizzare la procedura seguente per aggiungere destinazioni di montaggio a un file system EFS esistente.

Per creare una destinazione di montaggio su un file system EFS

1. Apri la console Amazon Elastic File System all'indirizzo https://console.aws.amazon.com/efs/.
2. Nel riquadro di navigazione a sinistra, scegli File system, quindi seleziona il file system per il quale desideri modificare il VPC.
3. Scegli Rete, quindi scegli Gestisci per visualizzare le destinazioni di montaggio per il file system.
4. Scegli il file system a cui desideri aggiungere le destinazioni di montaggio selezionandone il nome o l'ID del file system.

> **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.

5. Per i file system che utilizzano le classi di storage EFS Regional, scegli Aggiungi destinazione di montaggio per ogni destinazione di montaggio che desideri creare per il file system.
6. Definite le impostazioni del target di montaggio:

   a. Scegli la zona di disponibilità e l'ID di sottorete per il target di montaggio.

   b. Per il tipo di indirizzo IP, scegli di supportare IPv4 solo IPv4 gli indirizzi, IPv6 solo di supportare solo IPv6 gli indirizzi o Dual-stack per supportare entrambi gli indirizzi. IPv4 IPv6

> **Note**
>
> Il tipo di indirizzo IP deve corrispondere al tipo IP della sottorete. Inoltre, il tipo di indirizzo IP ha la precedenza sull'attributo di indirizzo IP della sottorete. Ad esempio, se il tipo di indirizzo IP è IPv4 -only e l'attributo di IPv6 indirizzamento è abilitato per la sottorete, le interfacce di rete create nella sottorete ricevono un IPv4 indirizzo dall'intervallo della sottorete. Per ulteriori informazioni, consulta la sezione Modifica dell'attributo di assegnazione degli indirizzi IP della sottorete.

c. Se conosci l'indirizzo IP in cui desideri posizionare la destinazione di montaggio, inseriscilo nella casella dell'indirizzo IP corrispondente al tipo di indirizzo IP. Se non specifichi un valore, Amazon EFS seleziona un indirizzo IP inutilizzato dalla sottorete specificata.

> **Note**
>
> Non puoi modificare l'indirizzo IP di un target di montaggio dopo che è stato creato. Per modificare un indirizzo IP, è necessario eliminare la destinazione di montaggio e crearne una nuova con il nuovo indirizzo.

7. Scegliete almeno un gruppo di sicurezza da associare al target di montaggio. È possibile modificare i gruppi di sicurezza in un secondo momento.
8. Scegli Save (Salva).

Usando il AWS CLI

Questa sezione fornisce esempi per la creazione di un target di montaggio AWS CLI utilizzando il `create-mount-target` comando. Il comando API equivalente è CreateMountTarget.

- Se non si specifica un tipo di indirizzo IP per il mount target, viene utilizzato IPv4 -only.
- Se non specifichi un indirizzo IP per la destinazione di montaggio, Amazon EFS assegna un indirizzo disponibile nella sottorete specificata.
- Il tipo di indirizzo IP ha la precedenza sull'attributo di indirizzamento IP della sottorete. Ad esempio, se il tipo di indirizzo IP è IPv4 -only e l'attributo di IPv6 indirizzamento è abilitato per la sottorete, le interfacce di rete create nella sottorete ricevono un IPv4 indirizzo dall'intervallo della sottorete. Per ulteriori informazioni, consulta la sezione Modifica dell'attributo di assegnazione degli indirizzi IP della sottorete.

> **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.

Esempio: crea un target di montaggio su un indirizzo disponibile su una sottorete IPv4

Il comando seguente specifica il file system, la sottorete e il gruppo di sicurezza per la destinazione di montaggio. La destinazione viene creata a un IPv4 indirizzo disponibile nella sottorete specificata.

```
$ 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 \
```

Il seguente esempio mostra il comando con i dati campione.

```
$ aws efs create-mount-target \
--file-system-id fs-0123456789abcdef1 \
--subnet-id  subnet-b3983dc4 \
--security-group sg-01234567 \
--region us-east-2 \
```

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.

```
{
    "OwnerID": "111122223333"
    "MountTargetId": "fsmt-f9a14450",
    "FileSystemId": "fs-0123456789abcdef1",
    "SubnetId": "subnet-b3983dc4",
    "LifeCycleState": "available",
    "IpAddress": "10.0.1.24",
    "NetworkInterfaceId": "eni-3851ec4e",
    "AvailabilityZoneId": "use2-az1",
    "AvailabilityZoneName": "us-east-2a",
    "VpcId": "vpc-3c39ef57"
}
```

Esempio: crea un target di montaggio a un indirizzo specifico IPv4

Il comando seguente specifica il file system, la sottorete, il gruppo di sicurezza e l' IPv4 indirizzo da utilizzare per la destinazione di montaggio. La destinazione viene creata all' IPv4 indirizzo specificato nella sottorete specificata.

```
$ 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 \
--ip-address IPv4-address
--region aws-region \
```

Il seguente esempio mostra il comando con i dati campione.

```
$ aws efs create-mount-target \
--file-system-id fs-0123456789abcdef1 \
--subnet-id  subnet-b3983dc4 \
--security-group sg-01234567 \
--ip-address 10.0.1.24 \
--region us-east-2 \
```

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.

```
{
    "OwnerID": "111122223333"
    "MountTargetId": "fsmt-f9a14450",
    "FileSystemId": "fs-0123456789abcdef1",
    "SubnetId": "subnet-b3983dc4",
    "LifeCycleState": "available",
    "IpAddress": "10.0.1.24",
    "NetworkInterfaceId": "eni-3851ec4e",
    "AvailabilityZoneId": "use2-az1",
    "AvailabilityZoneName": "us-east-2a",
    "VpcId": "vpc-3c39ef57"
}
```

Esempio: crea un target di montaggio a un indirizzo specifico IPv6

Il comando seguente specifica il file system, la sottorete, il gruppo di sicurezza e l' IPv6 indirizzo da utilizzare per la destinazione di montaggio. La destinazione viene creata all' IPv6 indirizzo specificato nella sottorete specificata.

```
$ 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 \
--ip-address-type IP-address-type \
```

```
--ipv6-address IPv6-address \
--region aws-region \
```

Il seguente esempio mostra il comando con i dati campione.

```
$ aws efs create-mount-target \
--file-system-id fs-0123456789abcdef1 \
--subnet-id  subnet-b3983dc4 \
--security-group sg-01234567 \
--ip-address-type IPV6_ONLY \
--ipv6-address 2001:0db8:85a3:0000:0000:8a2e:0370:7334 \
--region us-east-2 \
```

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.

```
{
    "OwnerID": "111122223333"
    "MountTargetId": "fsmt-f9a14450",
    "FileSystemId": "fs-0123456789abcdef1",
    "SubnetId": "subnet-b3983dc4",
    "LifeCycleState": "available",
    "Ipv6Address": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
    "NetworkInterfaceId": "eni-3851ec4e",
    "AvailabilityZoneId": "use2-az1",
    "AvailabilityZoneName": "us-east-2a",
    "VpcId": "vpc-3c39ef57"
}
```

Esempio: crea un target di montaggio su un IPv4 indirizzo disponibile su una sottorete dual-stack

Il comando specifica il file system, la sottorete, il gruppo di sicurezza, il tipo di indirizzo IP dual-stack e l'indirizzo per la destinazione di montaggio. IPv6 La destinazione viene creata a un IPv4 indirizzo disponibile e all' IPv6 indirizzo specificato nella sottorete dual-stack.

```
$ 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 \
--ip-address-type IP-address-type
--ipv6-address IPv6-address \
```

```
--region aws-region \
```

Il seguente esempio mostra il comando con i dati campione.

```
$ aws efs create-mount-target \
--file-system-id fs-0123456789abcdef1 \
--subnet-id  subnet-b3983dc4 \
--security-group sg-01234567 \
--ip-address-type DUAL_STACK \
--ipv6-address 2001:0db8:85a3:0000:0000:8a2e:0370:7334 \
--region us-east-2 \
```

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.

```
{
    "OwnerID": "111122223333"
    "MountTargetId": "fsmt-f9a14450",
    "FileSystemId": "fs-0123456789abcdef1",
    "SubnetId": "subnet-b3983dc4",
    "LifeCycleState": "available",
    "IpAddress": "10.0.1.24",
    "Ipv6Address": "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
    "NetworkInterfaceId": "eni-3851ec4e",
    "AvailabilityZoneId": "use2-az1",
    "AvailabilityZoneName": "us-east-2a",
    "VpcId": "vpc-3c39ef57"
}
```

Eliminazione degli obiettivi di montaggio

Quando si elimina una destinazione di montaggio, l'operazione interrompe in modo forzato qualsiasi mount del file system, il che potrebbe interrompere le istanze o le applicazioni che utilizzano tali mount. Per evitare il malfunzionamento delle applicazioni, arresta le applicazioni e disinstalla il file system prima di eliminare il target di montaggio. Per ulteriori informazioni, consulta Smontaggio dei file system.

È possibile eliminare le destinazioni di montaggio per un file system utilizzando o a livello di AWS Management Console programmazione AWS CLI utilizzando. AWS SDKs

Utilizzo della console

Utilizzare la procedura seguente per eliminare le destinazioni di montaggio per un file system EFS esistente.

Per eliminare le destinazioni di montaggio su un file system EFS

1. Smonta il file system. Per istruzioni, consultare Smontaggio dei file system.
2. Apri la console Amazon Elastic File System all'indirizzo https://console.aws.amazon.com/efs/.
3. Nel riquadro di navigazione a sinistra, scegli File system, quindi seleziona il file system per il quale desideri eliminare la destinazione di montaggio.
4. Scegli Rete, quindi scegli Gestisci per visualizzare le destinazioni di montaggio per il file system.
5. Per ogni destinazione di montaggio che desideri eliminare, scegli Rimuovi.
6. Scegli Save (Salva).

Usando il AWS CLI

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

> **Note**
>
> Prima di eliminare un target di montaggio, 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 \
```

Modifica del VPC di destinazione del montaggio

Puoi utilizzare un file system 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 EFS da queste destinazioni:

- EC2 Istanze Amazon nello stesso VPC
- EC2 istanze in un VPC connesse 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 VPCs che consente di instradare il traffico tra di loro. La connessione può utilizzare la versione 4 (IPv4) o la versione 6 (IPv6) del protocollo Internet privato. 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 modificare il VPC di un file system

Di seguito sono riportati i passaggi da eseguire per modificare il VPC per la configurazione di rete di un file system EFS.

1. Eliminare ogni destinazione di montaggio assegnata al file system. Per istruzioni, consultare Eliminazione degli obiettivi di montaggio.
2. Quando lo stato Mount targets per ogni mount target viene eliminato, assegna il nuovo VPC e crea nuovi target di montaggio per il file system. Per istruzioni, consultare Creazione di destinazioni di montaggio.

Modifica dei gruppi di sicurezza di Mount Target

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 si consente all' EC2 istanza di comunicare con il file system. Per ulteriori informazioni sui gruppi di sicurezza, consulta Utilizzo dei gruppi di sicurezza VPC.

È possibile aggiungere o rimuovere gruppi di sicurezza per la destinazione di montaggio di un file system utilizzando o AWS Management Console AWS CLI, a livello di codice, utilizzando. AWS SDKs

Utilizzo della console

Per modificare i gruppi di sicurezza per le destinazioni di montaggio

Utilizzare la procedura seguente per aggiungere o rimuovere i gruppi di sicurezza di destinazione di montaggio per un file system EFS esistente.

1. Apri la console Amazon Elastic File System all'indirizzo https://console.aws.amazon.com/efs/.
2. Nel riquadro di navigazione a sinistra, scegli File system, quindi seleziona il file system per il quale desideri gestire le destinazioni di montaggio.
3. Scegli Rete, quindi scegli Gestisci per visualizzare le destinazioni di montaggio per il file system.
4. Per rimuovere un gruppo di sicurezza da un target di montaggio, Scegli X accanto all'ID del gruppo di sicurezza.
5. Per aggiungere un gruppo di sicurezza a un target di montaggio, scegli la sicurezza dall'elenco dei gruppi di sicurezza.
6. Scegli Save (Salva).

Usando il AWS CLI

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
```

Gestione della velocità di trasmissione effettiva del file system

La velocità effettiva elastica è la modalità di throughput predefinita nella console Amazon EFS 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.

> **Note**
>
> Sebbene la velocità effettiva elastica sia progettata per adattarsi elasticamente alla velocità effettiva, consigliamo di implementare una governance adeguata attraverso il monitoraggio delle metriche con avvisi CloudWatch (MeteredIOBytes) e di utilizzo come parte delle migliori pratiche operative. Questo ti aiuta a mantenere un utilizzo ottimale delle risorse e a rimanere entro i parametri operativi pianificati. Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.

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. La modifica della modalità di throughput non causa tempi

di inattività delle applicazioni. 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.

Utilizzo della console

Per gestire la velocità effettiva del file system

1. Apri la console Amazon Elastic File System all'indirizzo 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 throughput massimo in lettura appare come tre volte la quantità di velocità di throughput 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.

Utilizzando il AWS CLI

Utilizza il comando update-file-systemCLI o l'azione UpdateFileSystem API per modificare la modalità di throughput di un file system.

Gestione del ciclo di vita dello storage

È possibile gestire i file system in modo che dispongano di uno storage conveniente per l'intero ciclo di vita. Utilizza la gestione del ciclo di vita per trasferire automaticamente i dati tra le classi di storage in base alla configurazione del ciclo di vita del file system. La configurazione del ciclo di vita comprende tre politiche del ciclo di vita impostate per il file system.

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. 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.

Le policy del ciclo di vita si applicano all'intero file system EFS.

Le policy del ciclo di vita EFS sono:

- Transizione alla IA: indica alla gestione del ciclo di vita quando spostare i file nello storage Infrequent Access, 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 quando si accede ai file nello storage IA o Archive. Per impostazione predefinita, i file non vengono spostati nuovamente nello storage Standard e rimangono nella classe di storage IA o Archive quando vi si accede.

  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 Configurazione delle politiche del ciclo di vita.

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 la transizione dei file verso o fuori dallo storage IA e Archive varia a seconda della dimensione del file e del carico di lavoro del file system. Ad esempio, la transizione di milioni di file di piccole dimensioni può richiedere più tempo rispetto alla transizione di un numero inferiore di file più grandi con la stessa dimensione di archiviazione totale.

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.

Le operazioni sui metadati per i file system nello storage IA o Archive, come l'elenco del contenuto 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.

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.

Configurazione delle politiche del ciclo di vita

Quando si crea un file system EFS con le impostazioni consigliate utilizzando il AWS Management Console, il file system viene configurato automaticamente con la seguente configurazione del ciclo di vita predefinita:

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

È possibile modificare le politiche del ciclo di vita predefinite durante la creazione di un file system con impostazioni personalizzate utilizzando AWS Management Console o quando si crea un file system utilizzando. AWS CLI In alternativa, è possibile modificare le politiche dopo la creazione del file system, come descritto nelle procedure seguenti.

Utilizzo della 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, configura le politiche del ciclo di vita:
   - Imposta Transition into IA su una delle opzioni disponibili. Per interrompere lo spostamento dei file nello storage IA, scegli Nessuno.
   - Imposta Transition into Archive su una delle opzioni 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 Archive allo storage Standard al primo accesso, seleziona Nessuno.
6. Per salvare le modifiche, scegliere Salva modifiche.

Usando il AWS CLI

È possibile utilizzare il 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
- Le politiche chiave sono contenute AWS KMS nella Guida per gli AWS Key Management Service sviluppatori
- Le sovvenzioni sono AWS KMS disponibili nella Guida per gli AWS Key Management Service sviluppatori.

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.

Gestione delle chiavi KMS per i file system EFS

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 .

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.

Argomenti

- Strumenti di monitoraggio
- In che modo Amazon EFS riporta le dimensioni dei file system e degli oggetti
- Visualizzazione della dimensione della classe di storage
- Monitoraggio delle metriche con Amazon CloudWatch
- Registrazione delle chiamate API Amazon EFS con AWS CloudTrail

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 politica di Amazon Auto EC2 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 delle metriche 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 What is Amazon CloudWatch Logs? 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 di controllare anche i file di registro dei 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.

In che modo Amazon EFS riporta le dimensioni dei file system e degli oggetti

Le seguenti sezioni descrivono come Amazon EFS riporta le dimensioni del file system, le dimensioni degli oggetti all'interno di un file system e la velocità effettiva del file system.

Misurazione degli oggetti del file system EFS

Gli oggetti che è possibile visualizzare in un file system EFS includono file, directory, collegamenti simbolici e file speciali (FIFOs 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 riporta lo spazio utilizzato per un oggetto, tramite l'`space_used`attributo NFSv4 .1, include la dimensione dei dati misurata corrente dell'oggetto ma non la dimensione dei 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'`du`utilità 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
```

Dimensione misurata di un file system EFS

La dimensione misurata di un file system 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.

È possibile visualizzare la dimensione misurata per un file system 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 il throughput Bursting.

- 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 metriche per Amazon EFS.
- Esegui il `df` comando 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

ai CloudWatch parametri per Amazon EFS Per ulteriori informazioni sul parametro `StorageBytes`, consulta CloudWatch metriche 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 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 1 KiB dopo i primi 4 KiB. Le operazioni sui dati vengono misurate con incrementi di 1 KiB dopo i primi 32 KiB.

> **Note**
>
> Sebbene Elastic Throughput sia progettato per adattarsi elasticamente alla velocità effettiva, consigliamo di implementare una governance adeguata attraverso il monitoraggio delle metriche con avvisi CloudWatch (MeteredIOBytes) e di utilizzo come parte delle best practice operative. Questo ti aiuta a mantenere un utilizzo ottimale delle risorse e a rimanere entro i parametri operativi pianificati. Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.

Misurazione della velocità di trasmissione effettiva con provisioning

Per i file system che utilizzano la modalità Provisioned Throughput, 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.

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.

Utilizzo della console

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 ai CloudWatch parametri per Amazon EFS.

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 del file system EFS.

Monitoraggio delle metriche 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 What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.

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.

Argomenti

- CloudWatch metriche per Amazon EFS
- Accesso ai CloudWatch parametri per Amazon EFS
- Utilizzo dei CloudWatch parametri per Amazon EFS
- Utilizzo della matematica metrica con le metriche CloudWatch
- Monitoraggio dei tentativi di montaggio riusciti e falliti
- Creazione di CloudWatch allarmi per monitorare Amazon EFS

CloudWatch metriche per Amazon EFS

Le metriche di Amazon EFS utilizzano lo `EFS` spazio dei nomi. Lo spazio dei nomi `AWS/EFS` include i parametri descritti di seguito. Tutte le metriche, ad eccezione di, `TimeSinceLastSync` si riferiscono a una singola dimensione,. `FileSystemId` Un ID del file system è disponibile nella console di gestione Amazon EFS e assume la forma di `fs-abcdef0123456789a`.

`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.

Questa metrica utilizza due dimensioni:

- `FileSystemId`dimensione: ID del file system di origine nella configurazione di replica.
- `DestinationFileSystemId`dimension — ID del file system di destinazione nella configurazione di replica.

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 Standard 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 con throughput Bursting, 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 scontate in base al limite di velocità effettiva.

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`

Totale IOBytes

Il numero effettivo di byte per ogni operazione del file system elaborata da Amazon EFS, senza sconti di lettura. Questo numero può differire dall'importo effettivo richiesto dalle tue applicazioni perché include dei valori minimi. Questo numero può anche essere superiore ai numeri indicati in`PermittedThroughput`.

Le operazioni relative ai dati sono misurate a 32 KiB e le altre operazioni sono misurate a 4 KiB. Dopo il minimo, tutte le operazioni vengono misurate per KiB.

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`

Il numero effettivo di byte per ogni 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`

Il numero effettivo di byte per ogni 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`

Il numero effettivo di byte per ogni operazione sui 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`

`MetadataReadIOBytes`

Il numero effettivo di byte per ogni operazione di lettura dei metadati.

La `Sum` statistica è il numero totale di byte associati alle operazioni di lettura dei metadati. La `Minimum` statistica è la dimensione della più piccola operazione di lettura dei metadati durante il periodo. La `Maximum` statistica è la dimensione della più grande operazione di lettura dei metadati durante il periodo. La `Average` statistica è la dimensione media delle operazioni di lettura dei metadati durante il periodo. La `SampleCount` statistica fornisce un conteggio delle operazioni di lettura dei 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`

`MetadataWriteIOBytes`

Il numero effettivo di byte per ogni operazione di scrittura dei metadati.

La `Sum` statistica è il numero totale di byte associati alle operazioni di scrittura dei metadati. La `Minimum` statistica è la dimensione della più piccola operazione di scrittura dei metadati durante il periodo. La `Maximum` statistica è la dimensione della più grande operazione di scrittura di metadati durante il periodo. La `Average` statistica è la dimensione media delle operazioni di scrittura dei metadati durante il periodo. La `SampleCount` statistica fornisce un conteggio delle operazioni di scrittura dei 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, esiste una connessione per EC2 istanza Amazon montata.

> **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 CloudWatch ogni 15 minuti.

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 (IA) 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 effettiva (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 dimensione misurata della classe di archiviazione, dopo aver arrotondato i file di piccole dimensioni a 128 KiB.
- `Archive`è la dimensione effettiva (in byte) dei dati archiviati nella classe di storage EFS Archive.
- `ArchiveSizeOverhead`è la differenza (in byte) tra la dimensione effettiva dei dati nella classe di storage EFS Archive (indicata nella `Archive` dimensione) e la dimensione misurata della classe di storage, dopo aver arrotondato i file di piccole dimensioni 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).

Accesso ai CloudWatch parametri per Amazon EFS

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

Per visualizzare CloudWatch metriche e allarmi (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 CloudWatch metriche e allarmi (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.

Utilizzo dei CloudWatch parametri per 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 posso determinare la quantità totale di dati trasferiti?	È possibile monitorare le `Sum` statistiche giornaliere `MeteredIOBytes` per vedere il totale dei dati trasferiti.
Come posso tenere traccia del numero di EC2 istanze Amazon 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.

Monitoraggio delle prestazioni del throughput

Le CloudWatch metriche per il monitoraggio del throughput —`TotalIOBytes`,`ReadIOBytes`,`WriteIOBytes`, 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 Standard 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 metrica con le metriche CloudWatch

Utilizzando la matematica dei parametri, puoi interrogare più CloudWatch metriche Amazon e utilizzare espressioni matematiche per creare nuove serie temporali basate su questi parametri. 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 Using math expression with CloudWatch metrics 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` • `DataWriteIOBytes` • `MetadataIOBytes` • `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
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	`Permitted Throughput`	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` • `DataWriteIOBytes`	Conteggio del campione	1 minuto

ID	Parametri utilizzabili	Statistic	Periodo
	• `MetadataIOBytes` • `TotalIOBytes`		

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` • `DataWriteIOBytes` • `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` • `DataWriteIOBytes` • `MetadataIOBytes`	sum	1 minuto
m2	• `DataReadIOBytes` • `DataWriteIOBytes` • `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 Lavorare con i AWS CloudFormation modelli nella Guida per l'AWS CloudFormation utente.

Monitoraggio dei tentativi di montaggio riusciti e falliti

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' EC2 istanza 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' EC2 istanza montando il file system. Per ulteriori informazioni, consulta Installazione o aggiornamento automatico del client Amazon EFS tramite AWS Systems Manager o Installazione manuale del client Amazon EFS.
2. `botocore`Effettua l'installazione sull' EC2 istanza che monterà il file system. Per ulteriori informazioni, consulta Installazione e aggiornamento `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. Allega la policy `AmazonElasticFileSystemsUtils` AWS gestita al ruolo IAM che hai collegato all' EC2 istanza 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/aws/efs/utilslog. Vedrai un flusso di log per ogni combinazione di EC2 istanza Amazon 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.

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.

> **Note**
>
> Al momento, non è possibile imporre la crittografia dei dati in transito.

Le seguenti procedure illustrano come creare allarmi per Amazon EFS.

Utilizzo della console

Per impostare allarmi utilizzando la console CloudWatch

1. Accedi a 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 Lo stato è ALLARME. 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.

Usando il AWS CLI

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.

Utilizzando l' CloudWatch API

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 con AWS 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 API di 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 la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni, consulta la sezione Cos'è AWS CloudTrail? nella Guida AWS CloudTrail per l'utente.

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 eventi recenti in Account AWS. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Per una registrazione continua degli eventi del tuo Account 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 crei un percorso nella console, il percorso si applica a tutti i Regione AWS file. Il trail registra gli eventi da tutti gli Regioni AWS elementi della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS CloudTrail :

- Creare un percorso per il tuo account AWS
- AWS integrazioni di servizi con log CloudTrail
- 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

Tutti gli Amazon EFS API Amazon EFS sono registrati 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 credenziali utente root o utente AWS Identity and Access Management (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 AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail UserIdentity nella Guida per l'AWS CloudTrail utente.

Informazioni sulle voci del file di log 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 log per ruoli collegati ai servizi 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 sui ruoli collegati ai servizi EFS, consulta 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 AWSService RoleForAmazonElasticFileSystem 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 log 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, consulta Utilizzo di IAM per controllare l'accesso ai file system.

L'esempio seguente mostra una voce di CloudTrail registro che mostra un evento. `NewClientConnection`


```
{
    "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 permette di scegliere se usare la crittografia dei dati inattivi, la crittografia dei dati in transito o entrambi i tipi, per i 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 di 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"
```

Utilizzo dei AWS report di fatturazione e utilizzo

Quando usi Amazon EFS, paghi solo per le risorse che usi e non sono previste tariffe minime o costi di configurazione. Come altri AWS servizi, anche se i prezzi sono indicati su base mensile, l'utilizzo viene ripartito proporzionalmente all'ora e ti viene fatturato l'utilizzo medio nell'arco di un mese.

AWS fornisce i seguenti report per Amazon EFS:

- Report di fatturazione: report multipli che forniscono viste di alto livello di tutte le attività per i AWS servizi che stai utilizzando, incluso Amazon EFS. AWS fattura sempre al proprietario del file system EFS le tariffe di Amazon EFS. Per ulteriori informazioni sui report di fatturazione, consulta AWS Billing report per Amazon EFS.
- Report sull'utilizzo: un riepilogo delle attività per un servizio specifico, aggregato per ora, giorno o mese. È possibile scegliere quale tipo di utilizzo e operazione includere. È inoltre possibile scegliere la modalità di aggregazione dei dati. Per ulteriori informazioni, consulta AWS report di utilizzo per Amazon EFS.

  I seguenti argomenti forniscono informazioni sulla fatturazione e sui report di utilizzo per Amazon EFS.

Argomenti

- Utilizzo dei tag del file system EFS per l'allocazione dei costi
- AWS Billing report per Amazon EFS
- AWS report di utilizzo per Amazon EFS
- Comprendere i report di fatturazione e utilizzo per Amazon EFS

Utilizzo dei tag del file system EFS per l'allocazione dei costi

Per tenere traccia dei costi di archiviazione o di altri criteri per singoli progetti o gruppi di progetti, etichettate i file system EFS utilizzando i tag di allocazione dei costi. Un tag di allocazione dei costi è una coppia chiave-valore associata a un file system. Dopo aver attivato i tag di allocazione dei costi, li AWS utilizza per organizzare i costi delle risorse nel rapporto di allocazione dei costi.

Il rapporto sull'allocazione dei costi elenca l' AWS utilizzo del tuo account per categoria di prodotto e utente dell'account collegato. Il report contiene le stesse voci di utilizzo indicate nel report di

fatturazione dettagliato (vedere Comprendere i report di fatturazione e utilizzo per Amazon EFS) e altre colonne relative alle chiavi dei tag.

AWS fornisce due tipi di tag di allocazione dei costi, tag AWS generati e tag definiti dall'utente. AWS definisce, crea e applica automaticamente la chiave `aws:createdBy` tag AWS generata dopo un CreateFileSystem evento Amazon EFS. Definisci, crei e applichi tag definiti dall'utente ai tuoi file system.

È necessario attivare entrambi i tipi di tag separatamente nella console Gestione di costi e fatturazione prima di poterli visualizzare nei report di fatturazione. Per ulteriori informazioni sui tag AWS generati, consulta Organizzazione e monitoraggio dei costi utilizzando i tag di allocazione dei AWS costi nella Guida per l'AWS Billing utente.

- Per ulteriori informazioni sulla creazione di tag definiti dall'utente per le risorse EFS, vedereEtichettatura delle risorse EFS.
- Per ulteriori informazioni sull'attivazione dei tag definiti dall'utente nella console di Billing and Cost Management, consulta Attivazione dei tag di allocazione dei costi definiti dall'utente nella Guida per l'utente.AWS Billing
- Per ulteriori informazioni sull'attivazione dei tag AWS generati nella console di Billing and Cost Management, consulta AWS Attivazione dei tag di allocazione dei costi generati nella Guida per l'utente.AWS Billing

Tag per l'allocazione dei costi definiti dall'utente

Un tag per l'allocazione dei costi definito dall'utente presenta i seguenti componenti:

- La chiave di tag: La chiave di tag corrisponde al nome del tag. Ad esempio, nel tag project/Trinity, project è la chiave. La chiave di tag è una stringa che fa distinzione tra maiuscole e minuscole, contenente da 1 a 128 caratteri Unicode.

- Il valore del tag. Il valore del tag è una stringa obbligatoria. Ad esempio, nel tag project/Trinity, Trinity è il valore. Il valore del tag è una stringa che fa distinzione tra maiuscole e minuscole, contenente da 0 a 256 caratteri Unicode.

Per ulteriori informazioni sui tag definiti dall'utente, vedere Utilizzo dei tag di allocazione dei costi definiti dall'utente nella Guida per l'utente.AWS Billing

AWS Billing report per Amazon EFS

La fattura mensile AWS separa le informazioni di utilizzo e i costi per AWS servizio e funzione. Sono disponibili diversi report di AWS fatturazione: il rapporto mensile, il rapporto sull'allocazione dei costi e i report di fatturazione dettagliati. Per ulteriori informazioni, consulta Comprendere la fattura nella Guida per l'AWS Billingutente.

Per report più dettagliati sull'utilizzo dello storage Amazon EFS, utilizza Esportazioni di dati AWS per creare esportazioni di AWS Cost and Usage Report (AWS CUR). Con AWS CUR 2.0, pubblichi i report di AWS fatturazione in un bucket Amazon Simple Storage Service (Amazon S3) di tua proprietà. Il report sull'utilizzo di Amazon EFS elenca le operazioni per tipo di utilizzo e Regione AWS. Per ulteriori informazioni, consulta Cost and Usage Report (CUR) 2.0 nella Guida per l'Esportazioni di dati AWS utente.

I file system EFS vengono fatturati in base alle seguenti categorie di utilizzo.

- Storage (per gigabyte [GB]): la quantità di dati archiviati nei file system EFS al mese, con prezzi diversi a seconda della classe di storage (EFS Standard, EFS Infrequent Access (IA) ed EFS Archive).
- Throughput (per GB o mebibyte al secondo [MiBps]): la quantità di dati trasferiti (operazioni di lettura/scrittura) o la quantità che supera la quantità assegnata, a seconda della velocità effettiva del file system, al mese.
- Accesso e transizione ai dati (per MiBps): la quantità di dati letti e trasferiti nelle classi di storage EFS Infrequent Access (IA) ed EFS Archive al mese.
- Archiviazione di backup (per GB): la quantità di spazio di archiviazione utilizzata dai backup al mese. L'aumento del periodo di conservazione dei backup o l'esecuzione di ulteriori backup di volume avviati dall'utente aumentano la quantità di storage di backup utilizzata dal file system. Per ulteriori informazioni, consulta Backup dei file system EFS
- Replica (per GB): i tassi di attività prevalenti di storage e lettura, scrittura e tiering per i file system EFS di origine e destinazione, nonché eventuali costi mensili applicabili per le attività di trasferimento dati tra di essi.

Per informazioni dettagliate sui costi di Amazon EFS, consulta la pagina dei prezzi di Amazon EFS.

Per informazioni sulla comprensione dei codici e delle abbreviazioni utilizzati nei report di fatturazione e utilizzo per Amazon EFS, consulta. Comprendere i report di fatturazione e utilizzo per Amazon EFS

AWS report di utilizzo per Amazon EFS

Quando si scarica un report di utilizzo, è possibile scegliere di aggregare i dati sull'utilizzo in base a ora, giorno o mese. Il report sull'utilizzo di Amazon EFS elenca le operazioni per tipo di utilizzo e Regione AWS. Per report più dettagliati sull'utilizzo dello storage Amazon EFS, scarica report di AWS utilizzo generati dinamicamente. È possibile scegliere quale tipo di utilizzo, operazione e periodo di tempo includere. È inoltre possibile scegliere la modalità di aggregazione dei dati. Per ulteriori informazioni sul download dei report di utilizzo, consulta Downloading an AWS Usage Report nella AWS Data Exports User Guide.

Il report sull'utilizzo di Amazon EFS include le seguenti informazioni:

- Servizio — Amazon EFS
- UsageType— Uno dei seguenti valori:
  - Un codice che identifica il tipo di storage
  - Un codice che identifica il tipo di richiesta
  - Un codice che identifica il tipo di trasferimento dei dati
  - Un codice che identifica la modalità di trasmissione
  - Un codice che identifica l'utilizzo del backup

  Per una spiegazione dettagliata dei tipi di utilizzo di Amazon EFS, consultaComprendere i report di fatturazione e utilizzo per Amazon EFS.
- Risorsa: il nome della risorsa associata all'utilizzo elencato.
- StartTime— Ora di inizio del giorno a cui si applica l'utilizzo, in UTC (Coordinated Universal Time).
- EndTime— Ora di fine del giorno a cui si riferisce l'utilizzo, in UTC (Coordinated Universal Time).
- UsageValue— Uno dei seguenti valori di volume. L'unità di misura tipica per i dati è gigabyte (GB). Tuttavia, a seconda del servizio e del report, potrebbero invece essere visualizzati terabyte (TB).
  - Il numero di richieste durante il periodo di tempo specificato
  - La quantità di dati trasferiti
  - La quantità di dati memorizzati in una data ora

Per informazioni sulla comprensione dei codici e delle abbreviazioni utilizzati nei report di fatturazione e utilizzo per Amazon EFS, consulta. Comprendere i report di fatturazione e utilizzo per Amazon EFS

Comprendere i report di fatturazione e utilizzo per Amazon EFS

I report di fatturazione e utilizzo di Amazon EFS utilizzano codici e abbreviazioni. Per i tipi di utilizzo indicati nella tabella seguente, sostituiscili *`region`* con le abbreviazioni di questo elenco:

- APE1: Asia Pacifico (Hong Kong)
- APN1: Asia Pacifico (Tokyo)
- APN2: Asia Pacifico (Seoul)
- APN3: Asia Pacifico (Osaka)
- APS1: Asia Pacifico (Singapore)
- APS2: Asia Pacifico (Sydney)
- APS3: Asia Pacifico (Mumbai)
- APS4: Asia Pacifico (Giacarta)
- APS5: Asia Pacifico (Hyderabad)
- APS6: Asia Pacifico (Melbourne)
- CAN1: Canada (Centrale)
- CAN2: Canada occidentale (Calgary)
- CNN1: Cina (Pechino)
- CNW1: Cina (Ningxia)
- AFS1: Africa (Città del Capo)
- EUC2: Europa (Zurigo)
- EUN1: Europa (Stoccolma)
- EUS2: Europa (Spagna)
- EUC1: Europa (Francoforte)
- EU: Europa (Irlanda)
- EUS1: Europa (Milano)
- EUW2: Europe (Londra)
- EUW3: Europa (Parigi)
- ILC1: Israele (Tel Aviv)
- MEC1: Medio Oriente (Emirati Arabi Uniti)

- MES1: Medio Oriente (Bahrein)
- SAE1: Sud America (San Paolo)
- UGW1: AWS GovCloud (Stati Uniti occidentali)
- UGE1: AWS GovCloud (Stati Uniti orientali)
- USE1 (o nessun prefisso): Stati Uniti orientali (Virginia settentrionale)
- USE2: Stati Uniti orientali (Ohio)
- USW1: Stati Uniti occidentali (California settentrionale)
- USW2: Stati Uniti occidentali (Oregon)

Per informazioni sui prezzi di Regione AWS, consulta la pagina dei prezzi di Amazon EFS.

La prima colonna della tabella che segue elenca i tipi di utilizzo presenti nei report di utilizzo e fatturazione. L'unità di misura tipica per i dati è gigabyte (GB). Per la quantità di throughput assegnata, tuttavia, vengono utilizzati al suo posto mebibyte al secondo ()MiBps.

Tipi di utilizzo per Amazon EFS

Tipo di utilizzo	CloudWatch parametr	Unità	Granularità	Descrizione
region-ArchiveDataAccess-Bytes	N/D	GB	N/D	La quantità di dati trasferiti o a cui si accede nello storage EFS Archive.
region-ArchiveEarlyDelete-ByteHrs	N/D	GB/mese	N/D	Utilizzo proporzionale dello storage per i file eliminati dallo storage EFS Archive prima della scadenza dell'impegno minimo di 90 giorni.
region-ArchiveEarlyDelete-SmallFiles	N/D	GB/mese	N/D	Utilizzo proporzionale dello storage per file di piccole dimensioni (inferiori a 128 KB) eliminati dallo storage EFS Archive prima della scadenza dell'impegno minimo di 90 giorni.

Tipo di utilizzo	CloudWatch parametr	Unità	Granularità	Descrizione
region-ArchiveTimedStorage-ByteHrs	StorageBytes.Archive	GB al mese	Orario	Il numero di GB al mese in cui i dati sono stati archiviati nello storage EFS Archive.
region-ArchiveTimedStorage-SmallFiles	StorageBytes.ArchiveSizeOverhead	GB/mese	Orario	Il numero di GB/mese in cui piccoli oggetti (inferiori a 128 KB) sono stati archiviati nello storage EFS Archive.
region-ETDataAccess-Bytes	TotalIOBytes	GB	Orario	La quantità di dati scritti o letti per i file utilizzando la velocità effettiva elastica.
region-IADataAccess-Bytes	N/D	GB	Orario	La quantità di dati a cui è stato effettuato l'accesso nello storage EFS Infrequent Access (IA).
region-IATimedStorage-ByteHrs	StorageBytes.IA	GB/mese	Orario	Il numero di GB al mese in cui i dati sono stati archiviati nello storage EFS IA.
region-IATimedStorage-ET-ByteHrs	StorageBytes.IA	GB/mese	Orario	Il numero di GB/mese in cui i dati per i file che utilizzano la velocità effettiva elastica sono stati archiviati nello storage EFS IA.
region-IATimedStorage-ET-SmallFiles	StorageBytes.IASizeOverhe	GB/mese	Orario	Il numero di GB/mese in cui file di piccole dimensioni (inferiori a 128 KB) sono stati archiviati nello storage EFS IA, per i file che utilizzano la velocità effettiva elastica.

Tipo di utilizzo	CloudWatch parametr	Unità	Granularità	Descrizione
region-IATimedStorage-SmallFiles	StorageBytes.IASizeOverhe	GB/mese	Orario	Il numero di GB al mese in cui file di piccole dimensioni (inferiori a 128 KB) sono stati archiviati nello storage EFS IA.
region-IATimedStorage-Z-ByteHrs	StorageBytes.IA	GB/mese	Orario	La dimensione effettiva dei dati archiviati nello storage EFS IA per i file system One Zone.
region-IATimedStorage-Z-SmallFiles	StorageBytes.IASizeOverhe	GB/mese	Orario	Il numero di GB/mese in cui file di piccole dimensioni (inferiori a 128 KB) sono stati archiviati nello storage EFS IA per i file system One Zone.
region-IncludedTP-MiBpsHrs	PermitteThroughput	MiBps-No	Orario	La quantità massima di throughput consentita a un file system.
region-ProvisionedTP-MiBpsHrs	PermitteThroughput	MiBps-No	Orario	Per i file system che utilizzano la velocità effettiva fornita o la velocità effettiva massima consentita.
region-TimedStorage-ByteHrs	StorageBytes.Standard	GB-mo	Orario	La quantità totale effettiva di dati archiviati nello storage EFS Standard per i file system regionali .
region-TimedStorage-Z-ByteHrs	StorageBytes.Standard	GB/mese	Orario	La quantità totale effettiva di dati archiviati nello storage EFS Standard per i file system One Zone.

Note

- Lo storage EFS Archive viene addebitato per una durata minima di archiviazione di 90 giorni, anche se i dati vengono eliminati prima di 90 giorni.
- Un costo di suddivisione in più livelli si applica ai dati distribuiti su più livelli dallo storage EFS Standard allo storage EFS Infrequent Access (IA) e dallo storage EFS IA allo storage EFS Standard.
- Gli storage EFS IA ed EFS Archive hanno una dimensione minima fatturabile dei file di 128 KB. I file di dimensioni inferiori a 128 KiB possono essere suddivisi su più livelli in queste classi di storage, ma vengono addebitati per 128 KiB di storage alla tariffa della classe di storage appropriata.
- Per i file system che utilizzano Elastic throughput, le operazioni sui metadati vengono misurate con incrementi di 1 KiB dopo i primi 4 KiB e le operazioni sui dati vengono misurate con incrementi di 1 KiB dopo i primi 32 KiB.
- L'utilizzo dello storage viene calcolato in gigabyte binari (GB), dove 1 GB corrisponde a 2 30 byte. In che modo Amazon EFS riporta le dimensioni dei file system e degli oggettiPer ulteriori dettagli su come viene misurato l'utilizzo dello storage e del throughput per calcolare la fattura Amazon EFS.
- I GB-mese si ottengono prendendo il numero totale di GB all'ora, aggregandoli nel corso di un mese e dividendoli per il numero di ore di quel mese.

Monitoraggio delle operazioni nei report di utilizzo

Le operazioni descrivono l'azione intrapresa sul file system EFS in base al tipo di utilizzo specificato. Le operazioni sono indicate con codici autoesplicativi, ad esempio `Read` o `Delete`. Per vedere quali azioni sul tuo file system hanno generato un tipo specifico di utilizzo, usa questi codici. Quando crei un report di utilizzo, puoi scegliere di specificare All Operations (Tutte le operazioni) o un'operazione specifica, ad esempio `Write`.

Specifiche prestazionali di 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
- Classi di archiviazione
- Modalità prestazionali
- Modalità di velocità di trasmissione effettiva
- Suggerimenti per le prestazioni Amazon EFS
- Risoluzione dei problemi di prestazioni di Amazon EFS
- Risoluzione dei problemi di AMI e kernel

Riepilogo delle prestazioni

Le prestazioni del file system vengono generalmente misurate utilizzando le dimensioni di latenza, velocità effettiva e Input/Output operazioni 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 Max I/O Performance ha latenze per operazione più elevate rispetto alla modalità a prestazioni General Purpose. 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 illustra le specifiche prestazionali 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	Per-file-system read [1]	Per-file-system scrivi [1]	Lettura/scrittura per client
Regionale	Elastic	A partire da 250 microsecondi (µs)	A partire da 2,7 millisecondi (ms)	900.000—2.500.000 [2]	500.000 [2]	20-60 gibibyte al secondo () GiBps	1—5 GiBps	1.500 mebibyte al secondo (3) MiBps
Regionale	Assegnata	A partire da 250 µs	A partire da 2,7 ms	55.000	25.000	3—10 GiBps	1—3,33 GiBps	500 MiBps
Regionale	Ottimizzazione	A partire da 250 µs	A partire da 2,7 ms	35.000	7,000	3—5 GiBps	1—3 GiBps	500 MiBps
Zona singola	Elastico, fornito, esplosivo	A partire	A partire	35.000	7,000	3 GiBps [4]	1 GiBps [4]	500 MiBps

Configurazione dello storage e della velocità di trasmissione effettiva	Latenza		Numero massimo di IOPS	Velocità di trasmissione effettiva massima
	da 250 µs	da 1,6 ms		

1. La velocità massima di lettura e scrittura dipende da Regione AWS. Un throughput superiore al throughput massimo Regione AWS di an richiede un aumento della quota di throughput. 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 Amazon EFS.
2. Per impostazione predefinita, i file system che utilizzano la velocità effettiva elastica generano un massimo di 90.000 IOPS di lettura per i dati a cui si accede raramente, 250.000 IOPS di lettura per i dati ad accesso frequente e 50.000 IOPS di scrittura. Se il carico di lavoro richiede più IOPS, puoi richiedere un aumento fino a 10 volte questi numeri. Per ulteriori informazioni, consulta Quote per Amazon EFS che è possibile incrementare. 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”.
3. Il throughput massimo combinato di lettura e scrittura è 1.500 MiBps per i file system che utilizzano la velocità effettiva elastica e montati utilizzando la versione 2.0 o successiva del client Amazon EFS (amazon-efs-utils versione) o il driver CSI di Amazon EFS (). aws-efs-csi-driver Per tutti gli altri file system, il limite di velocità effettiva è 500. MiBps Per ulteriori informazioni sul client Amazon EFS, consultaInstallazione del client Amazon EFS.
4. I file system One Zone che utilizzano la velocità di trasmissione Bursting possono garantire gli stessi livelli di velocità di per-file-system lettura e scrittura dei file system regionali che utilizzano la velocità effettiva di Bursting (lettura massima di 5 GiBps in lettura e 3 in scrittura). GiBps

Classi di archiviazione

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 offre latenze di primo byte di appena 250 microsecondi per le letture e 2,7 millisecondi 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 I/O modalità 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 General Purpose. La I/O modalità Max non è supportata per i file system One Zone o per i file system che utilizzano la velocità effettiva elastica.

> **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 metrica. `PercentIOLimit` CloudWatch Per ulteriori informazioni, consulta CloudWatch metriche 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 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 Monitoraggio delle 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 prestazionali 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.

Per ulteriori informazioni sulle metriche di Amazon EFS, consulta CloudWatch metriche 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**
>
> Sebbene il throughput elastico sia progettato per adattarsi elasticamente alla velocità effettiva, consigliamo di implementare una governance adeguata attraverso il monitoraggio delle metriche con CloudWatch (MeteredIOBytes) e avvisi di utilizzo come parte delle migliori pratiche operative. Questo ti aiuta a mantenere un utilizzo ottimale delle risorse e a rimanere entro i parametri operativi pianificati. Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.

Per informazioni sui limiti di throughput elastico per regione, vedere. 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 della linea di base di Bursting prevalenti). Regione AWS

Per informazioni sui limiti di velocità effettiva di Quote per Amazon EFS che è possibile incrementare Provisioned per regione, vedere.

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 nello storage Standard (50 per KiBps GiB), 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 • 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 • 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 • Passa a 100 in sola MiBps scrittura per 12 ore al giorno	• Drive 150 in sola lettura ininterro ttamente MiBps • 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 • Passa a 1 sola GiBps scrittura per 12 ore al giorno	• Drive 1.5 in modalità di sola lettura continua GiBps • 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 • 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 • 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.

I/O Dimensioni medie

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. A causa di questa latenza per operazione, la velocità effettiva complessiva generalmente aumenta all'aumentare della I/O dimensione media, poiché il sovraccarico viene ammortizzato su una maggiore quantità di dati.

Ottimizzazione dei carichi di lavoro che richiedono throughput e IOPS elevati

Per carichi di lavoro che richiedono velocità effettiva e IOPS elevati, utilizzate i file system regionali configurati con la modalità prestazionale General Purpose e la velocità effettiva elastica.

> **Note**
>
> Per ottenere il massimo livello di IOPS di 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 istanze di AWS calcolo Amazon EC2 e di altro tipo 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 abiliti le scritture asincrone sul tuo file system, le operazioni di scrittura in sospeso vengono memorizzate nel buffer sull'istanza Amazon prima di essere scritte su EC2 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**
>
> Il modello di richiesta scelto presenta dei compromessi in termini di coerenza (se utilizzi più EC2 istanze Amazon) e 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 Considerazioni sul montaggio per Linux.

Quando monti i tuoi file system su EC2 istanze Amazon, 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 Amazon EC2 macOS che eseguono macOS Big Sur, è supportata solo la versione 2.0. NFSv4

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 del tempo di andata e ritorno.
- 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"
```

Risoluzione dei problemi di prestazioni di 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
- Accesso negato ai file consentiti sul file system NFS
- Errori durante l'accesso alla console Amazon EFS
- L' EC2 istanza Amazon si blocca
- Blocco di un'applicazione che esegue la scrittura di grandi quantità di dati
- Prestazioni scadenti durante l'apertura di svariati file in parallelo
- Impostazioni NFS personalizzate che causano ritardi nelle operazioni di scrittura
- La creazione di backup con Oracle Recovery Manager è lenta

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 delle identità e degli accessi per Amazon EFS.

Accesso negato ai file consentiti sul file system NFS

Quando un utente a cui sono assegnati più di 16 gruppi di accesso IDs (GIDs) 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 ne supporta un massimo di 16 GIDs per utente e tutti gli altri GIDs vengono troncati dalla richiesta del client NFS, come definito nella RFC 5531.

Operazione da eseguire

Ristrutturate le mappature di utenti e gruppi NFS in modo che a ogni utente non vengano assegnati più di 16 gruppi di accesso (). GIDs

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 EC2 servizio Amazon 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.

L' EC2 istanza Amazon si blocca

Un' EC2 istanza Amazon può bloccarsi perché hai eliminato una destinazione di montaggio del file system senza prima smontare il file system.

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 perché questi 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 puoi usare NFSv4 .1, tieni presente che il client Linux NFSv4 .0 serializza le richieste di apertura e chiusura per ID utente e gruppo. IDs Questa serializzazione ha luogo anche quando più processi o più thread inviano molteplici richieste contemporaneamente. Il client invia solo un'operazione di apertura o chiusura alla volta a un server NFS, quando tutte corrispondono. IDs Per risolvere questi problemi, è possibile eseguire le seguenti azioni:

- Puoi eseguire ogni processo da un ID utente diverso sulla stessa EC2 istanza Amazon.
- Puoi lasciare l'utente IDs lo stesso per tutte le richieste aperte e modificare IDs invece il set di gruppi.
- Puoi eseguire ogni processo da un' EC2 istanza Amazon separata.

Impostazioni NFS personalizzate che causano ritardi nelle operazioni di scrittura

Hai impostazioni client NFS personalizzate e un' EC2istanza Amazon impiega fino a tre secondi per vedere un'operazione di scrittura eseguita su un file system da un'altra EC2 istanza Amazon.

Operazione da eseguire

Se si verifica questo problema, è possibile risolverlo in uno dei seguenti modi:

- Se il client NFS sull' EC2 istanza Amazon che sta leggendo i dati ha la memorizzazione nella cache degli attributi attivata, smonta il file system. Quindi rimontare utilizzando l'opzione `noac` per disabilitare il caching degli attributi. La memorizzazione nella cache degli attributi in NFSv4 .1 è abilitata 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 dei problemi di AMI e kernel

Di seguito, puoi trovare informazioni sulla risoluzione dei problemi relativi a determinate versioni di Amazon Machine Image (AMI) o del kernel quando usi Amazon EFS da un' EC2istanza Amazon.

Argomenti

- Non è possibile eseguire il comando chown

- Il file system continua a eseguire ripetutamente delle operazioni a causa di un bug del client
- Client in deadlock
- Il recupero dell'elenco dei file di una grande cartella impiega molto tempo

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.

Backup e replica dei dati in Amazon EFS

Per proteggere i tuoi dati, Amazon EFS esegue automaticamente il backup dei tuoi file system EFS. Per una maggiore resilienza e protezione dei dati, puoi replicare il tuo file system EFS in un file. Regione AWS Il backup e la replica dei file system EFS garantiscono la possibilità di fornire operazioni o servizi continui nel caso in cui succeda qualcosa ai dati del file system EFS. Ad esempio, in caso di danneggiamento o perdita dei dati.

Argomenti

- Backup dei file system EFS
- Replica dei file system EFS

Backup dei file system EFS

Amazon EFS è integrato nativamente con AWS Backup un servizio completamente gestito e basato su policy che puoi utilizzare per creare e gestire policy di backup per proteggere i tuoi dati in Amazon EFS. Per impostazione predefinita, il backup dei file system creati utilizzando la console Amazon EFS viene eseguito automaticamente. AWS Backup Quando si utilizza la CLI o l'API per creare un file system, i backup automatici sono abilitati per impostazione predefinita solo per i file system One Zone.

Utilizzando AWS Backup Amazon EFS, puoi eseguire le seguenti azioni:

- Gestisci la pianificazione e la conservazione automatiche dei backup configurando i piani di backup. È possibile specificare la frequenza di backup, quando eseguire il backup, per quanto tempo conservare i backup e una politica del ciclo di vita per i backup.
- Ripristina i backup dei dati di Amazon EFS. Puoi ripristinare i dati del file system su un file system nuovo o esistente. È inoltre possibile scegliere se eseguire un ripristino completo o un ripristino a livello di elemento.

Per ulteriori informazioni sull'utilizzo AWS Backup, consulta la Guida introduttiva alla Developer AWS Backup Guide.AWS Backup

Argomenti

- Come AWS Backup funziona con Amazon EFS
- Autorizzazioni IAM richieste

- Prestazioni di backup
- Gestione dei backup automatici dei file system EFS

Come AWS Backup funziona con Amazon EFS

Per impostazione predefinita, il backup dei file system creati utilizzando la console Amazon EFS viene eseguito automaticamente. AWS Backup Quando si utilizza la CLI o l'API per creare un file system, i backup automatici sono abilitati per impostazione predefinita solo per i file system One Zone. È possibile attivare i backup automatici dopo aver creato il file system EFS utilizzando l'API AWS CLI o. 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 Amazon EFS per tuo conto. Non è possibile eliminare il piano e il vault di backup predefiniti.

Viene eseguito 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.

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 e modificare i file system EFS mentre è in corso il 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.

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. Puoi vedere lo stato di tutti i tuoi backup nella Console di gestione. AWS Backup

Backup on-demand

Con AWS Backup, puoi salvare una singola risorsa in un archivio di backup su richiesta. 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.

Inoltre, AWS Backup trasferisce automaticamente i dati alla conservazione a freddo solo per i dati che non esistono più nel backup a caldo più recente. Ad esempio, il file system contiene 100 file quando si crea un backup e due file vengono eliminati il giorno successivo alla creazione del backup (100 file - 2 file = 98 file il secondo giorno). Quando trasferisci i dati alla conservazione a freddo, solo i due file eliminati vengono trasferiti nella conservazione a freddo e i restanti 98 file vengono fatturati come archiviazione a caldo.

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 AWS Backup limiti, consulta le AWS Backup quote nella Guida per gli AWS Backup sviluppatori.

Eliminazioni 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.

Autorizzazioni IAM richieste

AWS Backup crea un ruolo collegato al servizio per tuo conto nel tuo account. Questo ruolo dispone delle autorizzazioni richieste per eseguire backup Amazon EFS.

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 delle identità e degli accessi per Amazon EFS e Utilizzo di IAM per controllare l'accesso ai file system.

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 2.000 file al secondo o 400 megabyte al secondo (MBps), a seconda di quale sia la più lenta.
- Velocità di ripristino di 1.500 file al secondo o 200 MBps, a seconda di quale sia la più lenta.

La durata massima di un'operazione di backup 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.

Gestione dei backup automatici dei file system EFS

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 l'API AWS CLI o.

È possibile modificare le impostazioni del piano di backup predefinito utilizzando la AWS Backup console. Per ulteriori informazioni, consulta la sezione Gestione dei piani di backup nella Guida per gli AWS Backup sviluppatori. È possibile visualizzare tutti i backup automatici e modificare le impostazioni del piano di backup EFS predefinito utilizzando la console AWS Backup.

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.

Dopo aver creato un file system, è possibile attivare o disattivare i backup automatici utilizzando la console, l'API EFS o l'API EFS. AWS CLI

Utilizzo della console

1. Apri la console Amazon Elastic File System all'indirizzo 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. Scegli Save changes (Salva modifiche).

Usando il AWS 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"
    ```

    Amazon 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"
```

Amazon EFS risponde con la nuova policy di backup.

```
{
   "BackupPolicy": {
      "Status": "DISABLING"
   }
}
```

Replica dei file system EFS

Per una maggiore resilienza e protezione dei dati, puoi replicare il tuo file system EFS in un. Regione AWS Quando abiliti la replica su un file system EFS, 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 le esercitazioni quotidiane, puoi eseguire il failover sul tuo file system di replica. Per riprendere le operazioni, è quindi possibile eseguire il failback al file system principale.

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.

Dopo aver creato la configurazione di replica, 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. Vengono invece trasferiti 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 Visualizzazione dei dettagli della replica.

La replica è disponibile in tutti i paesi Regioni AWS in cui è disponibile Amazon EFS. Per replicare un file system EFS in una regione disabilitata per impostazione predefinita, è necessario prima attivare la regione. Per ulteriori informazioni, consulta Specificare cosa può utilizzare Regioni AWS il proprio account nella Guida AWS generale di riferimento. Se decidi di rinunciare a una regione in un secondo momento, Amazon EFS sospende tutte le attività di replica per quella regione. Per riprendere le attività di replica per la regione, attiva nuovamente l'opzione. Regione AWS

> **Note**
>
> La replica non supporta l'uso dei tag per il controllo degli accessi basato su attributi (ABAC).

Argomenti

- Costi
- Prestazioni di replica
- Autorizzazioni IAM richieste
- Configurazione della replica sul nuovo file system EFS
- Configurazione della replica su un file system EFS esistente
- Replica dei file system EFS su più account AWS
- Visualizzazione dei dettagli della replica
- Eliminazione di configurazioni di replica
- Utilizzo della replica

Costi

Per facilitare la replica, Amazon EFS crea directory e metadati nascosti sul file system di destinazione. Questi equivalgono a circa 12 mebibyte (MiB) di dati misurati per i quali ti viene fatturato. Per ulteriori informazioni sulla misurazione dello storage per i file system EFS, consulta In che modo Amazon EFS riporta le dimensioni dei file system e degli oggetti.

Prestazioni di replica

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 Visualizzazione dei dettagli della replica.

Puoi monitorare quando si è verificata 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 Visualizzazione dei dettagli della replica.

Autorizzazioni IAM richieste

Amazon EFS utilizza il ruolo collegato al servizio EFS denominato `AWSServiceRoleForAmazonElasticFileSystem` o il ruolo IAM specificato per sincronizzare la replica tra i file system di origine e di destinazione. Per fornire un ruolo IAM, l'utente o il ruolo IAM che crea la configurazione di replica deve disporre dell'autorizzazione. `iam:PassRole` Per ulteriori informazioni, consulta Concedere a un utente le autorizzazioni per passare un ruolo a un AWS servizio nella Guida per l'AWS Identity and Access Management utente.

- Per ulteriori informazioni su`iam:CreateServiceLinkedRole`, vedere l'esempio inUtilizzo di ruoli collegati ai servizi per Amazon EFS.
- Per ulteriori informazioni su un ruolo IAM personalizzato, consultaCrea un ruolo IAM con una policy di fiducia personalizzata.

> **Note**
>
> Se stai eseguendo la replica tra account, devi fornire un ruolo IAM quando crei la configurazione di replica. L'utilizzo del ruolo collegato al servizio non è consentito. Per ulteriori informazioni, consulta Replica dei file system EFS su più account AWS.

Il ruolo collegato al servizio o il ruolo IAM fornito durante la creazione della configurazione di replica deve disporre delle seguenti autorizzazioni per la replica.

- `elasticfilesystem:DescribeFileSystem`
- `elasticfilesystem:CreateFileSystem`
- `elasticfilesystem:CreateReplicationConfiguration`
- `elasticfilesystem:DeleteReplicationConfiguration`
- `elasticfilesystem:DescribeReplicationConfigurations`

È possibile utilizzare la policy `AmazonElasticFileSystemFullAccess` gestita per ottenere automaticamente tutte le autorizzazioni EFS richieste. Per ulteriori informazioni, consulta AWS politica gestita: AmazonElasticFileSystemFullAccess.

Configurazione della replica sul nuovo file system EFS

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 nel formato Regione AWS che preferisci. Quando esegui la replica su un nuovo file system, scegli il tipo di file system e la chiave AWS Key Management Service (AWS KMS) da utilizzare per la crittografia. Inoltre, Amazon EFS non crea alcun target di montaggio quando crea il file system di destinazione. Dopo aver creato la configurazione di replica, è necessario creare uno o più target di montaggio per montare un file system di destinazione.

> **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.

- 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 AWS KMS chiave 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.

Il file system di destinazione viene creato con impostazioni predefinite basate sul file system di origine. Le impostazioni aggiuntive possono essere modificate dopo la creazione.

- 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, consulta Gestione dei backup automatici dei file system EFS.
- 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 One Zone. In tal caso, viene utilizzata la modalità General Purpose. 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.

  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 del ciclo di vita dello storage.

Fase 1: Creare la configurazione di replica

Il primo passaggio per la replica su un nuovo file system consiste nel creare la configurazione di replica.

Utilizzo della console

1. Accedi AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Apri il file system che desideri replicare:
   a. Nel pannello di navigazione a sinistra, scegli File system.
   b. Nell'elenco dei file system, scegli il file system 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. Scegliete la scheda Replica.
4. Nella sezione Replica, scegli Crea replica.
5. Nella sezione Impostazioni di replica, definisci le impostazioni di replica:
   a. Per la configurazione della replica, scegli se eseguire la replica su un file system nuovo o esistente.
   b. Per Destinazione Regione AWS, scegliete il modo Regione AWS in cui replicare il file system.
6. Nella sezione Impostazioni del file system di destinazione, definite le impostazioni del file system di destinazione.
   a. Per Tipo di file system, scegli un'opzione di archiviazione per il file system:
      - Per creare un file system che archivia i dati in modo ridondante su più zone di disponibilità geograficamente separate all'interno di un' Regione AWS unica area, scegli Regionale.
      - Per creare un file system che archivia i dati in modo ridondante all'interno di una singola zona di disponibilità all'interno di una Regione AWS, scegli Una zona, 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, Amazon EFS utilizza la tua AWS Key Management Service chiave di servizio (`aws/elasticfilesystem`).AWS KMS Per utilizzare una chiave KMS diversa, scegli la chiave KMS o inserisci l'Amazon Resource Name (ARN) della chiave.

> **Important**
>
> Dopo aver creato il file system, non è possibile modificare la chiave KMS.

Crea la configurazione di replica ()AWS CLI

Questa sezione fornisce esempi per la creazione di una configurazione di replica AWS CLI utilizzando il `create-replication-configuration` comando. 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`*. L'esempio utilizza il `Region` parametro per creare un file system di destinazione in. *`eu-west-2`* Regione AWS Il `KmsKeyId` parametro specifica l'ID della chiave KMS da utilizzare per la crittografia del 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 AWS CLI risposte 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*. L'esempio utilizza il `AvailabilityZoneName` parametro per creare un file system di destinazione One Zone nella zona di *us-west-2a* disponibilità. Poiché non viene specificata alcuna chiave KMS, il file system di destinazione viene crittografato utilizzando la chiave di AWS KMS servizio predefinita dell'account (`aws/elasticfilesystem`).

```
aws efs create-replication-configuration \
--source-file-system-id fs-0123456789abcdef1 \
--destinations AvailabilityZoneName=us-west-2a
```

Fase 2: Installare il file system di destinazione

Amazon EFS non crea alcun target di montaggio quando crea il file system di destinazione. Per montare il file system di destinazione, è necessario creare una o più destinazioni di montaggio. Per ulteriori informazioni, consulta Montaggio dei file system EFS.

Configurazione della replica su un file system EFS esistente

Amazon EFS replica i dati e i metadati del file system di origine nel file system di destinazione, a tua scelta. Regione AWS Durante la replica, Amazon EFS identifica le differenze di dati tra i file system e le applica al file system di destinazione.

Per eseguire la replica su un file system esistente, esegui i seguenti passaggi.

Argomenti

- Passaggio 1: disattivare la protezione da sovrascrittura della replica del file system
- Fase 2: Creare la configurazione di replica

> **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.

Passaggio 1: disattivare la protezione da sovrascrittura della replica 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.

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.
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.

Autorizzazione richiesta

La disabilitazione della protezione da sovrascrittura della replica richiede le autorizzazioni per l'azione `elasticfilesystem:UpdateFileSystemProtection`. Per ulteriori informazioni, consulta AWS politica gestita: AmazonElasticFileSystemFullAccess.

Utilizzo della 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.
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.

Per disabilitare la protezione da sovrascrittura della replica ()AWS CLI

Nell'esempio seguente, il comando `update-file-system-protection` CLI disabilita la protezione da sovrascrittura della replica per il file system specificato. Il comando API equivalente è. UpdateFileSystemProtection

```
aws efs update-file-system-protection
 --file-system-id fs-0a8b2be428114d97c
 --replication-overwrite-protection DISABLED
```

Le AWS CLI risposte sono le seguenti.

```
{
    "ReplicationOverwriteProtection": "DISABLED"
}
```

Fase 2: Creare la configurazione di replica

Dopo aver disabilitato la protezione dalla sovrascrittura della replica sul file system di destinazione, è possibile creare la configurazione di replica. Quando si esegue la replica su un file system esistente, il file system di destinazione può trovarsi nello stesso account o in un account diverso rispetto al file system di origine.

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.

> **Note**
>
> Quando configuri inizialmente la replica su un file system esistente, Amazon EFS scrive o rimuove i dati esistenti dal file system di destinazione in modo che corrispondano ai dati nel file system di origine. Se non desideri modificare i dati nel file system di destinazione, dovresti invece replicarli su un nuovo file system. Per ulteriori informazioni, consulta Configurazione della replica sul nuovo file system EFS.

Prerequisiti

Avere una copia dell'ID del file system di destinazione (per la replica dello stesso account) o dell'ARN del file system di destinazione (per la replica tra account) che si desidera utilizzare.

Se il file system di destinazione si trova in un file system Account AWS diverso da quello di origine, crea un ruolo IAM che consenta ad Amazon EFS di eseguire la replica e assegnare politiche di risorse ai file system. Per ulteriori informazioni, consulta Replica dei file system EFS su più account AWS.

Utilizzo della console

1. Accedi AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
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.
4. Nella sezione Replica, scegli Crea replica.
5. Per la configurazione della replica, scegli il file system esistente.

6. Scegliete il file system di destinazione.

   - Per eseguire la replica su un file system che è lo Account AWS stesso del file system di origine:

     1. Seleziona Scegli un file system in questo account e, in Destinazione Regione AWS, seleziona il file system Regione AWS in cui replicare il file system.
     2. Scegliete Browse EFS, quindi selezionate il file system. Il percorso del file system di destinazione viene visualizzato nella casella Destinazione.

   - Per eseguire la replica su un file system che si trova in un file system Account AWS diverso da quello di origine:

     1. Scegli Specificare un file system in un altro account.
     2. Per l'ARN del file system di destinazione, inserisci l'Amazon Resource Name (ARN) del file system di destinazione.

   > **Note**
   >
   > Se la protezione da sovrascrittura della replica è abilitata sul file system, viene visualizzato un avviso. Scegli Disabilita protezione per aprire il file system in una nuova scheda e disattivare la relativa protezione da sovrascrittura da replica. Dopo aver disabilitato la protezione, torna alla scheda Crea replica e fai clic sul pulsante Aggiorna per cancellare il messaggio.

7. Per il ruolo IAM, inserisci l'ARN del ruolo IAM che consente ad Amazon EFS di replicarsi nel file system di destinazione. Questo è facoltativo per la replica sullo stesso account, ma necessario per la replica tra account. Per ulteriori informazioni, consulta Replica dei file system EFS su più account AWS.
8. Scegli Crea replica, digita conferma nella casella di immissione del messaggio di conferma, quindi scegli Crea replica. La sezione Replica mostra i dettagli della replica.

Per creare la configurazione di replica ()AWS CLI

Questa sezione fornisce esempi per la creazione di una configurazione di replica AWS CLI utilizzando il `create-replication-configuration` comando. Il comando API equivalente è CreateReplicationConfiguration.

Example : crea una configurazione di replica su un file system di destinazione esistente in un'altra regione

L'esempio seguente crea una configurazione di replica in cui l'ID del file system *fs-0123456789abcdef1* viene replicato nell'ID *fs-0a8b2be428114d97c* del file system in. *eu-west-2* Regione AWS

```
aws efs create-replication-configuration \
--source-file-system-id fs-0123456789abcdef1 \
--destinations "[{\"Region\":\"eu-west-2\",\"FileSystemId\":\"fs-0a8b2be428114d97c\"}]"
```

La AWS CLI risposta è la seguente:

```
{
    "SourceFileSystemId": "fs-0123456789abcdef1",
    "SourceFileSystemRegion": "us-east-1",
    "SourceFileSystemArn": "arn:aws:elasticfilesystem:us-east-1:111122223333:file-
system/fs-0123456789abcdef1",
    "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:us-
east-1:111122223333:file-system/fs-0123456789abcdef1",
    "CreationTime": "2024-10-20T20:40:13+00:00",
    "Destinations": [
        {
            "Status": "ENABLING",
            "FileSystemId": "fs-0a8b2be428114d97c",
            "Region": "eu-west-2",
            "OwnerId": "123456789012,
         }
    ],
    "SourceFileSystemOwnerId": "123456789012"
}
```

Example : crea una configurazione di replica tra account

L'esempio seguente crea una configurazione di replica in cui i file system di origine e di destinazione sono diversi. Account AWS L'ID del file system di origine *fs-0123456789abcdef1* nell'account *555666777888* viene replicato nell'ID del file system *fs-0a8b2be428114d97c* nell'account. *123456789012* L'esempio specifica l'Amazon Resource Name (ARN) del file system di destinazione e l'ARN del ruolo IAM nell'account di origine che consente ad Amazon EFS di eseguire la replica per suo conto. Poiché non viene specificata alcuna chiave KMS, il file system di destinazione

viene crittografato utilizzando la chiave di servizio predefinita AWS KMS dell'account (). `aws/elasticfilesystem`

```
aws efs
--region $REGION
--endpoint $ENDPOINT create-replication-configuration
--source-file-system-id fs-0123456789abcdef1
--destinations Region=eu-west-2,FileSystemId=arn:aws:elasticfilesystem:eu-west-2:123456789012:file-system/fs-0a8b2be428114d97c,RoleArn=arn:aws:iam::555666777888:role/cross-account-replication
```

La AWS CLI risposta è la seguente:

```
{
    "SourceFileSystemId": "fs-0123456789abcdef1",
    "SourceFileSystemRegion": "us-east-1",
    "SourceFileSystemArn": "arn:aws:elasticfilesystem:us-east-1:555666777888:file-system/fs-0123456789abcdef1",
    "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:us-east-1:555666777888:file-system/fs-0123456789abcdef1",
    "CreationTime": "2024-10-20T20:40:13+00:00",
    "Destinations": [
        {
            "Status": "ENABLING",
            "FileSystemId": "fs-0a8b2be428114d97c",
            "Region": "eu-west-2",
            "OwnerId": "123456789012,
            "RoleArn": "arn:aws:iam::555666777888:role/cross-account-replication"
        }
    ],
    "SourceFileSystemOwnerId": "555666777888"
}
```

Replica dei file system EFS su più account AWS

È possibile replicare i file system EFS su Account AWS. La replica su più account migliora la resilienza e l'affidabilità complessive delle strategie di disaster recovery (DR) e può aiutare a soddisfare i requisiti di conformità aziendali.

Ad esempio, le politiche di conformità potrebbero richiedere l'utilizzo di account diversi per ambienti diversi (ad esempio produzione, gestione temporanea e disaster recovery (DR)). Oppure potresti

scoprire che la replica tra diversi Account AWS offre un isolamento più forte, un controllo più granulare sulle autorizzazioni e sulle politiche di accesso e un controllo più diretto delle risorse. Se l'account di produzione è compromesso (ad esempio da violazioni della sicurezza, errori di configurazione o minacce interne), avere i server DR in un account separato può impedire all'aggressore di accedervi, ridurre la portata degli incidenti di sicurezza e ridurre al minimo il rischio di modifiche non autorizzate.

La replica trasversale richiede una configurazione aggiuntiva di sicurezza e policy. Account AWS Invece di utilizzare ruoli collegati ai servizi per eseguire la replica tra account, devi creare un ruolo IAM che dia ad Amazon EFS l'autorizzazione a eseguire la replica nell'account di destinazione. È inoltre necessario creare politiche sui file system che si desidera condividere tra gli account. Dopo aver creato le policy del ruolo e del file system IAM, crei la configurazione di replica.

Argomenti

- Crea un ruolo IAM con una policy di fiducia personalizzata
- Crea politiche sui file system di origine e di destinazione
- Crea la configurazione di replica

Crea un ruolo IAM con una policy di fiducia personalizzata

Affinché Amazon EFS esegua la replica tra account per conto dell'account di origine, è necessario creare un ruolo IAM sull'account di origine. Il ruolo deve avere una politica di `elasticfilesystem.amazonaws.com` fiducia per consentire ad Amazon EFS di assumere il ruolo e agire come responsabile del servizio. Il ruolo deve contenere tutte le autorizzazioni IAM necessarie per eseguire la replica (vediAutorizzazioni IAM richieste) e concedere l'autorizzazione esplicita per la replica sul file system dell'account di destinazione.

Prerequisiti

È necessario creare sia il file system di origine che il file system di destinazione nella configurazione di replica prima di poter creare il ruolo IAM per l'account di origine. Amazon EFS non può creare automaticamente il file system di destinazione durante la replica. Inoltre, devi conoscere e fornire l'Amazon Resource Name (ARN) per ogni file system.

Per creare il ruolo IAM per la replica tra account

Di seguito sono riportati i passaggi generali per la creazione di un ruolo IAM con policy di fiducia personalizzate per la replica tra account con Amazon EFS. Per step-by-step istruzioni sulla creazione

di un ruolo IAM, consulta Creare un ruolo utilizzando politiche di fiducia personalizzate nella Guida per l'AWS Identity and Access Management utente.

1. Nella AWS Identity and Access Management console dell'account di origine, crea un ruolo IAM che utilizzi la seguente politica di fiducia. Per istruzioni, consulta Creare un ruolo utilizzando criteri di fiducia personalizzati nella Guida per l'utente di AWS Identity and Access Management.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "elasticfilesystem.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Dopo aver creato il ruolo, assegna le seguenti autorizzazioni per il ruolo. Sostituisci `DESTINATION_FILE_SYSTEM_ARN` con l'ARN del file system di destinazione e sostituisci `SOURCE_FILE_SYSTEM_ARN` con l'ARN del file system di origine. Per istruzioni sull'assegnazione delle autorizzazioni al ruolo, consulta Creazione di politiche utilizzando l'editor JSON.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action":[
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:CreateReplicationConfiguration",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticfilesystem:DeleteReplicationConfiguration",
                "elasticfilesystem:ReplicationWrite"
            ],
            "Resource": "DESTINATION_FILE_SYSTEM_ARN"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "elasticfilesystem:ReplicationRead",
                "elasticfilesystem:DescribeFileSystems"
            ],
            "Resource": "SOURCE_FILE_SYSTEM_ARN"
        }
    ]
}
```

3. Copia o annota l'ARN per il ruolo IAM. È necessario fornire l'ARN quando si crea la configurazione di replica.

Crea politiche sui file system di origine e di destinazione

Per condividere i file system tra più account in Amazon EFS, devi assegnare policy sia al file system di destinazione che a quello di origine. Le politiche concedono o limitano l'accesso tra account al file system a cui vengono applicate. Solo i proprietari di account autorizzati a modificare i file system possono assegnare policy al file system del proprio account.

> **Important**
>
> Oltre a concedere o limitare l'accesso tra gli account, le policy devono concedere altre autorizzazioni necessarie ai client per lavorare con i file system, come. `elasticfilesystem:ClientMount` In caso contrario, il file system potrebbe essere inaccessibile ai client. Per esempi di policy, consulta Esempi di policy basate sulle risorse per Amazon EFS.

Politica per il file system di destinazione

Per consentire all'account di origine l'autorizzazione alla replica nel file system di destinazione e per eliminare la configurazione di replica dall'account di destinazione, è necessario creare la seguente politica sul file system di destinazione. Sostituisci `SOURCE_ACCOUNT_ROOT` con l'ID dell'account proprietario del file system di origine.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
     {
        "Sid": "Permissions for source account calls",
        "Effect": "Allow",
        "Principal": {
        "AWS": "SOURCE_ACCOUNT_ROOT"
       },
     "Action": [
         "elasticfilesystem:DescribeFileSystems",
         "elasticfilesystem:CreateReplicationConfiguration",
         "elasticfilesystem:DescribeReplicationConfigurations",
         "elasticfilesystem:DeleteReplicationConfiguration",
         "elasticfilesystem:ReplicationWrite"
         ],
      "Resource": "DESTINATION_FILE_SYSTEM_ARN"
      }
   ]
}
```

Politica per il file system di origine

Per consentire all'account di destinazione l'autorizzazione a eliminare la configurazione di replica dall'account di origine, è necessario assegnare la seguente policy al file system di origine. Sostituiscilo `DESTINATION_ACCOUNT_ROOT` con l'ID dell'account proprietario del file system di destinazione.

```
{
    "Version": "2012-10-17",
    "Id": "efs-policy",
    "Statement": [
        {
            "Sid": "Permission to delete the replication by the destination account",
            "Effect": "Allow",
            "Principal": {
                "AWS": "DESTINATION_ACCOUNT_ROOT"
            },
            "Action": "elasticfilesystem:DeleteReplicationConfiguration",
            "Resource": "SOURCE_FILE_SYSTEM_ARN"
        }
    ]
}
```

Per creare la politica del file system

Eseguire i passaggi seguenti sia per il file system di destinazione che per quello di origine, utilizzando le politiche della sezione precedente.

1. Accedi a AWS Management Console con l'account proprietario del file system, quindi apri la console Amazon EFS nella console Amazon EFS.
2. Apri il file system:
   a. Nel pannello di navigazione a sinistra, scegli File system.
   b. Nell'elenco File system, scegli il file system.
3. Nella scheda Politica del file system, scegli Modifica.
4. Incolla la policy nell'editor di policy {Json}, quindi scegli Salva.

Crea la configurazione di replica

Dopo aver creato il ruolo IAM e aggiunto le policy del file system ai file system di origine e destinazione, segui le istruzioni Configurazione della replica su un file system EFS esistente per creare la configurazione di replica.

Visualizzazione dei dettagli della 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 Amazon EFS AWS CLI, l'API o Amazon CloudWatch.

- Nella console EFS, la proprietà Last synced 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.
- Nell'API AWS CLI o — La `LastReplicatedTimestamp` proprietà nell'`Destination`oggetto 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 metriche per Amazon EFS.

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.
`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.
`PAUSED`	La replica è sospesa a causa di un problema di configurazione. Vengono fornite informazioni aggiuntive sul problema. Alcuni problemi che causano la sospensione della replica includono: • Errore di autorizzazione. I problemi di autorizzazione impediscono ad Amazon EFS di eseguire la replica. Assicurati che il ruolo IAM utilizzato per creare la configurazione di replica sia autorizzato a eseguire la replica. Assicurati inoltre che le policy del file system siano corrette. • AWS l'account non è disponibile. Assicurati che gli account di origine e di destinazione siano impostati come appropriati Regioni AWS e non siano sospesi. Per ulteriori informazioni, consulta Specificare quali tipi di Regioni AWS account possono essere utilizzati dal proprio account nella Guida AWS generale di riferimento. • La chiave KMS per il file system di origine o di destinazione non è accessibi le. Assicurati che la chiave KMS assegnata a ciascun file system sia accessibile. Per ulteriori informazioni, consulta Gestione delle chiavi KMS per i file system EFS.
`ERROR`	La configurazione di replica è in uno stato di errore ed è irreversibile. È necessario eliminare la configurazione di replica e crearne una nuova.

Stato di replica	Descrizione
	Vengono fornite ulteriori informazioni sul problema. Per la replica tra account o tra regioni, l'errore può essere causato dal fatto che la configurazione di replica è stata eliminata dall'altra o. Account AWS Regione AWS

Utilizzo della console

1. Apri la console Amazon Elastic File System all'indirizzo 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. Amazon EFS visualizza i dettagli sulla causa dello stato di pausa o di errore.
   - 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), al luogo Regione AWS in cui si trova e alla relativa autorizzazione. Un file system di origine ha l'autorizzazione In scrittura e un file system di destinazione ha l'autorizzazione di Sola lettura.

Utilizzando il AWS CLI

Per visualizzare una configurazione di replica, utilizzare il `describe-replication-configurations` comando. È possibile visualizzare la configurazione di replica per un file system

specifico o tutte le configurazioni di replica per un particolare file system in un. Account AWS Regione AWS Il comando API equivalente è DescribeReplicationConfigurations.

Se lo stato della configurazione di replica è `PAUSED` o`ERROR`, nel parametro vengono restituite informazioni sulla causa del problema e su come risolverlo. `StatusMessage`

Example : visualizza la configurazione di replica per un file system specifico

L'esempio seguente descrive la configurazione di replica per il file system. `fs-0123456789abcdef1`

```
aws efs describe-replication-configurations --file-system-id fs-0123456789abcdef1
```

Le AWS CLI risposte sono le seguenti.

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

Example : Visualizza la configurazione di replica per tutte le configurazioni di replica in un account

L'esempio seguente descrive la configurazione di replica per tutte le configurazioni di replica per un account in un file system. Regione AWS

```
aws efs describe-replication-configurations
```

Le AWS CLI risposte sono le seguenti.

```
 {
"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 Utilizzo della replica.

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 Amazon EFS AWS CLI, o l'API.

Per le repliche tra account o tra regioni, Amazon EFS elimina la configurazione di replica sia dagli account o dalle regioni di origine che di destinazione. Se c'è un problema di configurazione o di autorizzazioni che impedisce ad Amazon EFS di eliminare la configurazione di replica da entrambi i lati, puoi eliminare la configurazione solo dal lato locale (l'account o la regione da cui viene eseguita l'eliminazione). L'eliminazione della configurazione locale rende irrecuperabile la configurazione nell'altro account o regione.

Utilizzo della console

1. Apri la console Amazon Elastic File System all'indirizzo 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.

   Se stai eliminando una configurazione di replica tra account e c'è un problema che ti impedisce di eliminare la configurazione sia dal lato di origine che da quello di destinazione, puoi scegliere l'opzione per eliminare solo la configurazione di questo file system.

   > **Note**
   >
   > Elimina la configurazione del file system solo se Amazon EFS non è in grado di eliminare la configurazione di replica sia nell'account o nella regione di origine che di destinazione. L'eliminazione della configurazione locale rende irrecuperabile la configurazione nell'altro account o regione.

Usando il AWS CLI

Per eliminare una configurazione di replica, utilizzare la `delete-replication-configuration` CLI. Il comando API equivalente è DeleteReplicationConfiguration.

L'esempio seguente elimina la configurazione di replica per il file system di origine. `fs-0123456789abcdef1`

```
aws efs --region us-west-2 delete-replication-configuration \
--source-file-system-id fs-0123456789abcdef1
```

Se un problema di configurazione o di autorizzazioni impedisce ad Amazon EFS di eliminare la configurazione di replica da entrambi i lati, puoi eliminare la configurazione solo dal lato locale (l'account o la regione da cui viene eseguita l'eliminazione). L'eliminazione della configurazione locale rende irrecuperabile la configurazione nell'altro account o regione. Il parametro API equivalente è `DeletionMode` e il valore è. `LOCAL_CONFIGURATION_ONLY`

L'esempio seguente elimina la configurazione di replica per il file system di origine *fs-0123456789abcdef1* solo dal lato locale.

```
aws efs --region us-west-2 delete-replication-configuration \
```

```
--source-file-system-id fs-0123456789abcdef1
--deletion-mode LOCAL_CONFIGURATION_ONLY
```

Utilizzo della replica

In caso di emergenza o durante l'esecuzione di esercizi quotidiani di gioco, 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. Una volta mitigato il problema o terminata l'esercitazione del giorno di gioco, puoi continuare a utilizzare la replica come file system principale oppure puoi eseguire un failback per riprendere le operazioni sul file system principale 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 di replica.

Protezione dei dati 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. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e 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 Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con EFS o altro Servizi AWS utilizzando la console, l'API o AWS SDKs. 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
- Gestione delle identità e degli accessi per Amazon EFS
- Utilizzo di IAM per controllare l'accesso ai file system
- Controllo dell'accesso di rete ai file system EFS per i client NFS
- Utenti, gruppi e autorizzazioni a livello di Network File System (NFS)
- Utilizzo dei punti di accesso
- Blocco dell'accesso pubblico ai file system EFS
- Convalida della conformità per Amazon EFS
- Resilienza in Amazon EFS
- Isolamento di rete per Amazon EFS

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.

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

- AWS KMS
- Crittografia dei dati a riposo
- Crittografia dei dati in transito
- Risoluzione dei problemi di crittografia

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 dati a riposo - Amazon EFS utilizza Chiave gestita da AWS per Amazon EFS, `aws/elasticfilesystem`, per criptare e decriptare i metadati del file system (cioè i nomi dei file, i nomi delle directory e i contenuti delle directory).
- 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 della chiave 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 Gestione dell'accesso ai file system crittografati.

> **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, nei AWS CloudTrail log relativi alle AWS KMS azioni vengono visualizzati AWS account IDs

specifici di Amazon EFS. 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 .Il seguente elenco descrive tutte le autorizzazioni correlate a AWS KMS che sono richieste o comunque 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 sovvenzioni, consulta Grants AWS KMS nella Developer Guide.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 a riposo

Puoi creare file system crittografati utilizzando AWS Management Console AWS CLI, o programmaticamente tramite l'API Amazon EFS o una delle. AWS SDKs 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.

Imposizione della creazione di file system 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 del servizio (SCPs) 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.

> **Note**
>
> La crittografia a riposo non è abilitata per impostazione predefinita quando si crea un nuovo file system utilizzando l'API AWS CLI, e SDKs. Per ulteriori informazioni, consulta Crea usando il AWS CLI.

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 gli elementi essenziali AWS KMS della crittografia nella Guida per gli AWS Key Management Service sviluppatori.

Crittografia dei dati in transito

L'abilitazione della crittografia dei dati in transito per il tuo file system EFS viene effettuata abilitando Transport Layer Security (TLS) quando monti il file system utilizzando l'helper di montaggio di Amazon EFS. Per ulteriori informazioni, consulta Montaggio dei file system EFS utilizzando l'helper di montaggio 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.

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 connetterti al tuo file system EFS sulla porta 2049 utilizzando 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 21049, 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 queste versioni di Linux, il montaggio di un file system EFS tramite TLS non riesce.
> 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 EFS corrisponde a quale punto di montaggio locale, è possibile utilizzare il seguente comando. 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 assicura che il processo di stunnel di ogni montaggio sia in esecuzione e interrompe lo stunnel quando il file system EFS viene smontato. Se per qualsiasi motivo un processo stunnel si arresta in modo inatteso, il processo watchdog lo riavvia.

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
- Encrypted-at-rest il file system 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.

Encrypted-at-rest il file system 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.

Gestione delle identità e degli accessi per Amazon EFS

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a 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 software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Funzionamento di Amazon Elastic File System con IAM
- Esempi di policy basate su identità per Amazon Elastic File System
- Esempi di policy basate sulle risorse per Amazon EFS
- AWS politiche gestite per Amazon EFS
- Utilizzo di tag con Amazon EFS
- Utilizzo di ruoli collegati ai servizi per Amazon EFS
- Risoluzione dei problemi relativi all'identità e all'accesso di Amazon Elastic File System

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto 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 funzionalità 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 il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per

creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale 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 IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno 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 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, potresti avere un gruppo denominato IAMAdminse concedere a quel 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 Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente 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 Create a role for a third-party identity provider (federation) nella Guida per l'utente 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 informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
- Ruolo di servizio: 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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente 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 al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. È preferibile archiviare le chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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 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.

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'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'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 operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità 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 IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di

Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.

- 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 IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

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
ACLs	No
ABAC (tag nelle policy)	Parziale

Funzionalità IAM	Supporto di Amazon EFS
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Amazon EFS e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

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 operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente 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, consulta Esempi di policy basate su identità per Amazon Elastic File System.

Policy basate su risorse all'interno di Amazon EFS

Supporta le policy basate sulle risorse: sì

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente 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 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 sulle risorse per Amazon EFS.

Operazioni delle policy per Amazon EFS

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni 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, consulta 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 AWS JSON per specificare chi ha accesso a cosa. In altre parole, 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'operazione. 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). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse Amazon EFS e relativi ARNs, consulta Resources defined by Amazon Elastic File System nel Service Authorization Reference. 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 AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di 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.

ACLs in Amazon EFS

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Amazon EFS

Supporta ABAC (tag nelle policy): parzialmente

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente 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 accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni delle entità principali tra servizi per Amazon EFS

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta 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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità 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 ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

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 possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire 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 (console) nella Guida per l'utente IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Amazon EFS, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Elastic File System nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Amazon EFS
- Esempio: consentire agli utenti di visualizzare le loro autorizzazioni
- Esempio: applicazione della creazione di file system crittografati
- Esempio: applicazione della creazione di file system decrittografati

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 azioni possono comportare costi aggiuntivi per

l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le politiche AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente 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 il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente 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 consentirti di elencare e visualizzare i dettagli sulle risorse Amazon EFS presenti 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 consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la console Amazon EFS, collega anche la policy `AmazonElasticFileSystemReadOnlyAccess` AWS gestita di 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 AWS politiche gestite 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 cpllegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l' AWS CLI API o. 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 l' AWS Management Console AWS API o AWS CLI l'SDK:

```
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 l' AWS Management Console AWS CLI AWS API o l'SDK:

```
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 AWS Organizations servizio (SCP). Per ulteriori informazioni sulle politiche di controllo dei servizi in AWS Organizations, consulta le politiche di controllo dei servizi nella Guida per l'AWS Organizations utente.

Esempi di policy basate sulle risorse per Amazon EFS

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 specifico AWS
- Esempio: concedere accesso in sola lettura
- Esempio: assicurati che i client connessi mantengano l'accesso dopo aver configurato la replica tra account
- Esempio: concedere l'accesso a un punto di accesso EFS

Esempio: concedere l'accesso in lettura e scrittura a un ruolo specifico AWS

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: 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 Abilita il root squashing utilizzando l'autorizzazione IAM per i client NFS.

Esempio: assicurati che i client connessi mantengano l'accesso dopo aver configurato la replica tra account

È possibile utilizzare la seguente politica basata sulle risorse per garantire che tutti i client connessi al file system mantengano l'accesso dopo aver impostato la replica tra account per il file system. Per ulteriori informazioni sulla replica tra account, vedere Replica dei file system EFS su più account AWS

I seguenti requisiti si applicano alla creazione della policy.

- Utilizzate l'helper di montaggio EFS per montare il file system. Se il file system viene montato utilizzando il client NFS, ai client connessi verrà negato l'accesso a causa di errori del server.
- Utilizzate l'opzione -o iam o -o tls nel comando mount per passare le credenziali al mount target EFS.

```
{
    "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"
            ],
            "Resource": "arn:aws:elasticfilesystem:us-east-2:111122223333:file-system/
fs-1234abcd",
            "Condition": {
               "Bool": {
                   "elasticfilesystem:AccessedViaMountTarget": "true"
               }
```

```
            }
        }
    ]
}
```

Esempio: 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.

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

AWS politiche gestite per Amazon EFS

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti 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 politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSService RoleForAmazonElasticFileSystem

Amazon EFS utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForAmazonElasticFileSystem` per consentire ad Amazon EFS di gestire AWS le risorse per tuo conto. Questo ruolo si fida che il `elasticfilesystem.amazonaws.com` servizio assuma il ruolo. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon EFS.

AWS politica gestita: AmazonElasticFileSystemFullAccess

È possibile allegare la policy `AmazonElasticFileSystemFullAccess` alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo ad Amazon EFS e l'accesso ai AWS servizi 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 ai 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 () VPCs e attributi VPC associati a un file system 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 AWS le risorse per conto dell'utente.
- `iam:PassRole`— Concede l'autorizzazione a trasferire un ruolo IAM ad Amazon EFS.

Per visualizzare le autorizzazioni per questa policy, consulta AmazonElasticFileSystemFullAccessla AWS Managed Policy Reference Guide.

AWS politica gestita: AmazonElasticFileSystemReadOnlyAccess

È possibile allegare la policy `AmazonElasticFileSystemReadOnlyAccess` alle identità IAM.

Questa politica garantisce l'accesso in sola lettura 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 responsabili di visualizzare le zone di disponibilità, le interfacce di rete e i relativi attributi, i gruppi di sicurezza, le sottoreti VPCs e i relativi attributi nella console Amazon EFS.
- `kms`— Consente ai responsabili di elencare gli alias per le AWS KMS chiavi nella console Amazon EFS.

Per visualizzare le autorizzazioni per questa policy, consulta la AWS Managed Policy AmazonElasticFileSystemReadOnlyAccessReference Guide.

AWS politica gestita: AmazonElasticFileSystemClientFullAccess

Puoi collegare la policy `AmazonElasticFileSystemClientFullAccess` anche alle tue entità IAM.

Questa politica garantisce l'accesso dei client di lettura e scrittura ai file system EFS. Questa policy consente ai client NFS di montare, leggere e scrivere su file system EFS.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonElasticFileSystemFullAccessla AWS Managed Policy Reference Guide.

AWS politica gestita: AmazonElasticFileSystemClientReadWriteAccess

Puoi collegare la policy `AmazonElasticFileSystemClientReadWriteAccess` anche alle tue entità IAM.

Questa politica garantisce l'accesso dei client di lettura e scrittura ai file system EFS. Questa policy consente ai client NFS di montare, leggere e scrivere su file system EFS.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonElasticFileSystemClientReadWriteAccessla AWS Managed Policy Reference Guide.

Aggiornamenti di Amazon EFS alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon EFS da quando questo servizio ha iniziato a tracciare queste 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	Policy: AmazonElasticFileSystemFullAccess Amazon EFS ha aggiunto quanto segue: • `ReplicationRead` e `ReplicationWrite` autorizzare la lettura e la scrittura dei dati del file system per la replica. • `iam:PassRole` autorizzare Amazon EFS a creare configurazioni di replica.	7 novembre 2024

Modifica	Descrizione	Data
Aggiornamento a una policy esistente	Policy: AmazonElasticFileSystemServiceRolePolicy Amazon EFS ha aggiunto `ReplicationRead` e `ReplicationWrite` concesso l'autorizzazione a leggere e scrivere i dati del file system per la replica.	7 novembre 2024
Aggiornamento a una policy esistente	Policy: AmazonElasticFileSystemReadOnlyAccess Amazon EFS ha aggiunto l'`ReplicationRead` azione per autorizzare la lettura dei dati del file system per la replica.	7 novembre 2024
Aggiornamento a una policy esistente	Policy: AmazonElasticFileSystemReadOnlyAccess Amazon EFS ha aggiunto nuove autorizzazioni che consentono agli account di origine e destinazione di accedere ai file system per le repliche tra account.	7 agosto 2024
Aggiornamento a una policy esistente	Policy: AmazonElasticFileSystemFullAccess 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	Policy: AmazonElasticFileSystemServiceRolePolicy 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 configura zioni di replica dei file system per conto dell'utente.	25 gennaio 2022

Modifica	Descrizione	Data
Aggiornamento a una policy esistente	Policy: AmazonElasticFileSystemReadOnlyAccess 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 configura zioni di replica dei file system.	25 gennaio 2022
Aggiornamento a una policy esistente	Policy: AmazonElasticFileSystemFullAccess Amazon EFS ha aggiunto nuove autorizzazioni per consentire ai committenti di creare, descrivere ed eliminare le repliche di Amazon EFS. Le autorizza zioni sono necessarie per consentire agli utenti di gestire le configurazioni di replica dei file system.	25 gennaio 2022
Monitoraggio delle informazioni iniziato	Policy: AmazonElasticFileSystemClientReadWri teAccess Concede privilegi di lettura e scrittura sui file system Amazon EFS ai client NFS.	3 gennaio 2022
Monitoraggio delle informazioni iniziato	Policy: AmazonElasticFileSystemServiceRolePolicy Autorizzazioni del ruolo collegato ai servizi per Amazon EFS.	8 ottobre 2021
Aggiornamento a una policy esistente	Policy: AmazonElasticFileSystemFullAccess 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

Modifica	Descrizione	Data
Aggiornamento a una policy esistente	Policy: AmazonElasticFileSystemReadOnlyAccess Amazon EFS ha aggiunto nuove autorizzazioni per consentire alle entità principali di descrivere le preferenze dell'account Amazon EFS. Le autorizzazioni 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 tracciare le modifiche per le sue politiche AWS gestite.	7 maggio 2021

Utilizzo di tag con Amazon EFS

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

- Etichettatura delle risorse EFS
- Controllo dell'accesso in base ai tag di una risorsa
- A cosa serve ABAC? AWS nella Guida per l'utente di IAM

> **Note**
>
> La replica Amazon EFS non supporta l'uso dei tag per il controllo degli accessi basato su attributi (ABAC).

Per applicare tag alle risorse Amazon EFS durante la creazione, gli utenti devono disporre di determinate autorizzazioni AWS Identity and Access Management (IAM).

Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione

Le seguenti operazioni API di Amazon EFS per l'assegnazione di tag al momento della creazione consentono di specificare tag quando crei la risorsa.

- `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 la risorsa, come `elasticfilesystem:CreateAccessPoint` o `elasticfilesystem:CreateFileSystem`. Se i tag sono specificati nell'azione di creazione della risorsa, AWS esegue un'autorizzazione aggiuntiva sull'`elasticfilesystem:TagResource`azione per verificare se gli utenti sono autorizzati a 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 con tag solo durante la creazione. 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 di Amazon EFS

Per controllare l'accesso alle operazioni e risorse di gateway, è possibile utilizzare le policy IAM basate su tag. È possibile fornire il controllo in due modi:

- È possibile controllare l'accesso alle risorse Amazon EFS in base ai tag su queste risorse.
- Puoi controllare quali tag possono essere trasferiti in una condizione di richiesta IAM.

Per informazioni su come utilizzare i tag per controllare l'accesso alle AWS risorse, consulta Controlling access using tags nella IAM User Guide.

Controllo dell'accesso in base ai tag di una risorsa

Per controllare le operazioni che un utente o un ruolo può eseguire su una risorsa di Amazon EFS, è possibile usare i tag sulla risorsa. Ad esempio, è possibile consentire o negare operazioni API specifiche su una risorsa di gateway di file 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 policy di esempio consente all'utente di creare un file system solo quando lo contrassegna 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 Policy: elimina i file system con tag specifici

La seguente policy di esempio consente a un utente di eliminare 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 servizio AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente ad Amazon EFS. Il ruolo predefinito collegato al servizio Amazon EFS include le autorizzazioni richieste dal servizio per chiamare altri Servizi AWS utenti per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Amazon EFS perché consente di evitare l'aggiunta manuale delle autorizzazioni necessarie. Amazon EFS definisce le autorizzazioni dei ruoli collegati al servizio e solo Amazon EFS può assumere i suoi ruoli. Le autorizzazioni definite includono

la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare il ruolo collegato ai servizi Amazon EFS solo dopo aver eliminato il 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 al servizio consente di rendere visibili tutte le chiamate API. AWS CloudTrail In questo modo il monitoraggio e i requisiti di controllo sono più semplici perché è possibile tenere traccia di tutte le azioni che Amazon EFS esegue a tuo nome. Per ulteriori informazioni, consulta Voci di log per ruoli collegati ai servizi EFS.

Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Autorizzazioni del ruolo collegato ai servizi per Amazon EFS

Amazon EFS utilizza il ruolo collegato al servizio denominato AWSServiceRoleForAmazonElasticFileSystemper consentire ad Amazon EFS di richiamare e gestire AWS risorse per conto dei tuoi file system EFS.

Il ruolo AWSService RoleForAmazonElasticFileSystem collegato al servizio si fida che l'utente assuma il `elasticfilesystem.amazonaws.com` ruolo.

La policy delle autorizzazioni del ruolo consente ad Amazon EFS di eseguire le seguenti operazioni:

```
{
    "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",
                "elasticfilesystem:ReplicationRead",
                "elasticfilesystem:ReplicationWrite"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> È necessario configurare manualmente le autorizzazioni IAM per AWS KMS quando si crea un nuovo file system EFS crittografato a riposo. Per ulteriori informazioni, consulta Crittografia dei dati a riposo.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta le autorizzazioni dei ruoli collegati ai servizi nella Guida per l'utente IAM.

Creazione di un ruolo collegato ai servizi per Amazon EFS

Nella maggior parte dei casi, non è necessario creare manualmente un ruolo collegato al servizio. Quando crei obiettivi di montaggio o una configurazione di replica per il tuo file system EFS nell'API AWS Management Console AWS CLI, nella o nell' AWS API, Amazon EFS crea il ruolo collegato al servizio per te.

Inoltre, se lo service-linked-role elimini manualmente e poi devi crearlo di nuovo, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account. Quando crei obiettivi di montaggio o una configurazione di replica per il tuo file system EFS, Amazon EFS crea il ruolo collegato al servizio per te.

Se, tuttavia, Amazon EFS non crea service-linked-role o se hai iniziato a utilizzare Amazon EFS prima che supportasse i ruoli collegati ai servizi, puoi creare manualmente il ruolo collegato al servizio. Per istruzioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM.

Modifica di un ruolo collegato ai servizi per Amazon EFS

Amazon EFS non consente di modificare il ruolo collegato al servizio `AWSServiceRoleForAmazonElasticFileSystem`. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Update a service-linked role nella IAM User Guide.

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. Per ulteriori informazioni, consulta Pulisci le risorse e proteggi il tuo account AWS.

> **Note**
>
> Se il servizio Amazon EFS utilizza tale ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione non riesca. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSService RoleForAmazonElasticFileSystem servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi Amazon EFS

Amazon EFS supporta l'utilizzo di ruoli collegati al servizio in tutti i luoghi in Regioni AWS cui il servizio è disponibile. Per ulteriori informazioni, consulta gli endpoint AWS del servizio nella Guida per l'Riferimenti generali di AWS utente.

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
- Non sono autorizzato a eseguire iam: PassRole
- Desidero consentire a persone esterne Account AWS a me di accedere alle mie risorse Amazon EFS

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`*.

Se hai bisogno di assistenza, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire l'operazione `iam:PassRole`, per poter passare un ruolo ad Amazon EFS dovrai aggiornare le policy.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

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`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero consentire a persone esterne Account AWS a me 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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon EFS supporta queste funzionalità, consulta Funzionamento di Amazon Elastic File System con IAM.
- Per scoprire come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in Account AWS un altro Account AWS di tua proprietà nella IAM User Guide.

- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Utilizzo di IAM per controllare l'accesso ai file system

È possibile utilizzare policy di identità e policy delle risorse IAM per controllare l'accesso del client 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 EFS al fine di utilizzare l'autorizzazione IAM per controllare l'accesso 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 di utilizzare	Booleano

Chiave di condizione EFS	Descrizione	Operatore
	TLS durante la connessione a un file system EFS.	
`aws:SourceIp`	Utilizzare questa chiave per confrontare l'indirizzo IP del richiedente con l'indirizzo IP specificato nella policy. La chiave di condizione `aws:SourceIp` può essere utilizzata solo per intervalli di indirizzi IP pubblici.	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 che non utilizzano destinazioni di montaggio del file system.	Booleano

Esempi di policy del file system

Per visualizzare esempi di policy dei file system di Amazon EFS, consulta Esempi di policy basate sulle risorse per Amazon EFS.

Controllo dell'accesso di rete ai file system 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. Puoi utilizzare i meccanismi di sicurezza a livello di rete disponibili con Amazon EC2, come le regole del gruppo di sicurezza VPC e la rete. ACLs Puoi anche utilizzare AWS IAM per controllare l'accesso NFS con una policy del file system EFS e policy basate sull'identità.

Argomenti

- Utilizzo dei gruppi di sicurezza VPC
- Utilizzo degli endpoint VPC di interfaccia in Amazon EFS

Utilizzo dei gruppi di sicurezza VPC

Quando usi Amazon EFS, specifichi gruppi di sicurezza VPC per le tue EC2 istanze e gruppi di sicurezza per gli obiettivi di montaggio EFS associati al file system. Un gruppo di sicurezza funge da firewall e le regole aggiunte definiscono il flusso di traffico. Nell'esercizio Guida introduttiva, hai creato un gruppo di sicurezza quando hai avviato l'istanza EFS. 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'esercizio Getting started. Tuttavia, per un sistema di produzione, è necessario configurare gruppi di sicurezza con autorizzazioni minime da utilizzare con Amazon EFS.

È possibile autorizzare l'accesso in entrata e in uscita verso il file system EFS. A tale scopo, aggiungi regole che consentono alle istanze EFS di connettersi al file system EFS tramite la destinazione di montaggio utilizzando la porta NFS (Network File System).

- Ogni EC2 istanza che installa il file system deve avere un gruppo di sicurezza con una regola che consenta l'accesso in uscita alla destinazione di montaggio sulla porta NFS.
- Il target di montaggio EFS deve disporre di un gruppo di sicurezza con una regola che consenta l'accesso in entrata da ogni EC2 istanza su cui si desidera montare il file system.

Porte di origine per lavorare con Amazon 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 stabilire una connessione di rete alla porta NFS (porta TCP 2049) di uno degli obiettivi di montaggio del file system. Analogamente, un NFSv4 client.1 può affermare un ID utente e di gruppo quando accede a un file system solo se è in grado di effettuare questa 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:
  - EC2 Istanze Amazon nell'Amazon VPC locale
  - EC2 istanze connesse VPCs
  - Server locali connessi a un Amazon VPC AWS Direct Connect tramite e AWS Virtual Private Network una (VPN)
- Liste di controllo dell'accesso alla rete (ACLs) per le sottoreti VPC del client e delle destinazioni di montaggio, per l'accesso dall'esterno delle sottoreti del target di montaggio — Per montare un file system, il client deve essere in grado di stabilire una connessione TCP alla porta NFS di una destinazione di montaggio e ricevere il traffico di ritorno.
- Regole dei gruppi di sicurezza VPC del client e delle destinazioni di montaggio, per tutti gli accessi: affinché un' EC2 istanza possa montare un file system, devono essere in vigore le seguenti regole del gruppo 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 Gestione dei target di montaggio.

Creazione dei gruppi di sicurezza

Per creare gruppi di sicurezza per EC2 istanze e destinazioni di montaggio EFS

Di seguito sono riportati i passaggi generali da eseguire durante la creazione dei gruppi di sicurezza per Amazon EFS. Per istruzioni sulla creazione dei gruppi di sicurezza, consulta Create a security group nella Amazon VPC User Guide.

1. Per le tue EC2 istanze, crea un gruppo di sicurezza con le seguenti regole:
   - Una regola in entrata che consente l'accesso in entrata che consente l'utilizzo di Secure Shell (SSH) da qualsiasi host. Facoltativamente, è possibile limitare l'indirizzo Source (Origine).
   - Una regola in uscita che consente a tutto il traffico di uscire. Quando si crea un gruppo di sicurezza, per impostazione predefinita viene creato con una regola in uscita, quindi non è necessario aggiungerne uno.
2. Per il tuo target di montaggio EFS, crea un gruppo di sicurezza con le seguenti regole:
   - Una regola in entrata che consente l'accesso dal gruppo EC2 di sicurezza. Identifica il gruppo EC2 di sicurezza come fonte.
   - Una regola in uscita per aprire la connessione TCP su tutte le porte NFS. Identifica il gruppo EC2 di sicurezza come destinazione.

Utilizzo degli endpoint VPC di interfaccia in Amazon EFS

Puoi stabilire una connessione privata tra il cloud privato virtuale (VPC, Virtual Private Cloud) e l'API Amazon EFS creando un endpoint VPC di interfaccia. L'endpoint fornisce connettività sicura all'API Amazon EFS senza richiedere un gateway Internet, un'istanza NAT o una connessione rete privata virtuale (VPN). Per ulteriori informazioni, consulta Accedere a un AWS servizio utilizzando un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Gli endpoint VPC dell'interfaccia sono alimentati da AWS PrivateLink, una funzionalità che consente la comunicazione privata tra AWS i servizi utilizzando indirizzi IP privati. Per utilizzarlo AWS PrivateLink, crea un endpoint VPC di interfaccia per Amazon EFS nel tuo VPC utilizzando la console Amazon VPC, l'API o l'interfaccia a riga di comando. In questo modo si crea un'interfaccia di rete elastica nella sottorete con un indirizzo IP privato che serve le richieste API Amazon EFS. Puoi anche accedere a un endpoint VPC da ambienti locali o da altri dispositivi AWS VPN, AWS Direct Connect

oppure VPCs tramite peering VPC. Per ulteriori informazioni, consulta Connect your VPC ai servizi utilizzando AWS PrivateLink nella Amazon VPC User Guide.

Creazione di un endpoint di interfaccia per Amazon EFS

Per creare un endpoint VPC di interfaccia per Amazon EFS, utilizzare una delle seguenti opzioni:

- **com.amazonaws.*region*.elasticfilesystem**: crea un endpoint per le operazioni API di Amazon EFS.
- **com.amazonaws.*region*.elasticfilesystem-fips**— Crea 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 gli endpoint e le quote di Amazon Elastic File System nel. Riferimenti generali di Amazon Web Services

Per ulteriori informazioni su come creare un endpoint di interfaccia, consulta Accedere a un AWS servizio utilizzando un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Creazione di una policy sugli endpoint VPC per Amazon EFS

Per controllare l'accesso all'API Amazon EFS, puoi allegare una policy AWS Identity and Access Management (IAM) al tuo endpoint VPC. La policy specifica quanto segue:

- Il principale che può eseguire azioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

Per ulteriori informazioni, consulta Controllo degli accessi agli endpoint VPC tramite le policy degli endpoint nella Guida per l'utente di Amazon VPC.

Nell'esempio seguente viene illustrata una policy di endpoint VPC che nega a chiunque l'autorizzazione per creare un file system 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": "*"
        }
    ]
}
```

Utenti, gruppi e autorizzazioni a livello di Network File System (NFS)

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.

Agli oggetti del file system EFS è associata una modalità in stile UNIX. 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 il codice numerico mappato IDs per verificare le autorizzazioni quando un utente tenta di accedere a un oggetto del file system.

> **Note**
>
> Il protocollo NFS supporta un massimo di 16 gruppi IDs (GIDs) per utente e gli eventuali gruppi aggiuntivi GIDs 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.

Argomenti

- Autorizzazioni di file e directory
- Esempi di casi d'uso e autorizzazioni del file system EFS
- Autorizzazioni ID utente e di gruppo per 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

Autorizzazioni di file e directory

I file e le directory in un file system EFS supportano le autorizzazioni di lettura, scrittura ed esecuzione standard in stile UNIX basate sull'ID utente e di gruppo dichiarato dal client di montaggio NFSv4 .1, a meno che non vengano sovrascritte da un punto di accesso EFS. Per ulteriori informazioni, consulta 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 nell'asserzione dell'ID utente e del gruppo. È possibile 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 file system e Creazione di access point.

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`.

Esempi di casi d'uso e autorizzazioni del file system EFS

Dopo aver creato un file system EFS e aver montato le destinazioni per il file system nel tuo VPC, puoi montare il file system remoto localmente sulla tua 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 step-by-step istruzioni, consultaTutorial: creazione di sottodirectory scrivibili per utente.
- Consenti agli utenti di scrivere nella directory principale del file system EFS. Un utente con privilegi di root può concedere ad altri utenti l'accesso al file system.
  - Per modificare la proprietà del file system EFS in un utente e un gruppo non root, utilizzare quanto segue:

    ```
    $ 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 EC2 istanze su cui è montato il file system.

Autorizzazioni ID utente e di gruppo per file e directory all'interno di un file system

I file e le directory in un file system EFS supportano le autorizzazioni standard di lettura, scrittura ed esecuzione in stile UNIX basate sull'ID utente e sul gruppo. IDs 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. È possibile utilizzare i punti di accesso EFS per sovrascrivere l'ID utente e il gruppo IDs utilizzati dal client NFS. Quando gli utenti tentano di accedere a file e directory, Amazon EFS controlla l'utente IDs e il gruppo IDs per verificare che ogni utente disponga dell'autorizzazione ad accedere agli oggetti. Amazon EFS li utilizza anche IDs per indicare il proprietario e il proprietario del gruppo per i nuovi file e directory 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' EC2 istanza, puoi assegnare qualsiasi ID utente numerico (UID) e ID di gruppo (GID) all'utente. Gli utenti numerici IDs sono impostati nel file sui sistemi Linux. `/etc/passwd` Il gruppo numerico IDs si trova nel `/etc/group` file. Questi file definiscono le mappature tra i nomi e. IDs Al di fuori dell' EC2 istanza, Amazon EFS non esegue alcuna autenticazione di questi IDs, incluso l'ID root 0.

Se un utente accede a un file system EFS da due EC2 istanze diverse, a seconda che l'UID dell'utente sia lo stesso o diverso in tali istanze, si riscontra un comportamento diverso, come segue:

- Se l'utente IDs è lo stesso su entrambe EC2 le istanze, Amazon EFS ritiene che indichi lo stesso utente, indipendentemente dall' EC2 istanza utilizzata. L'esperienza utente durante l'accesso al file system è la stessa in entrambe le EC2 istanze.
- Se l'utente IDs non è lo stesso in entrambe EC2 le istanze, Amazon EFS considera gli utenti come utenti diversi. L'esperienza utente non è la stessa quando si accede al file system EFS da due EC2 istanze diverse.
- Se due utenti diversi su EC2 istanze diverse condividono un ID, Amazon EFS li considera lo stesso utente.

Potresti prendere in considerazione la possibilità di gestire le mappature degli ID utente tra le istanze in modo coerente EC2 . 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 utilità NFS del sistema operativo includono un demone chiamato ID Mapper che gestisce la mappatura tra i nomi utente e. IDs Su Amazon Linux, il daemon viene chiamato `rpc.idmapd` e su Ubuntu viene chiamato `idmapd`. Traduce utente e gruppo IDs in nomi e viceversa. Tuttavia, Amazon EFS si occupa solo di dati numerici. IDs Ti consigliamo di disattivare questo processo sulle tue EC2 istanze. 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, consulta Utilizzo di IAM per controllare l'accesso ai file system.

Abilita il root squashing utilizzando l'autorizzazione IAM per i client NFS

Puoi configurare Amazon EFS per impedire l'accesso root al tuo file system EFS per tutti i AWS principali ad eccezione di una singola workstation di gestione. A tale scopo è possibile configurare l'autorizzazione AWS Identity and Access Management (IAM) per i client NFS (Network File System).

A tale scopo è necessario configurare due policy di autorizzazione IAM, come riportato di seguito:

- 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 EC2 gestione Amazon che richiede l'accesso root al file system utilizzando un profilo di EC2 istanza. Per ulteriori informazioni sui profili delle EC2 istanze Amazon, consulta Use instance profiles nella AWS Identity and Access Management User Guide.
- Assegna la policy `AmazonElasticFileSystemClientFullAccess` AWS gestita al ruolo IAM della workstation di gestione. Per ulteriori informazioni sulle politiche AWS gestite per Amazon EFS, consultaGestione delle identità e degli accessi per Amazon EFS.

Per abilitare il root squashing root l'autorizzazione IAM per i client NFS, utilizzare le procedure seguenti.

Disattivazione dell'accesso root al file system

1. Apri la console Amazon Elastic File System all'indirizzo https://console.aws.amazon.com/efs/.
2. Seleziona File system.
3. Scegli il file system su cui vuoi abilitare il root squashing.
4. Nella pagina dei dettagli del file system, scegli Policy del file system, quindi scegli Modifica. Viene visualizzata la pagina Policy del file system.
5. Scegli Impedisci l'accesso root per impostazione predefinita* in Opzioni di policy. L'oggetto JSON della policy viene visualizzato nell'editor delle policy.
6. Scegliere 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 gestita `AmazonElasticFileSystemClientFullAccess` al ruolo della workstation, concede l'accesso root alla workstation in base alla relativa policy 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. Crea un ruolo per Amazon EC2 chiamato`EFS-client-root-access`. IAM crea un profilo di istanza con lo stesso nome del EC2 ruolo che hai creato.
3. Assegna la policy AWS gestita `AmazonElasticFileSystemClientFullAccess` al EC2 ruolo che hai 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. Associa il profilo dell' EC2 istanza all'istanza che stai utilizzando come workstation di gestione, come descritto di seguito. Per ulteriori informazioni, consulta Allegare un ruolo IAM a un'istanza nella Amazon EC2 User Guide for Linux Instances.

   a. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.

   b. Nel riquadro di navigazione, scegliere Instances (Istanze).

   c. Seleziona 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'helper di montaggio di EFS sulla workstation di gestione. Per ulteriori informazioni sull'EFS mount helper mount helper e sul amazon-efs-utils pacchetto, vedere. Installazione del client Amazon EFS

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' EC2 istanza Amazon per montare automaticamente il file system con l'autorizzazione IAM. Per maggiori informazioni sul montaggio di un file system EFS con autorizzazione IAM, consulta Montaggio con autorizzazione IAM.

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 Utilizzo dei punti di accesso.

Utilizzo dei punti di accesso

I punti di accesso EFS sono punti di ingresso specifici dell'applicazione in un file system EFS che semplificano la gestione dell'accesso delle applicazioni 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 le policy AWS Identity and Access Management (IAM) per far sì 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**
>
> Per utilizzare i punti di accesso, è necessario creare almeno un target di montaggio sul file system EFS.

Puoi creare punti di accesso per un file system EFS esistente utilizzando AWS Management Console, the AWS Command Line Interface (AWS CLI) e l'API Amazon EFS. Un file system EFS può avere un massimo di 10.000 punti di accesso. Non è possibile modificare un punto di accesso esistente dopo la sua creazione.

Per step-by-step le procedure per creare un punto di accesso, vedereCreazione di access point.

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.

Argomenti

- Applicazione di un'identità utente mediante un punto di accesso
- Applicazione di una directory radice con un punto di accesso
- Utilizzo di punti di accesso nelle policy IAM

Applicazione di un'identità utente mediante 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 dell'utente.

- ID gruppo - L'ID numerico del gruppo POSIX dell'utente.
- Gruppo secondario IDs : un elenco opzionale di gruppi IDs secondari.

Quando l'imposizione degli utenti è abilitata, Amazon EFS sostituisce l'utente e il gruppo del client NFS IDs 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 di gruppo e il gruppo secondario IDs del punto di accesso durante la valutazione delle autorizzazioni del file system. EFS ignora i client NFS. IDs

> **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 radice 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 la directory principale con proprietà e autorizzazioni configurabili. Amazon EFS non creerà la directory principale se non si specificano la proprietà e i permessi 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 quando si crea un punto di accesso:

- `OwnerUid` - L'ID utente POSIX numerico da utilizzare come proprietario della directory radice.
- `OwnerGiD` - L'ID gruppo POSIX numerico da utilizzare come gruppo proprietario della directory radice.
- Permessi - 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 Utenti, gruppi e autorizzazioni a livello di Network File System (NFS).

Amazon EFS crea una directory principale del punto di accesso solo se per la OwnUid directory sono specificati ownGid e autorizzazioni. 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 monti un file system con un punto di accesso, la directory principale per il 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 radice 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 si specificano la proprietà e i permessi per la directory principale di un punto di accesso, Amazon EFS non creerà la directory principale. Tutti i tentativi di montare il punto di accesso falliranno.

Modello di protezione per le directory radice del punto di accesso

Quando è in essere un override della directory radice, il comportamento di Amazon EFS è simile a quello di un server Linux NFS con l'opzione `no_subtree_check` 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 atto un override della directory principale, Amazon EFS non rivela gli handle di file per i file al di fuori della directory principale specificata. Tuttavia, in alcuni casi un utente potrebbe ottenere un handle di file per un file al di fuori del 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 di 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 il nome della risorsa Amazon (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 ai file system EFS

La funzionalità di accesso pubblico a blocchi di Amazon EFS fornisce impostazioni per aiutarti a gestire l'accesso pubblico ai file system EFS. Per impostazione predefinita, i nuovi file system EFS non consentono l'accesso pubblico. Tuttavia, è possibile modificare le policy di file system per consentire l'accesso pubblico.

Important

L'abilitazione dell'accesso pubblico a blocchi aiuta a proteggere le risorse impedendo che l'accesso pubblico venga concesso attraverso le politiche delle risorse direttamente collegate al file system. Oltre ad attivare l'opzione Blocca accesso pubblico, controllare attentamente le seguenti policy per verificare che non concedano l'accesso pubblico:

- Politiche basate sull'identità collegate ai AWS principali associati (ad esempio, i ruoli IAM)
- Politiche basate sulle risorse collegate alle AWS risorse associate (ad esempio, chiavi (KMS))AWS Key Management Service

Argomenti

- Blocco dell'accesso pubblico con AWS Transfer Family
- Significato di "pubblico"

Blocco dell'accesso pubblico con AWS Transfer Family

Quando usi Amazon EFS con AWS Transfer Family, le richieste di accesso al file system ricevute da un server Transfer Family di proprietà di un account diverso dal file system vengono bloccate se il file system consente l'accesso pubblico. Amazon EFS valuta le policy IAM del file system e, se la policy è pubblica, blocca la richiesta. Per consentire AWS Transfer Family l'accesso al tuo file system, aggiorna la politica del file system in modo che non sia considerata pubblica.

Note

L'uso di Transfer Family con Amazon Account AWS EFS è disabilitato per impostazione predefinita per i 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 l' AWS assistenza.

Significato di "pubblico"

Nel valutare se un file system consente l'accesso pubblico, Amazon EFS presuppone che la policy 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 di file system deve concedere

l'accesso solo a valori fissi (valori che non contengono caratteri jolly) di uno o più degli elementi seguenti:

- Un insieme di routing inter-domain senza classe ()CIDRs, utilizzando. `aws:SourceIp` Per ulteriori informazioni su CIDR, vedere RFC 4632il sito Web di RFC Editor.
- Un AWS responsabile, un utente, un ruolo o un responsabile 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 non pubblica questa policy del file system utilizzando la chiave di condizione EFS `elasticfilesystem:AccessedViaMountTarget` impostata su true. È possibile utilizzare

`elasticfilesystem:AccessedViaMountTarget` per consentire le azioni EFS specificate ai client che accedono al file system EFS utilizzando un target di montaggio del file system. La seguente policy non pubblica utilizza la chiave `elasticfilesystem:AccessedViaMountTarget` condizionale 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 su queste chiavi di condizione Amazon EFS, consulta Chiavi di condizione EFS per client. Per ulteriori informazioni sulla creazione di policy di file system, consulta Creazione di policy del file system.

Convalida della conformità per Amazon EFS

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Ambito per programma di conformitàServizi AWS di conformità e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide 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 regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e 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.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Amazon EFS

L'infrastruttura AWS globale è costruita attorno a Regioni AWS e Availability Zones ()AZs. Regioni AWS forniscono più reti fisicamente separate e isolate AZs, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con AZs, è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra le zone senza interruzioni. AZssono più disponibili, tolleranti ai guasti e scalabili rispetto alle tradizionali infrastrutture di data center singoli o multipli.

I file system di Amazon EFS sono resilienti a uno o più guasti della zona di disponibilità all'interno di Regione AWS. i target di montaggio stesse sono progettate per offrire elevata disponibilità. Nella progettazione mirata all'elevata disponibilità e al failover verso altre aree AZs, tenete presente che, sebbene gli indirizzi IP e il DNS delle destinazioni di montaggio in ciascuna zona di distribuzione siano statici, si tratta di componenti ridondanti supportati da più risorse. Per ulteriori informazioni, consulta Come funziona Amazon EFS con Amazon EC2 .

Per ulteriori informazioni sulle zone di disponibilità, Regioni AWS consulta Global Infrastructure.AWS

Isolamento di rete per Amazon EFS

In quanto servizio gestito, Amazon Elastic File System è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad 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.

Questi APIs sono richiamabili da qualsiasi posizione di rete, ma Amazon EFS supporta politiche di accesso basate sulle risorse che possono includere restrizioni basate sull'indirizzo IP di origine. Puoi anche utilizzare le policy di Amazon EFS per controllare l'accesso da endpoint Amazon Virtual Private Cloud (Amazon VPC) specifici o specifici. VPCs In effetti, questo isola l'accesso alla rete a una determinata risorsa Amazon EFS solo dal VPC specifico all'interno AWS della rete.

Quote Amazon EFS

Di seguito vengono fornite informazioni sulle quote relative all'utilizzo di Amazon EFS.

Argomenti

- Quote per Amazon EFS che è possibile incrementare
- Quote di risorse di Amazon EFS che non puoi modificare
- Limiti per i client NFS
- Quote per i file system Amazon EFS
- Funzionalità NFSv4 2.0 e 4.1 non supportate
- Ulteriori considerazioni
- Risoluzione degli errori di funzionamento dei file relativi alle quote

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 i valori limite di Amazon EFS e richiedere un aumento della quota per il numero di file system EFS in un Regione AWS IOPS di lettura per i dati a cui si accede di frequente.

Inoltre, puoi richiedere un aumento delle quote Amazon EFS seguenti contattando l’assistenza AWS . Per ulteriori informazioni, consulta Richiesta di aumento delle quote. Il team di assistenza Amazon EFS esamina ogni richiesta individualmente.

- Numero di file system per ogni account cliente.
- Numero di punti di accesso per ogni file system.
- Numero massimo di IOPS di lettura per file system utilizzando la velocità effettiva elastica. Quando aumenta l'IOPS di lettura per i file system a cui si accede di frequente, aumentano anche gli IOPS di lettura per i file system a cui si accede raramente e gli IOPS di scrittura.
- Throughput elastico per file system regionale per tutti i client connessi in un. Regione AWS
- Throughput assegnato per file system regionale per tutti i client connessi in un. Regione AWS

La tabella seguente elenca le quote di risorse predefinite generali che è possibile richiedere di modificare.

Risorsa	Quota predefinita
Numero di file system per ogni account cliente in un Regione AWS	1.000
Numero di punti di accesso per ogni file system	10.000
Numero massimo di IOPS per file system utilizzando la velocità effettiva elastica È possibile richiedere un aumento fino a 10 volte della quota predefinita di IOPS di lettura per i dati a cui si accede di frequente. L'aumento degli IOPS di lettura per i dati ad accesso frequente comporta anche un aumento degli IOPS di lettura per i dati ad accesso meno frequente e degli IOPS di scrittura.	Dati a cui si accede raramente: 90.000 Dati ad accesso frequente letti: 250.000 Scrivi: 50.000

La tabella seguente elenca le quote di throughput elastiche per file system per tutti i client connessi in ciascuno di essi. Regione AWS

File system regionali: velocità effettiva elastica totale predefinita 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)	60 gibibyte al secondo () GiBps	5 GiBps

Regione AWS	Velocità di trasmissione effettiva massima in lettura	Velocità di trasmissione effettiva massima in scrittura (throughput misurato)
Stati Uniti orientali (Virginia settentrionale) Stati Uniti occidentali (Oregon) Asia Pacific (Mumbai) Region Regione Asia Pacifico (Seoul) Regione Asia Pacifico (Singapore) Regione Asia Pacifico (Sydney) Regione Asia Pacifico (Tokyo) Europe (Frankfurt) Region Regione Europa (Irlanda) Regione Europa (Londra)		
Tutti gli altri Regioni AWS	20 GiBps	1 GiBps

La tabella seguente elenca le quote di throughput fornite per file system per tutti i client connessi in ciascuno di essi. Regione AWS

File system regionali: velocità effettiva totale predefinita fornita 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)	10 GiBps	3.33 GiBps

Regione AWS	Velocità di trasmissione effettiva massima in lettura	Velocità di trasmissione effettiva massima in scrittura (throughput misurato)
Stati Uniti orientali (Virginia settentrionale) Stati Uniti occidentali (Oregon) Europa (Irlanda)		
Tutti gli altri Regioni AWS	3 GiBps	1 GiBps

Richiesta di aumento delle quote

Per richiedere un aumento di queste quote Supporto AWS, procedi nel seguente modo. Il team Amazon EFS esamina ogni richiesta di incremento della quota.

Per richiedere un aumento della quota tramite Supporto AWS

1. Apri la pagina Supporto AWS 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 connessioni per ogni file system.
- Quote di throughput elastiche e fornite per file system One Zone per tutti i client connessi in un file system. Regione AWS
- Incremento delle quote di throughput per file system Regional o One Zone per tutti i client connessi in un. Regione AWS

La tabella seguente elenca le quote di risorse generali che non possono essere modificate.

Quote di risorse generali che non possono essere modificate

Risorsa	Quota
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)	1.400
Numero di gruppi di sicurezza per ogni destinazione di montaggio	5
Numero di tag per ogni file system	50
Numero di VPCs 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.

La tabella seguente elenca i limiti totali di throughput predefiniti di Elastic e Provisioned per file system per tutti i client connessi in ciascuno di essi. Regione AWS

File system a zona unica: velocità effettiva totale predefinita (Elastic e Provisioned) 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)
Tutti Regioni AWS	3 GiBps	1 GiBps

La tabella seguente elenca i limiti totali di throughput di Bursting per file system per tutti i client connessi in ciascuno di essi. Regione AWS

File system regionali e One Zone: velocità effettiva 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) Stati Uniti orientali (Virginia settentrionale) Stati Uniti occidentali (Oregon) Asia Pacifico (Sydney) Europa (Irlanda)	5 GiBps	3 GiBps
Tutti gli altri Regioni AWS	3 GiBps	1 GiBps

Limiti per i client NFS

Si applicano le seguenti quote per i client NFS, presupponendo un client Linux 1.1: NFSv4

- La velocità massima combinata di lettura e scrittura è di 1.500 mebibyte al secondo (MiBps) per i file system che utilizzano la velocità effettiva elastica e montati utilizzando la versione 2.0 o successiva del client Amazon EFS (versione) amazon-efs-utils o il driver Amazon EFS CSI (). aws-efs-csi-driver Il throughput massimo per tutti gli altri file system è 500. MiBps Per ulteriori informazioni sulle prestazioni, consultare Riepilogo delle prestazioni. 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 gruppi IDs (GIDs) per utente e gli eventuali gruppi aggiuntivi GIDs 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
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 2.0 e 4.1 non supportate

Sebbene Amazon EFS non supporti NFSv2 o NFSv3 supporti sia NFSv4 .1 che NFSv4 .0, ad eccezione delle seguenti funzionalità:

- pNFS
- Attributi estesi
- 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`.
- Elenchi di controllo degli accessi () ACLs
- 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

- NFSv41. Conservazione dei dati
- SetUID su cartelle
- Tipi di file non supportati quando si utilizza l'operazione CREATE: dispositivi a blocchi (NF4BLK), dispositivi a caratteri (NF4CHR), directory degli attributi (NF4ATTRDIR) e attributo denominato (NAMEDATTR). NF4
- 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 _ACL. FATTR4

  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 Guida per l'Riferimenti generali di AWS utente.
- 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 Tutorial: Montaggio con client locali.

Risoluzione degli errori di funzionamento dei file relativi alle quote

Quando si accede ai file system EFS, si applicano determinati limiti ai file nel file system. Il superamento di tali limiti può causare errori nelle operazioni sui file. Per ulteriori informazioni sui limiti basati sui file in Amazon EFS, consulta. Quote Amazon EFS

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"

- Il comando ha esito negativo con l'errore "Errore di I/O"
- Il comando ha esito negativo con l'errore "Nome del file troppo lungo"
- Il comando ha esito negativo con l'errore "File non trovato"
- Il comando ha esito negativo con l'errore "Troppi link"
- Il comando ha esito negativo con l'errore "File troppo grande"

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.

API Amazon EFS

L'API EFS Amazon è un protocollo di rete basato su HTTP (RFC 2616). Per ogni chiamata API, effettui una richiesta HTTP all'endpoint API Amazon EFS specifico della regione Regione AWS in cui desideri gestire i file system. L'API fa riferimento ai documenti JSON (RFC 4627) per la definizione dei contenuti delle richieste/risposte HTTP.

Le API Amazon EFS fanno riferimento a 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.

La specifica operazione Amazon EFS sulla quale viene mappata una specifica richiesta è determinata da una combinazione di metodo della richiesta (GET, PUT, POST o DELETE) e modello corrispondente all'URI della richiesta, tra i tanti disponibili. Se l'operazione è PUT o POST, Amazon EFS estrae gli argomenti di chiamata dal segmento del percorso Request-URI, dai parametri delle query e dall'oggetto JSON nel corpo della richiesta.

> **Note**
>
> Sebbene i nomi delle operazioni, ad esempio`CreateFileSystem`, non compaiano sul web, questi nomi sono significativi nelle politiche AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per Amazon EFS.
> Il nome dell'operazione viene utilizzato anche per denominare i comandi negli strumenti a riga di comando e negli elementi dell'SDK. AWS APIs Ad esempio, esiste un AWS CLI comando denominato `create-file-system` che corrisponde all'operazione. `CreateFileSystem`
> Il nome dell'operazione appare anche nei AWS CloudTrail log delle chiamate API Amazon EFS.

Endpoint API

Un endpoint è un URL che funge da punto di ingresso per un servizio AWS Web. Amazon EFS supporta i seguenti tipi di endpoint:

- IPv4 endpoint
- Endpoint dual-stack (entrambi e) IPv4 IPv6
- Endpoint FIPS

Quando si effettua una richiesta, è possibile specificare l'endpoint da utilizzare. Se non si specifica un endpoint, l' IPv4 endpoint viene utilizzato per impostazione predefinita. Per utilizzare un tipo di endpoint diverso, devi specificarlo nella richiesta. Per esempi su come eseguire questa operazione, consulta Specificazione degli endpoint. Per una tabella degli endpoint disponibili, consulta Endpoint e quote Amazon EFS.

IPv4 endpoint

IPv4 gli endpoint supportano solo il IPv4 traffico. IPv4 gli endpoint sono disponibili per tutte le regioni. Il formato dell' IPv4 endpoint dipende dalla regione.

- Per gli IPv4 endpoint nelle regioni AWS commerciali, il formato è. `elasticfilesystem.region.amazonaws.com`

  Ad esempio, se specifichi `elasticfilesystem.us-west-2.amazonaws.com` come endpoint, indirizziamo la tua richiesta all'endpoint della regione degli Stati Uniti occidentali (Oregon) (us-west-2).

- Per gli IPv4 endpoint nelle regioni della Cina, il formato `èelasticfilesystem.region.amazonaws.com.cn`.

  Ad esempio, l'endpoint dell'API Amazon EFS per la regione Cina (Pechino) `èelasticfilesystem.cn-north-1.amazonaws.com.cn`.

Endpoint dual-stack (e) IPv4 IPv6

Gli endpoint dual-stack supportano sia il traffico che il traffico. IPv4 IPv6 Quando effettui una richiesta a un endpoint dual-stack, l'URL dell'endpoint si risolve in un indirizzo IPv6 o in un IPv4 indirizzo, a seconda del protocollo utilizzato dalla rete e dal client. Il formato dell'endpoint dual-stack dipende dalla regione.

- Per gli endpoint dual-stack nelle regioni commerciali, il formato è. AWS `efs.aws-region.api.aws`

Ad esempio, l'endpoint dual-stack per la regione Stati Uniti occidentali (Oregon) (us-west-2) è. `efs.eu-west-2.api.aws`

- Per gli endpoint dual-stack nelle regioni della Cina, il formato è. `efs.region.api.amazonwebservices.com.cn`

  Ad esempio, l'endpoint dual-stack per la regione Cina (Pechino) è. `efs.cn-north-1.api.amazonwebservices.com.cn`

Specificazione degli endpoint

Gli esempi seguenti mostrano come specificare un endpoint per la regione Stati Uniti occidentali (California settentrionale) (us-west-1) utilizzando per Amazon EFS. AWS CLI

IPv4

```
aws efs get-rest-apis --region us-west-1 --endpoint-url https://elasticfilesystem.us-west-1.amazonaws.com
```

Dual-stack

```
aws efs get-rest-apis --region us-west-1 --endpoint-url https://efs.us-west-1.api.aws
```

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 delle identità e degli accessi per Amazon EFS
- Operazioni

- Tipi di dati

Gestione della frequenza massima di richieste della Query API per Amazon EFS

Le richieste API di Amazon EFS vengono limitate per ciascuna Account AWS regione per migliorare le prestazioni del servizio. Tutte le chiamate API di Amazon EFS insieme, indipendentemente dal fatto che provengano da un'applicazione AWS CLI, dalla console o dalla console Amazon EFS, non devono superare la frequenza massima di richieste API consentita. La frequenza massima di richieste API può variare da uno all'altro Regioni AWS. Le richieste API effettuate vengono attribuite al sottostante Account 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.

Tentativi ripetuti o elaborazione batch

L'applicazione potrebbe aver bisogno di riprovare a eseguire una richiesta API dopo una prima esecuzione con esito negativo o per elaborare più risorse (ad esempio, tutti i propri 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 dell'intervallo di attesa

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, consulta Retry behavior in.Riferimenti generali di Amazon Web Services

Operazioni

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. Un file system può avere un massimo di 10.000 punti di accesso a meno che non si richieda un aumento. 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 dei punti di accesso, è possibile che si verifichi una limitazione della risposta a tali 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 pari a 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 Tagging AWS resources nella General Reference Guide. 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 pari a 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 della Account AWS risorsa del punto di accesso.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

PosixUser

L'identità POSIX completa, inclusi l'ID utente, l'ID di gruppo e il gruppo secondario IDs sul punto di accesso utilizzato per tutte le operazioni sui 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 `FileSystemId` valore specificato non esiste nel file del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 del chiamante Account AWS con il token di creazione specificato, questa operazione esegue le seguenti operazioni:

- 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 l'uso `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. Puoi montare il tuo file system Amazon EFS su un' EC2 istanza nel tuo VPC utilizzando la destinazione 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, specifica 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 One Zone non sono disponibili in tutte le zone di disponibilità in Regioni AWS cui è disponibile Amazon EFS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 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 tutti i paesi in Regioni AWS 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 pari a 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, hai la possibilità di specificare una AWS Key Management Service chiave 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 si utilizza`KmsKeyId`, è necessario impostare il parametro:`Encrypted` su `true`CreateFileSystem.

> **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. Supporto 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 Taggare AWS le risorse nella Guida di riferimento AWS generale.

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 della zona di disponibilità per Regione AWS us-east-1 e ha la stessa posizione in tutti. Account AWS

Tipo: stringa

AvailabilityZoneName

Descrive la zona di AWS disponibilità in cui si trova il file system ed è valido 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 pari a 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 pari a 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 di un file AWS KMS key utilizzato 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

Quello 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 1970-01-01T00:00:00Z. 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 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 di disponibilità `us-west-2b`.

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateMountTarget

Crea un target di montaggio per un file system. È quindi possibile montare il file system sulle EC2 istanze utilizzando la destinazione di montaggio. Per ulteriori informazioni sulle destinazioni di montaggio, vedere Gestione delle destinazioni di montaggio.

Per creare una destinazione di montaggio per un file system EFS, lo stato del ciclo di vita del file system deve essere. `available` Per ulteriori informazioni, consulta DescribeFileSystems.

Dopo aver creato la destinazione di montaggio, Amazon EFS restituisce una risposta che include un indirizzo IP `MountTargetId` e un indirizzo IP (`IpAddressoIpv6Address`). Utilizzi questo indirizzo IP per montare il file system in un' EC2 istanza. Durante il montaggio del file system è anche possibile utilizzare il nome DNS del target di montaggio. L' EC2 istanza su cui si monta il file system utilizzando la destinazione di montaggio può risolvere il nome DNS della destinazione di montaggio nel relativo indirizzo IP. Per ulteriori informazioni, consulta Come funziona Amazon EFS.

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. Per ulteriori informazioni, consulta Creazione di target di montaggio.

Se la richiesta soddisfa i requisiti, Amazon EFS procede in questo modo:

- Crea un nuovo target di montaggio nella sottorete specificata.
- Crea una nuova interfaccia di rete nella sottorete con quanto segue:
  - La descrizione `Mount target` *`fsmt-id`* `for file system` *`fs-id`* dove *`fsmt-id`* è l'ID del target di montaggio, ed *`fs-id`* è. `FileSystemId`
  - La `requesterManaged` proprietà dell'interfaccia di rete è impostata su e il `requesterId` valore impostato su`EFS`. `true`

  Ogni destinazione di montaggio ha una corrispondente interfaccia di EC2 rete gestita dal richiedente. Dopo aver creato l'interfaccia di rete, Amazon EFS imposta il `NetworkInterfaceId` campo nella descrizione della destinazione di montaggio sull'ID dell'interfaccia di rete e l'indirizzo IP 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.

Questa operazione richiede autorizzazioni per le seguenti operazioni sul file system:

- `elasticfilesystem:CreateMountTarget`

Questa operazione richiede anche le autorizzazioni per le seguenti EC2 azioni Amazon:

- `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",
   "IpAddressType": "string",
   "Ipv6Address": "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

Se `IpAddressType` for the mount target è IPv4 (`IPV4_ONLY`o`DUAL_STACK`), specifica l' IPv4 indirizzo da utilizzare. Se non lo specifichi`IpAddress`, Amazon EFS seleziona un indirizzo IP inutilizzato dalla sottorete specificata per. `SubnetId`

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 7. La lunghezza massima è 15 caratteri.

Modello: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Campo obbligatorio: no

IpAddressType

Il tipo di indirizzo IP per la destinazione di montaggio. I valori possibili sono `IPV4_ONLY` (solo IPv4 indirizzi), `IPV6_ONLY` (solo IPv6 indirizzi) e `DUAL_STACK` (dual-stack, entrambi IPv4 e IPv6 indirizzi). Se non si specifica un`IpAddressType`, allora viene `IPV4_ONLY` utilizzato.

> **Note**
>
> `IPAddressType`Deve corrispondere al tipo di IP della sottorete. Inoltre, il `IPAddressType` parametro sostituisce il valore impostato come indirizzo IP predefinito per la sottorete nel VPC. Ad esempio, se `IPAddressType` è `IPV4_ONLY` ed è`true`, allora `AssignIpv6AddressOnCreation` IPv4 viene utilizzato per la destinazione di montaggio. Per ulteriori informazioni, consulta la sezione Modifica dell'attributo di assegnazione degli indirizzi IP della sottorete.

Tipo: stringa

Valori validi: `IPV4_ONLY | IPV6_ONLY | DUAL_STACK`

Campo obbligatorio: no

Ipv6Address

Se `IPAddressType` for the mount target è IPv6 (`IPV6_ONLYoDUAL_STACK`), allora specifica l' IPv6 indirizzo da utilizzare. Se non lo specifichi`Ipv6Address`, Amazon EFS seleziona un indirizzo IP inutilizzato dalla sottorete specificata per. `SubnetId`

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 39.

Campo obbligatorio: no

SecurityGroups

Gruppo di sicurezza VPC IDs, del modulo. `sg-xxxxxxxx` Questi devono essere per lo stesso VPC della sottorete specificata. Il numero massimo di gruppi di sicurezza dipende dalla quota dell'account. Per ulteriori informazioni, consulta Amazon VPC Quotas nella Amazon VPC User Guide (consulta la tabella dei gruppi di sicurezza). Se non specifichi un gruppo di sicurezza, Amazon EFS utilizza il gruppo di sicurezza predefinito per il VPC della sottorete.

Tipo: matrice di stringhe

Membri della matrice: numero massimo di 100 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 11. La lunghezza massima è 43 caratteri.

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. Il tipo di sottorete deve essere dello stesso tipo di. `IpAddressType`

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 15. La lunghezza massima è 47 caratteri.

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",
   "Ipv6Address": "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. Le zone di disponibilità sono mappate indipendentemente in base ai nomi di ciascuna. Account AWS Ad esempio, la zona `us-east-1a` di disponibilità dell'utente Account AWS potrebbe non corrispondere a quella `us-east-1a` di un'altra Account AWS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 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

L' IPv4 indirizzo per la destinazione di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 7. La lunghezza massima è 15 caratteri.

Modello: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Ipv6Address

L' IPv6 indirizzo per il target di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 39.

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. La lunghezza massima è 45 caratteri.

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

Account AWS ID 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. La lunghezza massima è 47 caratteri.

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 la destinazione di montaggio è diversa dalla zona di disponibilità del file system. 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 `FileSystemId` valore specificato non esiste nella cartella del richiedente. Account AWS

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 ha specificato un indirizzo IP (`IpAddressoIpv6Address`) che è 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

Ha restituito no `IpAddress` o `Ipv6Address` è stato fornito nella richiesta e non ci sono indirizzi IP liberi nella sottorete specificata.

Codice di stato HTTP: 409

SecurityGroupLimitExceeded

Restituito se il numero `SecurityGroups` specificato nella richiesta è superiore al limite, che si basa sulla quota dell'account. Elimina alcuni gruppi di sicurezza o richiedi l'aumento della quota dell'account. Per ulteriori informazioni, consulta Amazon VPC Quotas nella Amazon VPC User Guide (consulta la tabella dei gruppi di sicurezza).

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

Crea un target di montaggio a un IPv4 indirizzo disponibile su una sottorete

La richiesta seguente specifica solo il file system e la sottorete per la destinazione di montaggio. La destinazione viene creata a un IPv4 indirizzo disponibile nella sottorete specificata, con il gruppo di sicurezza predefinito associato al VPC.

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

{
    "OwnerId": "231243201240",
    "MountTargetId": "fsmt-55a4413c",
    "FileSystemId": "fs-01234567",
    "SubnetId": "subnet-01234567",
    "LifeCycleState": "available",
    "IpAddress": "172.31.22.183"
    "NetworkInterfaceId":"eni-1bcb7772"
    "AvailabilityZoneId": "eus1-az2",
    "AvailabilityZoneName": "eu-south-1b",
    "VpcId": "vpc-08d45b31fa009a15e"
}
```

Crea un target di montaggio a un indirizzo specifico IPv4

La richiesta seguente specifica il file system, la sottorete, il gruppo di sicurezza e l' IPv4indirizzo da utilizzare per la destinazione 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"
   "AvailabilityZoneId": "eus1-az2",
   "AvailabilityZoneName": "eu-south-1b",
   "VpcId": "vpc-08d45b31fa009a15e"
}
```

Crea una destinazione di montaggio a un indirizzo specifico IPv6

La richiesta seguente specifica il file system, la sottorete, il gruppo di sicurezza e l' IPv6indirizzo da utilizzare per la destinazione 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",
   "Ipv6Address":"2001:0db8:85a3:0000:0000:8a2e:0370:7334",
   "IpAddressType": "IPV6_ONLY",
   "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",
   "Ipv6Address":"2001:0db8:85a3:0000:0000:8a2e:0370:7334",
   "NetworkInterfaceId":"eni-1bcb7772"
   "AvailabilityZoneId": "eus1-az2",
   "AvailabilityZoneName": "eu-south-1b",
   "VpcId": "vpc-08d45b31fa009a15e"
}
```

Crea una destinazione di montaggio a un IPv4 indirizzo disponibile su una sottorete dual-stack

La richiesta seguente specifica il file system, la sottorete e il tipo di indirizzo per la destinazione di montaggio. La destinazione viene creata a un IPv4 indirizzo disponibile nella sottorete dual-stack specificata, con il gruppo di sicurezza predefinito associato al VPC.

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

{
    "OwnerId": "251839141158",
    "MountTargetId": "fsmt-55a4413c",
    "FileSystemId": "fs-01234567",
    "SubnetId":"subnet-fd04ff94",
    "LifeCycleState": "available",
    "IpAddress": "172.31.22.183"
    "Ipv6Address": "2a05:d01a:419:8611:3e57:75ab:5719:b238",
    "NetworkInterfaceId": "eni-01234567",
    "AvailabilityZoneId": "eus1-az2",
    "AvailabilityZoneName": "eu-south-1b",
    "VpcId": "vpc-08d45b31fa009a15e"
}
```

Crea un target di montaggio su Ipv4 e indirizzi specifici su una sottorete dual-stack IPv6

La seguente richiesta specifica il file system, la sottorete, il gruppo di sicurezza, l'indirizzo e l'indirizzo per la destinazione di montaggio. IPv4 IPv6 La destinazione viene creata all' IPv6indirizzo IPv4 e specificato su una sottorete dual-stack.

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",
   "IpAddressType": "DUAL_STACK",
   "IpAddress": "10.0.1.25",
   "Ipv6Address":"2001:0db8:85a3:0000:0000:8a2e:0370:7334",
   "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": "231243201240",
    "MountTargetId": "fsmt-55a4413c",
    "FileSystemId": "fs-01234567",
    "SubnetId": "subnet-01234567",
    "LifeCycleState": "available",
    "IpAddress": "10.0.1.25",
    "Ipv6Address":"2001:0db8:85a3:0000:0000:8a2e:0370:7334",
    "NetworkInterfaceId": "eni-01234567",
    "AvailabilityZoneId": "eus1-az2",
    "AvailabilityZoneName": "eu-south-1b",
    "VpcId": "vpc-08d45b31fa009a15e"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++

- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateReplicationConfiguration

Crea una configurazione di replica su un file system EFS nuovo o esistente. 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.
- File system di destinazione: il file system di destinazione in cui viene replicato il file system di origine. In una configurazione di replica può esistere un solo file system di destinazione.

> **Note**
>
> Un file system può far parte di una sola configurazione di replica.

I parametri di destinazione per la configurazione di replica dipendono dal fatto che si stia eseguendo la replica su un nuovo file system o su un file system esistente e se si stia eseguendo la replica su più file. Account AWS Per ulteriori informazioni, consulta DestinationToCreate.

Questa operazione richiede le autorizzazioni per l'operazione `elasticfilesystem:CreateReplicationConfiguration`. Inoltre, sono necessarie altre autorizzazioni a seconda della modalità di replica dei file system. Per ulteriori informazioni, consulta Autorizzazioni richieste per la replica 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",
         "RoleArn": "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,
            "OwnerId": "string",
            "Region": "string",
            "RoleArn": "string",
            "Status": "string",
            "StatusMessage": "string"
        }
    ],
    "OriginalSourceFileSystemArn": "string",
    "SourceFileSystemArn": "string",
    "SourceFileSystemId": "string",
    "SourceFileSystemOwnerId": "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})$`

SourceFileSystemOwnerId

ID del file system di origine Account AWS in cui risiede.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

SourceFileSystemRegion

Il file system EFS di origine Regione AWS in cui si trova.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 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 è già stato creato il numero massimo di file system consentiti per account.

Codice di stato HTTP: 403

FileSystemNotFound

Restituito se il `FileSystemId` valore specificato non esiste nel file del richiedente. Account AWS

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 AWS Backup servizio non è disponibile nel paese Regione AWS in cui è stata effettuata la richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 `AccessPointId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 automaticamente quando si utilizza la AWS console 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 `FileSystemId` valore specificato non esiste nel richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript

- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK 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' EC2 istanza 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 EC2 azione di Amazon 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. La lunghezza massima è 45 caratteri.

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 nell' 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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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?
deletionMode=DeletionMode HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

DeletionMode

Durante la replica incrociata Account AWS o trasversale Regioni AWS, Amazon EFS elimina la configurazione di replica sia dall'account o dalla regione di origine che di destinazione (`ALL_CONFIGURATIONS`) per impostazione predefinita. Se c'è un problema di configurazione o di autorizzazioni che impedisce ad Amazon EFS di eliminare la configurazione di replica da entrambi i lati, puoi utilizzare la `LOCAL_CONFIGURATION_ONLY` modalità per eliminare la configurazione di replica solo dal lato locale (l'account o la regione da cui viene eseguita l'eliminazione).

> **Note**
>
> Utilizza la `LOCAL_CONFIGURATION_ONLY` modalità solo nel caso in cui Amazon EFS non sia in grado di eliminare la configurazione di replica nell'account o nella regione di origine e di destinazione. L'eliminazione della configurazione locale rende irrecuperabile la configurazione nell'altro account o regione.
> Inoltre, non utilizzate questa modalità per la replica dello stesso account e della stessa regione, poiché così facendo si verificherebbe un errore di eccezione. BadRequest

Valori validi: `ALL_CONFIGURATIONS | LOCAL_CONFIGURATION_ONLY`

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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 tag e sulle relative restrizioni, consulta Restrizioni relative ai tag nella Guida AWS Billing and Cost Management per l'utente.

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 pari a 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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 pari a 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 pari a 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

Errori

AccessPointNotFound

Restituito se il `AccessPointId` valore specificato non esiste nel richiedente. Account AWS

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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeAccountPreferences

Restituisce le impostazioni delle preferenze dell'account per l'utente Account AWS associato all'utente che effettua la richiesta, nella versione corrente Regione AWS.

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 pari a 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 pari a 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, nella versione corrente Regione AWS.

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 `FileSystemId` valore specificato non esiste nel richiedente Account AWS.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

PolicyNotFound

Restituito se `no backup` è specificato per un file system One Zone EFS.

Codice di stato HTTP: 404

ValidationException

Restituito se il AWS Backup servizio non è disponibile nel paese Regione AWS in cui è stata effettuata la richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 pari a 1. La lunghezza massima è 20000 caratteri.

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 `FileSystemId` valore specificato non esiste nel richiedente Account AWS.

Codice di stato HTTP: 404

InternalServerError

Restituito se si è verificato un errore lato server.

Codice di stato HTTP: 500

PolicyNotFound

Restituito se no backup è specificato per un file system One Zone EFS.

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeFileSystems

Restituisce la descrizione di un file system Amazon EFS specifico se viene fornito il file system `CreationToken` o `FileSystemId`. Altrimenti, restituisce le descrizioni di tutti i file system di proprietà del chiamante Account AWS nell' Regione AWS 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 pari a 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 pari a 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 pari a 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 pari a 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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeLifecycleConfiguration

Restituisce l'`LifecycleConfiguration`oggetto corrente per il file system 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 `FileSystemId` valore specificato non esiste nel richiedente Account AWS.

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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`.

Il comando CLI corrispondente è. `describe-mount-targets`

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 pari a 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. La lunghezza massima è 45 caratteri.

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",
            "Ipv6Address": "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 pari a 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 pari a 1. La lunghezza massima è 128 caratteri.

Modello: `.+`

Errori

AccessPointNotFound

Restituito se il `AccessPointId` valore specificato non esiste nel richiedente. Account AWS

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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 nell' 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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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. La lunghezza massima è 45 caratteri.

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. La lunghezza massima è 43 caratteri.

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 nell' 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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeReplicationConfigurations

Recupera la configurazione di replica per un file system specifico. Se non viene specificato un file system, Regione AWS vengono recuperate tutte le configurazioni di replica per l' Account AWS in an.

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. Per la replica tra account e regioni, un account può solo descrivere la configurazione di replica per un file system nella propria regione.

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 pari a 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,
               "OwnerId": "string",
               "Region": "string",
               "RoleArn": "string",
               "Status": "string",
               "StatusMessage": "string"
            }
         ],
         "OriginalSourceFileSystemArn": "string",
         "SourceFileSystemArn": "string",
         "SourceFileSystemId": "string",
         "SourceFileSystemOwnerId": "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 pari a 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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 AWS Backup servizio non è disponibile nel paese Regione AWS in cui è stata effettuata la richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 pari a 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 pari a 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 pari a 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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListTagsForResource

Elenca tutti i tag di una risorsa EFS di primo livello. È necessario fornire l'ID della 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 pari a 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 pari a 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 `AccessPointId` valore specificato non esiste in quello del richiedente. Account AWS

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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 i `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. La lunghezza massima è 45 caratteri.

Modello: `^fsmt-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

SecurityGroups

Una serie di gruppi di sicurezza VPC. IDs

Tipo: matrice di stringhe

Membri della matrice: numero massimo di 100 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 11. La lunghezza massima è 43 caratteri.

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 nell' Account AWS del chiamante.

Codice di stato HTTP: 404

SecurityGroupLimitExceeded

Restituito se il numero `SecurityGroups` specificato nella richiesta è maggiore del limite, che si basa sulla quota dell'account. Elimina alcuni gruppi di sicurezza o richiedi l'aumento della quota dell'account. Per ulteriori informazioni, consulta Amazon VPC Quotas nella Amazon VPC User Guide (consulta la tabella dei gruppi di sicurezza).

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

Sostituzione dei 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 una delle lingue AWS SDKs specifiche, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutAccountPreferences

Utilizzate questa operazione per impostare la preferenza dell'account corrente Regione AWS per utilizzare la risorsa lunga da 17 caratteri (63 bit) o corta da 8 caratteri (32 bit) IDs per il nuovo file system EFS e montare le risorse di destinazione. Tutte le risorse esistenti non IDs sono influenzate dalle modifiche apportate. È possibile impostare la preferenza ID durante il periodo di attivazione quando EFS passa a una risorsa lunga. IDs Per ulteriori informazioni, consulta Managing Amazon EFS resource IDs.

> **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 l' AWS assistenza se ricevi un errore e devi usare l'abbreviazione IDs di file system e mount delle risorse target.

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 Regione AWS, nella versione corrente `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 l' AWS assistenza se ricevi un errore e devi usare l'abbreviazione IDs per file system e mount delle 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 l'utente Account AWS, nella versione 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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 `FileSystemId` valore specificato non esiste nel richiedente Account AWS.

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 AWS Backup servizio non è disponibile nel paese Regione AWS in cui è stata effettuata la richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 pari a 1. La lunghezza massima è 20000 caratteri.

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 pari a 1. La lunghezza massima è 20000 caratteri.

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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 file system EFS `FileSystemPolicy` che consente a tutti AWS i principali di montare 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 una delle lingue specifiche, consulta quanto segue AWS SDKs:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK 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 `LifecycleConfiguration` oggetto a un file system crittografato, sono necessarie le stesse AWS Key Management Service autorizzazioni di quando è stato 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 fornisce 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 `FileSystemId` valore specificato non esiste nel file del richiedente. Account AWS

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 di trasmissione elastica 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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK per Ruby V3

TagResource

Crea un tag per una risorsa EFS. È possibile creare tag per i file system e i punti di accesso 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 `AccessPointId` valore specificato non esiste in quello del richiedente. Account AWS

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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UntagResource

Rimuove i tag da una risorsa EFS. È possibile rimuovere tag per i file system e i punti di accesso 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 pari a 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 `AccessPointId` valore specificato non esiste in quello del richiedente. Account AWS

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 `FileSystemId` valore specificato non esiste in quello del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 desideri fornire per un 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. Supporto 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 della zona di disponibilità per Regione AWS us-east-1 e ha la stessa posizione in tutti. Account AWS

Tipo: stringa

AvailabilityZoneName

Descrive la zona di AWS disponibilità in cui si trova il file system ed è valido 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 pari a 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 pari a 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 di un file AWS KMS key utilizzato 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

Quello 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 1970-01-01T00:00:00Z. 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 `FileSystemId` valore specificato non esiste nel file del richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 `FileSystemId` valore specificato non esiste nel richiedente. Account AWS

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK 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 pari a 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 Account AWS proprietario 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

L'identità POSIX completa, inclusi l'ID utente, l'ID di gruppo e il gruppo secondario IDs sul punto di accesso utilizzato per tutte le operazioni sui 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 una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CreationInfo

Obbligatorio se `RootDirectory` > `Path` specificato non esiste. Speciifica il POSIX IDs e le autorizzazioni da applicare al punto di accesso >. `RootDirectory` `Path` 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 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.

> **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 massimo pari a 4294967295.

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 massimo pari a 4294967295.

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: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 4 caratteri.

Modello: `^[0-7]{3,4}$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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 pari a 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 della configurazione di replica. Per ulteriori informazioni sullo stato della replica, consulta Visualizzazione dei dettagli della replica nella Amazon EFS User Guide.

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

OwnerId

ID del file system di destinazione Account AWS in cui risiede.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

Campo obbligatorio: no

RoleArn

Amazon Resource Name (ARN) del ruolo IAM nell'account di origine che consente ad Amazon EFS di eseguire la replica per suo conto. È facoltativo per la replica sullo stesso account e necessario per la replica tra account.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Campo obbligatorio: no

StatusMessage

Messaggio che fornisce dettagli sullo `ERRROR` stato `PAUSED` o della configurazione della destinazione di replica. Per ulteriori informazioni sui messaggi di stato della replica, consulta Visualizzazione dei dettagli della replica nella Amazon EFS User Guide.

Tipo: string

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DestinationToCreate

Descrive, nella configurazione di replica, il file system di destinazione nuovo o esistente.

- Se si desidera eseguire la replica su un nuovo file system, non specificare l'ID del file system per il file system di destinazione. Amazon EFS crea un nuovo file system vuoto. Per lo storage a zona singola, specifica la zona di disponibilità in cui creare il file system. Per utilizzare una AWS Key Management Service chiave diversa dalla chiave KMS predefinita, specificala. Per ulteriori informazioni, consulta Configurazione della replica sul nuovo file system Amazon EFS nella Guida per l'utente di Amazon EFS.

  > **Note**
  >
  > Dopo aver creato il file system, non è possibile modificare la chiave KMS o la modalità di prestazioni.

- Se desideri eseguire la replica su un file system esistente che si trova nello stesso account del file system di origine, devi fornire l'ID o Amazon Resource Name (ARN) del file system su cui eseguire la replica. La protezione da sovrascrittura della replica del file system deve essere disabilitata. Per ulteriori informazioni, consulta Replicazione su un file system esistente nella Amazon EFS User Guide.
- Se stai replicando il file system su un file system che si trova in un account diverso dal file system di origine (replica tra account), devi fornire l'ARN per il file system e il ruolo IAM che consente ad Amazon EFS di eseguire la replica sull'account di destinazione. La protezione da sovrascrittura della replica del file system deve essere disabilitata. Per ulteriori informazioni, consulta Replicating across Account AWS nella Amazon EFS User Guide.

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 pari a 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: no

FileSystemId

L'ID o l'ARN del file system da utilizzare per la destinazione. Per la replica tra account, deve essere un ARN. La replica da sovrascrittura della replica del file system deve essere disabilitata. Se non viene specificato alcun ID o ARN, viene creato un nuovo file system.

> **Note**
>
> Quando configuri inizialmente la replica su un file system esistente, Amazon EFS scrive o rimuove i dati esistenti dal file system di destinazione in modo che corrispondano ai dati nel file system di origine. Se non desideri modificare i dati nel file system di destinazione, dovresti invece replicarli su un nuovo file system. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/efs/latest/ug/create-replication.html.

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

Specificate la chiave AWS Key Management Service (AWS KMS) che desiderate utilizzare 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 - L'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 l'archiviazione regionale, specificare Regione AWS in che modo creare il file system di destinazione. La regione deve essere abilitata per il Account AWS file system proprietario del file system di origine. Per ulteriori informazioni, vedere Managing Regioni AWS nella AWS General Reference Guide.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 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

RoleArn

Amazon Resource Name (ARN) del ruolo IAM nell'account di origine che consente ad Amazon EFS di eseguire la replica per suo conto. È facoltativo per la replica sullo stesso account e necessario per la replica tra account.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 2048.

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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 pari a 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

Quello 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 1970-01-01T00:00:00Z. 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 della zona di disponibilità per Regione AWS us-east-1 e ha la stessa posizione in tutti. Account AWS

Tipo: string

Campo obbligatorio: no

AvailabilityZoneName

Descrive la zona di AWS disponibilità in cui si trova il file system ed è valido 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 pari a 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 di un file AWS KMS key utilizzato 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 una delle lingue specifiche, consulta quanto segue AWS SDKs:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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 una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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 1970-01-01T00:00:00Z.

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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

MountTargetDescription

Fornisce una descrizione di un target di montaggio.

Indice

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

LifeCycleState

Stato del ciclo di vita del target di montaggio.

Tipo: stringa

Valori validi: `creating | available | updating | deleting | deleted | error`

Campo obbligatorio: sì

MountTargetId

ID del target di montaggio assegnato dal sistema.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 13. La lunghezza massima è 45 caratteri.

Modello: `^fsmt-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

SubnetId

L'ID della sottorete del target di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 15. La lunghezza massima è 47 caratteri.

Modello: `^subnet-[0-9a-f]{8,40}$`

Campo obbligatorio: sì

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: string

Campo obbligatorio: no

AvailabilityZoneName

Il nome della zona di disponibilità in cui si trova il target di montaggio. Le zone di disponibilità sono mappate indipendentemente in base ai nomi di ciascuna. Account AWS Ad esempio, la zona `us-east-1a` di disponibilità dell'utente Account AWS potrebbe non corrispondere a quella `us-east-1a` di un'altra Account AWS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 64 caratteri.

Modello: `.+`

Campo obbligatorio: no

IpAddress

L' IPv4 indirizzo per la destinazione di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 7. La lunghezza massima è 15 caratteri.

Modello: `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Campo obbligatorio: no

Ipv6Address

L' IPv6 indirizzo per il target di montaggio.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 39.

Campo obbligatorio: no

NetworkInterfaceId

L'ID dell'interfaccia di rete creata da Amazon EFS al momento della creazione del target di montaggio.

Tipo: string

Campo obbligatorio: no

OwnerId

Account AWS ID proprietario della risorsa.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

Campo obbligatorio: no

VpcId

L'ID del cloud privato virtuale (VPC) in cui è configurato il target di montaggio.

Tipo: string

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++

- AWS SDK per Java V2
- AWS SDK per Ruby V3

PosixUser

L'identità POSIX completa, inclusi l'ID utente, l'ID di gruppo e qualsiasi gruppo secondario IDs, 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

Gruppo POSIX secondario IDs utilizzato per tutte le operazioni del file system che utilizzano questo punto di accesso.

Tipo: array di lunghezze

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 16 elementi.

Intervallo valido: valore minimo di 0. Valore massimo pari a 4294967295.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consultate quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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 pari a 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

SourceFileSystemOwnerId

ID del file system di origine Account AWS in cui risiede.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 14.

Modello: `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ResourceIdPreference

Descrive il tipo di risorsa e la relativa preferenza ID per l'utente Account AWS, nella versione 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 una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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 POSIX IDs e le autorizzazioni da applicare ai punti di accesso. `RootDirectory` 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 pari a 1. Lunghezza massima di 100.

Modello: `^(\/|(\/(?!\.)+[^$#<>;`|&?{}^*/\n]+){1,4})$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue AWS SDKs specifiche, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK 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: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Campo obbligatorio: sì

Value

Il valore della chiave del tag.

Tipo: stringa

Limitazioni di lunghezza: lunghezza massima di 256.

Modello: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Cronologia dei documenti

- Versione API: 01-02-2015
- Ultimo aggiornamento della documentazione: 9 giugno 2025

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
Support per IPv6	La versione 6 del protocollo Internet (IPv6) è supportata su Amazon EFS Service APIs e mount target. Per ulteriori informazioni sull'API Amazon EFS, consulta l'API Amazon EFS. Per ulteriori informazioni sugli obiettivi di montaggio, consulta Gestione degli obiettivi di montaggio.	9 giugno 2025
Aumento elastico della produttività in alcuni casi Regioni AWS	La velocità massima di lettura per i file system che utilizzano la velocità effettiva elastica nelle seguenti regioni è aumentata da 20 GiBps a 60 GiBps: Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Sydney) ed Europa (Londra). Per ulteriori informazioni, consulta le quote di Amazon EFS che puoi aumentare.	2 maggio 2025

Aumento elastico del throughput in alcuni casi Regioni AWS	La velocità massima di lettura per i file system che utilizzano la velocità effettiva elastica in regioni specifiche è 60. GiBps In tutte le altre regioni, il limite di velocità effettiva di lettura per i file system che utilizzano la velocità effettiva elastica è stato aumentato da 10 a 20. GiBps Per ulteriori informazioni, consulta le quote di Amazon EFS che puoi aumentare.	10 aprile 2025
Quota di punti di accesso aumentata	Il numero massimo di punti di accesso che un singolo file system può avere è passato da 1.000 a 10.000. È inoltre possibile richiedere un aumento di questo limite. Per ulteriori informazioni, consulta Quote di risorse che è possibile aumentare.	10 febbraio 2025
Velocità di backup e ripristino migliorate	La velocità di esecuzione dei backup e dei ripristini è migliorata. Per ulteriori informazioni, consulta Prestazioni di Backup.	8 gennaio 2025

Quota IOPS aumentata su richiesta	Ora puoi richiedere un aumento degli IOPS per i file system EFS utilizzando la modalità di throughput elastico. Per ulteriori informazioni, consulta le quote di Amazon EFS che puoi aumentare.	26 novembre 2024
Supporta la replica tra account	Amazon EFS supporta la replica tra account. Per ulteriori informazioni, consulta Replicazione dei file system EFS su tutti Account AWS.	19 novembre 2024
Politica AWS gestita esistente aggiornata	`ReplicationRead` , `ReplicationWrite` , `iam:PassRole` vengono aggiunti alla `AmazonElasticFileSystemFullAccess` policy. Per ulteriori informazioni, consulta AmazonElasticFileSystemFullAccess.	7 novembre 2024
Politica AWS gestita esistente aggiornata	`ReplicationRead` e `ReplicationWrite` aggiunto a `AmazonElasticFileSystemServiceRolePolicy` .Per ulteriori informazioni, vedere AmazonElasticFileSystemServiceRolePolicy.	7 novembre 2024

Politica AWS gestita esistente aggiornata	Autorizzazione `ReplicationRead` aggiunta alla `AmazonElasticFileSystemReadOnlyAccess` politica esistente. Per ulteriori informazioni, consulta AmazonElasticFileSystemReadOnlyAccess.	7 novembre 2024
Limite di throughput elastico aumentato	Il limite di throughput elastico è aumentato a 60 gibibyte al secondo (GiBps) per aree specifiche Regioni AWS e a 10 GiBps per tutte le altre regioni. Per ulteriori informazioni, consulta Throughput elastico totale predefinito per tutti i client connessi in ciascuna di esse. Regione AWS	14 ottobre 2024
Politica AWS gestita esistente aggiornata	L'elemento opzionale `Sid` (statement ID) è ora incluso nella dichiarazione `AmazonElasticFileSystemReadOnlyAccess` politica. Il valore di `Sid` è `ElasticFileSystemReadOnlyAccess` . Per ulteriori informazioni sull'elemento `Sid` policy, consulta IAM JSON policy elements: Sid.	7 agosto 2024

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	31 luglio 2024
Quota aumentata per i bersagli da montare	Il numero massimo di target di montaggio per ogni cloud privato virtuale (VPC) è passato da 400 a 1.400. Per ulteriori informazioni, consulta le Quote di risorse di Amazon EFS che non puoi modificare.	15 maggio 2024
Aumento del limite di throughput combinato per i file system elastici	Il throughput massimo combinato di lettura e scrittura è 1.500 MiBps per i file system che utilizzano la velocità effettiva elastica e montati utilizzando la versione 2.0 o successiva del client Amazon EFS (amazon-efs-utils versione) o il driver Amazon EFS CSI (). aws-efs-csi-driver Per ulteriori informazioni, consulta la tabella riassuntiva delle prestazioni in Amazon EFS Performance.	30 aprile 2024

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 la protezione su un file system. Per ulteriori informazioni, consulta gli aggiornamenti di Amazon EFS alle policy AWS gestite.	27 novembre 2023

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 della 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, consulta 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 EC2 Mac in esecuzione su macOS Ventura. Per ulteriori informazioni, consulta Distribuzioni supportate.	10 aprile 2023
Supporto aggiuntivo aggiunto Regione AWS	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 cui la replica EFS non supportava socket e named pipe, oppure. FIFOs	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 target di montaggio sono ora assegnati 17 caratteri IDs. Per ulteriori informazioni, consulta Working with Amazon EFS resources.	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 il test del formato ID risorsa a 17 caratteri	Amazon EFS passerà dall'uso di 8 caratteri IDs a 17 caratteri IDs per file system e destinazi oni di montaggio il 1° ottobre 2021. Durante questa transizio ne, puoi attivare e iniziare a utilizzare risorse di 17 caratteri su base individua le. IDs Regione AWS Per ulteriori informazioni, consulta Resource. IDs	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 One Zone su un' EC2 istanza 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) rappresentano 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

Regione AWS Supporto aggiuntivo aggiunto	Amazon EFS è ora disponibile per tutti gli utenti nella regione Asia Pacifico (Osaka-Locale) Regione AWS.	3 marzo 2021
Supporto aggiunto per le istanze Amazon EC2 macOS che eseguono macOS Big Sur	Ora puoi montare il tuo file system Amazon EFS da istanze EC2 macOS 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 utilizzarlo AWS Systems Manager per installare o aggiornare automaticamente i client Amazon EFS (`amazon-efs-utils`) sulle tue EC2 istanze. 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 velocità MB/s di trasmissione 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 Creare il file system EFS.	16 luglio 2020
La nuova console Amazon EFS è ora disponibile	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, consulta 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 (Bahrein). 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 EC2 istanza.	Ora puoi configurare nuove EC2 istanze Amazon per montare i tuoi file system EFS al momento del lancio nella Launch Instance Wizard. EC2 Per ulteriori informazioni, consulta Fase 2. Crea EC2 le tue risorse e avvia la tua EC2 istanza.	17 ottobre 2019
Supporto per Service Quotas aggiunto	Ora puoi visualizzare tutti i limiti di Amazon EFS nella console Service Quotas. 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-premises.	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, consulta Mounting from Another Account o VPC e Come funziona Amazon EFS con Direct Connect e. VPNs	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, consulta 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 metrica con le metriche CloudWatch .	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 Installazione del client Amazon EFS. 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. Il nome DNS di un file system si risolve automaticamente nell'indirizzo IP di una destinazione di montaggio nella zona di disponibilità per l'istanza Amazon connessa. EC2 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 Etichettatura delle risorse EFS.	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 aggiornat a 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.