



Guide de l'utilisateur

Amazon Elastic File System



Amazon Elastic File System: Guide de l'utilisateur

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

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est ce qu'Amazon Elastic File System ?	1
Vous utilisez Amazon EFS pour la première fois ?	3
Comment ça marche	3
Comment Amazon EFS fonctionne avec Amazon EC2	5
Comment Amazon EFS fonctionne avec un AWS Direct Connect VPN AWS géré	8
Comment fonctionne Amazon EFS avec AWS Backup	9
Fonctionnalités	10
Authentification et contrôle d'accès	10
Cohérence des données dans Amazon EFS	10
Disponibilité et durabilité	11
Réplication	18
Premiers pas	19
Prérequis	19
Création d'un système de fichiers et lancement d'une EC2 instance	19
Transférez des fichiers vers votre système de fichiers	20
Prérequis	21
Nettoyage des ressources	21
Installation du client EFS	23
Dépendances pour les outils EFS	24
Distributions prises en charge :	24
Installation manuelle du client EFS	26
Installation du client Amazon EFS sur les instances Amazon EC2 Linux	26
Pour installer le client Amazon EFS sur d'autres distributions Linux	27
Installation du client EFS sur des instances EC2 Mac	28
Installation automatique du client EFS	28
Ce que fait le client Amazon EFS lors de l'installation	29
Systèmes d'exploitation pris en charge par Systems Manager	29
Configuration AWS Systems Manager pour installer le client EFS	31
Installation et mise à niveau botocore	32
Mise à niveau d'stunnel	33
Résolution des problèmes liés à l'installation de Stunnel	35
Activation du mode FIPS	36
Création et gestion de ressources	38
Récapitulatif de l'implémentation	39

Ressource IDs	41
Jeton de création et idempotence	41
Création de systèmes de fichiers	42
Autorisations IAM requises pour créer des systèmes de fichiers	43
Options de configuration pour les systèmes de fichiers	43
Suppression de systèmes de fichiers	60
Création de politiques de système de fichiers	61
Création de points d'accès	63
Supprimer des points d'accès	66
Balisage de ressources	67
Principes de base des étiquettes	67
Restrictions liées aux balises	68
Utilisation de balises pour le contrôle d'accès	69
Baliser vos ressources	69
Tutoriel : Création de sous-répertoires accessibles en écriture par utilisateur	70
Montage des systèmes de fichiers	73
Considérations relatives au montage pour Linux	73
Utilisation de l'assistant de Montage EFS	75
Paramètres de montage utilisés par l'assistant de montage EFS	77
Obtention de journaux de support	78
Prérequis	79
Montage sous EC2 Linux	81
Montage sur EC2 Mac	83
Montage depuis une autre région	85
Montage de systèmes de fichiers Zone unique	85
Montage avec autorisation IAM	89
Montage avec points d'accès EFS	90
Montage de plusieurs EC2 instances	91
Montage à partir d'un autre compte ou VPC	92
Utilisation de NFS	96
Prérequis	96
NFS Support	97
Installation du client NFS	98
Paramètres de montage NFS recommandés	100
Montage EC2 avec DNS	102
Montage avec une adresse IP	105

Montage automatique de systèmes de fichiers	106
Nouvelles instances EC2 Linux	107
Instances EC2 Linux existantes	109
Instances Linux et Mac utilisant NFS	113
Démontage des systèmes de fichiers	115
Tutoriel : Création et montage d'un système de fichiers à l'aide du AWS CLI	116
Prérequis	118
Configuration du AWS CLI	118
Étape 1 : Création de EC2 ressources	120
Étape 2 : Création de ressources EFS	125
Étape 3 : Monter et tester le système de fichiers	128
Étape 4 : nettoyer	132
Tutoriel : Montage avec des clients locaux	134
Prérequis	135
Étape 1 : Création de vos ressources EFS	137
Étape 2 : Installation du client NFS	139
Étape 3 : Monter le système de fichiers Amazon EFS sur votre client sur site	139
Étape 4 : Nettoyer les ressources et protéger votre compte AWS	141
Facultatif : Chiffrement des données en transit	142
Tutoriel : monter un système de fichiers à partir d'un autre VPC	145
Prérequis	146
Étape 1 : Déterminer l'ID de la zone de disponibilité de la cible de montage	146
Étape 2 : Déterminer l'adresse IP cible du montage	147
Étape 3 : ajouter une entrée d'hôte pour la cible de montage	148
Étape 4 : monter votre système de fichiers à l'aide de l'assistant de montage EFS	149
Étape 5 : Nettoyez les ressources et protégez votre Compte AWS	151
Résolution des problèmes de montage	152
Le montage du système de fichiers sur l'instance Windows échoue	152
Accès refusé par le serveur	152
Le montage automatique échoue et l'instance ne répond pas	152
Le montage de plusieurs systèmes de fichiers Amazon EFS dans /etc/fstab échoue	153
La commande de montage échoue avec le message d'erreur « type de fs erroné »	154
La commande de montage échoue avec le message d'erreur « option de montage incorrecte »	154
Le montage avec point d'accès échoue	155

Le montage du système de fichiers échoue immédiatement après la création du système de fichiers	155
Le montage du système de fichiers se bloque, puis échoue avec une erreur de dépassement de délai d'attente	156
Le montage d'un système de fichiers avec NFS à l'aide d'un nom DNS échoue	156
Échec du montage d'un système de fichiers avec « nfs ne répond pas »	157
L'état de cycle de vie de la cible de montage est bloqué	158
L'état du cycle de vie cible du montage indique une erreur	158
Le montage ne répond pas	158
Le client monté est déconnecté	159
Les opérations sur un système de fichiers nouvellement monté renvoient l'erreur « mauvaise gestion de fichier »	160
Le démontage d'un système de fichiers échoue	160
Transfert de données	162
En utilisant AWS DataSync	162
En utilisant AWS Transfer Family	163
Conditions préalables à l'utilisation AWS Transfer Family avec Amazon EFS	164
Configuration de votre système de fichiers EFS pour AWS Transfer Family	164
Gestion des systèmes de fichiers	170
Comprendre l'état du système de fichiers	170
Gérer des cibles de Montage	171
Cibles de montage et zones de disponibilité	172
Création de cibles de montage	175
Supprimer des cibles de montage	181
Modification du VPC cible de montage	183
Modification des groupes de sécurité cibles de montage	183
Gestion du débit	185
Gestion du cycle de vie du stockage	187
Opérations sur le système de fichiers pour la gestion du cycle de vie	188
Configuration des politiques de cycle de vie	188
Gestion de l'accès aux systèmes de fichiers chiffrés	191
Gestion des clés KMS pour les systèmes de fichiers EFS	192
Surveillance	194
Outils de surveillance	195
Outils automatisés	195
Outils de surveillance manuelle	196

Mesures sur un système de fichiers	197
Objets de mesure	197
Taille du système de fichiers mesurée	198
Débit de mesure	200
Affichage de classe de stockage	201
Surveillance des métriques avec CloudWatch	202
CloudWatch métriques	203
Accès aux CloudWatch métriques	210
Utilisation de CloudWatch métriques	211
Utiliser les mathématiques métriques avec CloudWatch les métriques	213
Surveillance des réussites et des échecs des tentatives de montage	219
Création d'alarmes	220
Journalisation des appels d'API CloudTrail avec	222
Informations Amazon EFS dans CloudTrail	223
Présentation des entrées des fichiers journaux Amazon EFS	224
Entrées du fichier journal Amazon EFS pour les systèmes de encrypted-at-rest fichiers	231
Utilisation des rapports de facturation et d'utilisation	232
Utilisation des balises de répartition des coûts	232
Balises de répartition des coûts définies par l'utilisateur	233
Rapports de facturation	234
Rapports d'utilisation	235
Présentation des rapports d'utilisation et de facturation	236
Opérations de suivi dans vos rapports d'utilisation	241
Spécifications de performance	242
Récapitulatif des performances	242
Classes de stockage	244
Modes de performances	245
Modes de débit	245
Choix d'un mode de débit	246
Débit élastique	246
Débit alloué	247
Restrictions relatives au débit de commutation et à la modification du montant provisionné ..	250
Conseils sur les performances	250
I/O Taille moyenne	250
Optimisation des charges de travail exigeant un débit et des IOPS élevés	250
Connexions simultanées	251

Modèle de demande	251
Paramètres de Montage du client NFS	252
Optimisation des performances des petits fichiers	253
Optimisation des performances de disque	253
Optimisation de la taille NFS read_ahead_kb	254
Résolution des problèmes de performances	255
Impossible de créer un système de fichiers EFS	256
Accès refusé aux fichiers autorisés sur le système de fichiers NFS	256
Erreurs lors de l'accès à la console Amazon EFS	256
L' EC2 instance Amazon se bloque	257
Une application qui écrit de grandes quantités de données se bloque	257
Performances médiocres à l'ouverture de plusieurs fichiers en parallèle	258
Paramètres NFS personnalisés entraînant des délais d'écriture	258
La création de sauvegardes avec Oracle Recovery Manager est lente	259
Résolution des problèmes d'AMI et de noyau	260
Impossible d'exécuter la commande chown	260
Le système de fichiers continue à effectuer des opérations plusieurs fois en raison d'un bogue client	261
Client bloqué	261
L'affichage de la liste de fichiers d'un répertoire volumineux prend beaucoup de temps.	261
Sauvegarde et réplication des données	263
Sauvegarde des systèmes de fichiers	263
Comment AWS Backup fonctionne avec Amazon EFS	264
Autorisations IAM requises	266
Performances de sauvegarde	266
Gestion des sauvegardes automatiques	267
Répliquer des systèmes de fichiers	268
Coûts	270
Performance de réplication	270
Autorisations IAM requises	270
Configuration de la réplication vers un nouveau système de fichiers	271
Configuration de la réplication vers un système de fichiers existant	276
Réplication entre comptes AWS	283
Affichage des détails de réplication	287
Supprimer des configuration de réplication	292
Utilisation de la réplique	294

Sécurisation des données	296
Chiffrement de données	297
AWS KMS	298
Chiffrement de données au repos	301
chiffrement des données en transit	302
Résolution des problèmes de chiffrement	304
Gestion des identités et des accès	307
Public ciblé	307
Authentification par des identités	308
Gestion des accès à l'aide de politiques	312
Comment Amazon Elastic File System fonctionne avec IAM	315
Exemples de politiques basées sur l'identité	323
Exemples de stratégies basées sur les ressources	327
AWS politiques gérées	331
Utilisation des balises avec Amazon EFS	337
Utilisation des rôles liés à un service pour Amazon EFS	341
Résolution des problèmes	345
Contrôle de l'accès aux données du système de fichiers	347
Stratégie de système de fichiers par défaut	348
Actions EFS pour les clients	348
Clés de condition EFS pour les clients NFS	349
Exemples de stratégie de système de fichiers	350
Contrôle de l'accès réseau	350
Utilisation de groupes de sécurité VPC	350
Utilisation des points de terminaison d'un VPC	353
Utilisateurs, groupes et autorisations de niveau NFS	355
Autorisations sur les fichiers et les répertoires	356
Exemples de cas d'utilisation et d'autorisations du système de fichiers EFS	357
Autorisations d'identification d'utilisateur et de groupe pour les fichiers et les répertoires d'un système de fichiers	358
Aucun écrasement racine	359
Mise en cache des autorisations	362
Modification de la propriété d'un objet du système de fichiers	362
Points d'accès EFS	362
Utilisation des points d'accès	363
Application forcée d'une identité d'utilisateur	364

Application forcée d'un répertoire racine	365
Utilisation des points d'accès dans les stratégies IAM	367
Blocage de l'accès public aux systèmes de fichiers	368
Blocage de l'accès public avec AWS Transfer Family	369
La signification du mot « public »	369
Validation de conformité	371
Résilience	372
Isolement de réseau	374
Quotas	375
Les quotas Amazon EFS que vous pouvez augmenter	375
Demande d'augmentation de quota	378
Les quotas de ressources Amazon EFS que vous ne pouvez pas Modifier	378
Quotas pour les clients NFS	380
Quotas pour les systèmes de fichiers Amazon EFS	381
Fonctionnalités NFSv4 4.0 et 4.1 non prises en charge	382
Considérations supplémentaires	383
Résolution des erreurs de fonctionnement des fichiers liées aux quotas	384
Échec de la commande avec l'erreur « Quota de disque dépassé »	384
Échec de la commande avec l'erreur « Erreur d'E/S »	385
Échec de la commande avec l'erreur « Le nom de fichier est trop long »	385
Échec de la commande avec l'erreur « Fichier introuvable »	386
Échec de la commande avec l'erreur « Trop de liens »	386
Échec de la commande avec l'erreur « Fichier trop volumineux »	386
API Amazon EFS	387
Points de terminaison d'API	387
IPv4 points de terminaison	388
Points de terminaison à double pile (IPv4 et IPv6)	388
Spécification des points de terminaison	389
Version de l'API	389
Rubriques en relation	389
Utilisation du débit de demandes d'API de requête pour Amazon EFS	390
Interrogation	390
Nouvelles tentatives ou traitement par lots	390
Calcul de l'intervalle de veille	390
Actions	391
CreateAccessPoint	393

CreateFileSystem	401
CreateMountTarget	417
CreateReplicationConfiguration	432
CreateTags	438
DeleteAccessPoint	441
DeleteFileSystem	443
DeleteFileSystemPolicy	447
DeleteMountTarget	450
DeleteReplicationConfiguration	454
DeleteTags	457
DescribeAccessPoints	460
DescribeAccountPreferences	465
DescribeBackupPolicy	468
DescribeFileSystemPolicy	471
DescribeFileSystems	475
DescribeLifecycleConfiguration	481
DescribeMountTargets	485
DescribeMountTargetSecurityGroups	491
DescribeReplicationConfigurations	495
DescribeTags	499
ListTagsForResource	504
ModifyMountTargetSecurityGroups	508
PutAccountPreferences	512
PutBackupPolicy	515
PutFileSystemPolicy	518
PutLifecycleConfiguration	524
TagResource	533
UntagResource	537
UpdateFileSystem	540
UpdateFileSystemProtection	548
Types de données	552
AccessPointDescription	553
BackupPolicy	556
CreationInfo	557
Destination	559
DestinationToCreate	562

FileSystemDescription	566
FileSystemProtectionDescription	571
FileSystemSize	572
LifecyclePolicy	574
MountTargetDescription	576
PosixUser	580
ReplicationConfigurationDescription	582
ResourceIdPreference	584
RootDirectory	585
Tag	587
Historique du document	588
.....	dcxix

Qu'est ce qu'Amazon Elastic File System ?

Amazon Elastic File System (Amazon EFS) fournit un stockage de fichiers entièrement élastique sans serveur pour vous permettre de partager des données de fichiers sans provisionner ni gérer la capacité et les performances de stockage. Amazon EFS est conçu pour se mettre à l'échelle à la demande et peut atteindre plusieurs pétaoctets sans perturber les applications. Il augmente ou diminue automatiquement la capacité au fil de vos ajouts et suppressions de fichiers. Comme Amazon EFS propose une interface de services web simple, vous pouvez créer et configurer des systèmes de fichiers rapidement et facilement. Le service gère toute l'infrastructure de stockage de fichiers pour vous, ce qui vous libère des tâches compliquées liées au déploiement, à l'application de correctifs et à la gestion des configurations de systèmes de fichiers complexes.

Amazon EFS prend en charge le protocole Network File System version 4 (NFSv4.1 et NFSv4 .0), de sorte que les applications et les outils que vous utilisez aujourd'hui fonctionnent parfaitement avec Amazon EFS. Amazon EFS est accessible sur la plupart des types d'instances de calcul Amazon Web Services EC2, notamment Amazon, Amazon ECS AWS Lambda, Amazon EKS et AWS Fargate.

Le service est conçu pour être hautement évolutif, hautement disponible et hautement durable. Amazon EFS propose les types de systèmes de fichiers suivants pour répondre à vos besoins de disponibilité et de durabilité :

- Régional (recommandé) — Les systèmes de fichiers régionaux (recommandé) stockent les données de manière redondante dans plusieurs zones de disponibilité géographiquement séparées au sein d'une même zone. Région AWS Le stockage des données dans plusieurs zones de disponibilité garantit la disponibilité continue des données, même lorsqu'une ou plusieurs zones de disponibilité d'une zone Région AWS ne sont pas disponibles.
- Les systèmes de fichiers One Zone — One Zone stockent les données dans une seule zone de disponibilité. Le stockage des données dans une zone de disponibilité unique garantit leur disponibilité continue. Dans le cas peu probable de perte ou d'endommagement de la totalité ou d'une partie de la zone de disponibilité, les données stockées dans ces types de systèmes de fichiers risquent d'être perdues.

Pour plus d'informations sur les types de systèmes de fichiers, consultez [Types de système de fichiers EFS](#).

Amazon EFS est conçu pour fournir le débit, le nombre d'opérations d'E/S par seconde et la faible latence nécessaires pour de nombreuses charges de travail. Ils peuvent atteindre une capacité de plusieurs pétaoctets, présentent de hauts niveaux de débit et autorisent un accès parallèle massif des instances à vos données. Pour la plupart des charges de travail, nous recommandons d'utiliser les modes par défaut, à savoir le mode de performance à usage général et les modes de débit élastique.

- Usage général — Le mode de performance à usage général est idéal pour les applications sensibles à la latence, telles que les environnements de serveur Web, les systèmes de gestion de contenu, les répertoires de base et le service de fichiers général.
- Élastique : le mode de débit élastique est conçu pour augmenter ou diminuer automatiquement les performances de débit afin de répondre aux besoins de votre activité de charge de travail.

Pour plus d'informations sur les performances et les modes de débit de l'EFS, consultez [Spécifications de performance d'Amazon EFS](#).

Amazon EFS fournit des file-system-access éléments sémantiques, tels que la cohérence renforcée des données et le verrouillage des fichiers. Pour de plus amples informations, veuillez consulter [Cohérence des données dans Amazon EFS](#). &EFS; vous permet également de contrôler précisément l'accès à vos systèmes de fichiers grâce à des autorisations POSIX (Portable Operating System Interface). Pour de plus amples informations, veuillez consulter [Sécurisation de vos données dans Amazon EFS](#).

Amazon EFS prend en charge les fonctionnalités d'authentification, d'autorisation et de chiffrement pour vous aider à répondre à vos exigences de sécurité et de conformité. Amazon EFS prend en charge deux formes de chiffrement pour les systèmes de fichiers, le chiffrement en transit et le chiffrement au repos. Vous pouvez activer le chiffrement au repos lors de la création d'un système de fichiers EFS. Si vous le faites, toutes vos données et métadonnées sont chiffrées. Vous pouvez activer le chiffrement des données en transit lors du montage du système de fichiers. L'accès des clients NFS à Amazon EFS est contrôlé à la fois par des politiques AWS Identity and Access Management (IAM) et des politiques de sécurité réseau, telles que les groupes de sécurité. Pour plus d'informations, consultez [Chiffrement des données dans Amazon EFS](#), [Gestion des identités et des accès pour Amazon EFS](#) et [Contrôle de l'accès réseau aux systèmes de fichiers EFS pour les clients NFS](#).

 Note

L'utilisation d'Amazon EFS avec des EC2 instances Amazon basées sur Microsoft Windows n'est pas prise en charge.

Vous utilisez Amazon EFS pour la première fois ?

Si vous utilisez Amazon EFS pour la première fois, nous vous recommandons de lire les sections suivantes dans l'ordre :

1. Pour une présentation générale des produits et de la tarification , [consultez Amazon EFS](#).
2. Pour une présentation technique d'Amazon EFS, consultez [Comment fonctionne Amazon EFS](#).
3. Essayez l'[Premiers pas](#)exercice.

Si vous souhaitez en savoir plus sur Amazon EFS, les rubriques suivantes traitent du service plus en détail :

- [Création et gestion des ressources EFS](#)
- [Gestion des systèmes de fichiers EFS](#)
- [API Amazon EFS](#)

Comment fonctionne Amazon EFS

Amazon Elastic File System (EFS) fournit un système de fichiers set-and-forget élastique simple, sans serveur. Avec Amazon EFS, vous pouvez créer un système de fichiers, le monter sur une EC2 instance Amazon, puis lire et écrire des données depuis et vers votre système de fichiers. Vous pouvez monter un système de fichiers EFS dans votre cloud privé virtuel (VPC) via le protocole Network File System versions 4.0 et 4.1 (NFSv4). Nous vous recommandons d'utiliser un client Linux NFSv4 .1 de dernière génération, tel que ceux que l'on trouve dans les dernières versions d'Amazon Linux, Amazon Linux 2, Red Hat, Ubuntu et macOS Big Sur AMIs, en conjonction avec l'assistant de montage EFS. Pour obtenir des instructions, veuillez consulter [Installation du client Amazon EFS](#).

Pour obtenir la liste des Amazon Machine Images (AMIs) Amazon EC2 Linux et macOS compatibles avec ce protocole, consultez [NFS Support](#). Pour certains AMIs, vous devez installer un client NFS

pour monter votre système de fichiers sur votre EC2 instance Amazon. Pour obtenir des instructions, veuillez consulter [Installation du client NFS](#).

Vous pouvez accéder à votre système de fichiers EFS simultanément à partir de plusieurs clients NFS, de sorte que les applications qui s'étendent au-delà d'une simple connexion peuvent accéder à un système de fichiers. Amazon EC2 et d'autres instances de AWS calcul exécutées dans plusieurs zones de disponibilité au sein d'une même instance Région AWS peuvent accéder au système de fichiers, de sorte que de nombreux utilisateurs peuvent accéder à une source de données commune et la partager.

Pour obtenir une liste des Régions AWS emplacements dans lesquels vous pouvez créer un système de fichiers EFS, consultez le [Référence générale d'Amazon Web Services](#).

Pour accéder à votre système de fichiers EFS dans un VPC, vous devez créer une ou plusieurs cibles de montage dans le VPC. Une cible de montage fournit l'adresse IP d'un NFSv4 point de terminaison sur lequel vous pouvez monter un système de fichiers EFS. Vous montez votre système de fichiers à l'aide de son nom DNS (Domain Name Service), qui correspond à l'adresse IP de la cible de montage EFS située dans la même zone de disponibilité que votre EC2 instance. Vous pouvez créer une cible de montage dans chaque zone de disponibilité dans Région AWS. Si votre VPC comporte plusieurs sous-réseaux dans une zone de disponibilité, vous pouvez créer une cible de montage dans l'un de ces sous-réseaux. Toutes les EC2 instances de cette zone de disponibilité partagent alors cette cible de montage.

 Note

Un système de fichiers EFS ne peut avoir de cibles de montage que dans un seul VPC à la fois.

Les cibles de montage sont elles-mêmes conçues pour être hautement disponibles. Lorsque vous concevez votre application pour garantir une haute disponibilité et un basculement vers d'autres zones de disponibilité, n'oubliez pas que les adresses IP et le DNS de vos cibles de montage sont statiques dans chaque zone de disponibilité et qu'il s'agit d'éléments redondants sauvegardés par plusieurs ressources. Pour plus d'informations sur les cibles de montage, consultez [Gérer des cibles de Montage](#).

Une fois le système de fichiers monté à l'aide de son nom DNS, vous l'utilisez comme tout autre système de fichiers compatible POSIX. Pour plus d'informations sur les autorisations de niveau

NFS et les considérations associées, consultez [Utilisateurs, groupes et autorisations au niveau du système de fichiers réseau \(NFS\)](#).

Vous pouvez monter vos systèmes de fichiers EFS sur les serveurs de votre centre de données sur site lorsque vous êtes connecté à votre Amazon VPC AWS Direct Connect avec ou. AWS VPN Vous pouvez monter vos systèmes de fichiers EFS sur des serveurs locaux pour migrer des ensembles de données vers EFS, activer des scénarios d'éclatement dans le cloud ou sauvegarder vos données sur site sur Amazon EFS.

Vous trouverez ci-dessous une description de la manière dont Amazon EFS fonctionne avec d'autres services.

Rubriques

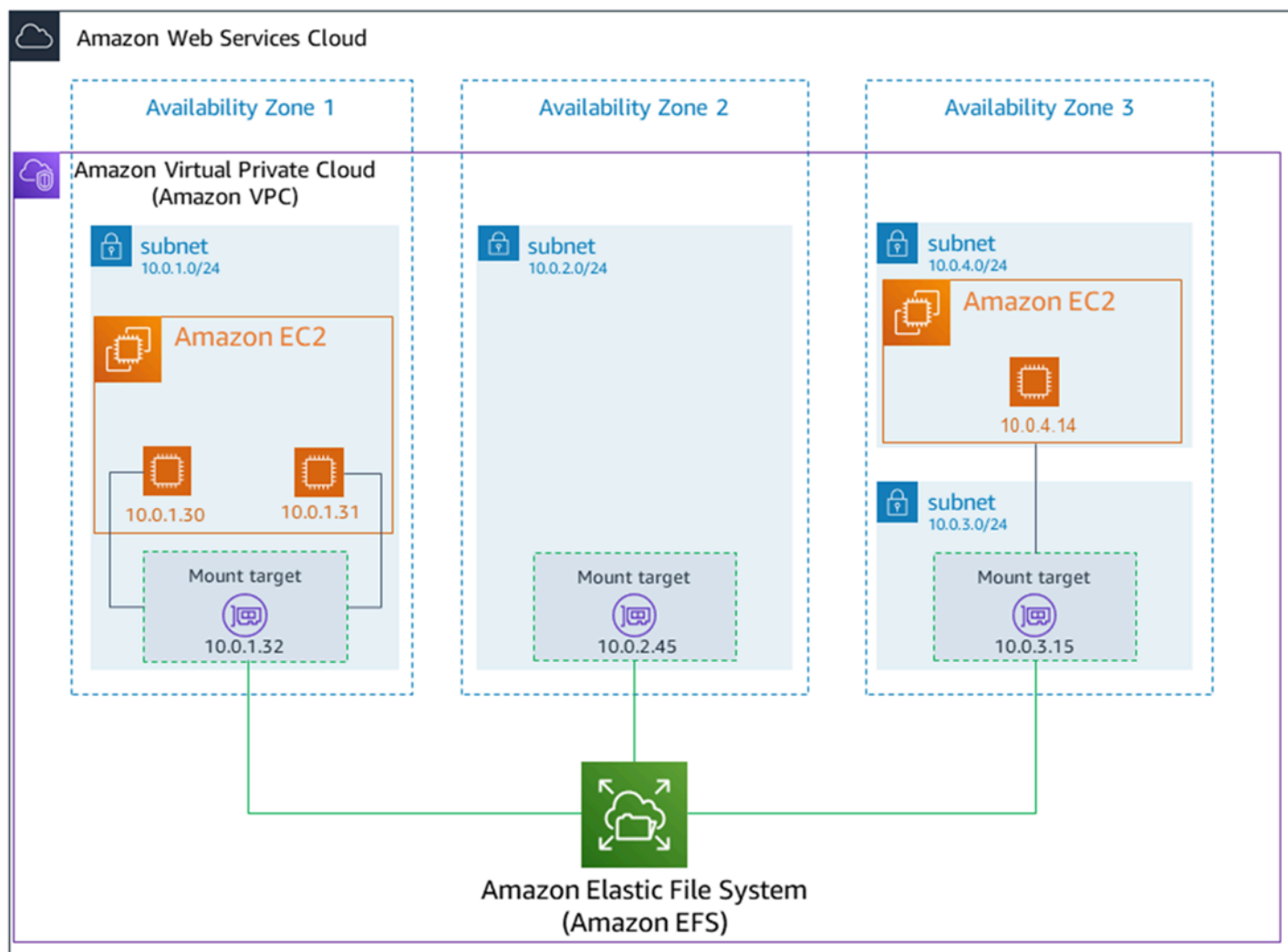
- [Comment Amazon EFS fonctionne avec Amazon EC2](#)
- [Comment Amazon EFS fonctionne avec un AWS Direct Connect VPN AWS géré](#)
- [Comment fonctionne Amazon EFS avec AWS Backup](#)

Comment Amazon EFS fonctionne avec Amazon EC2

Cette section explique comment les systèmes de fichiers Amazon EFS Regional et One Zone sont montés sur les EC2 instances d'un Amazon VPC.

Systèmes de fichiers EFS régionaux

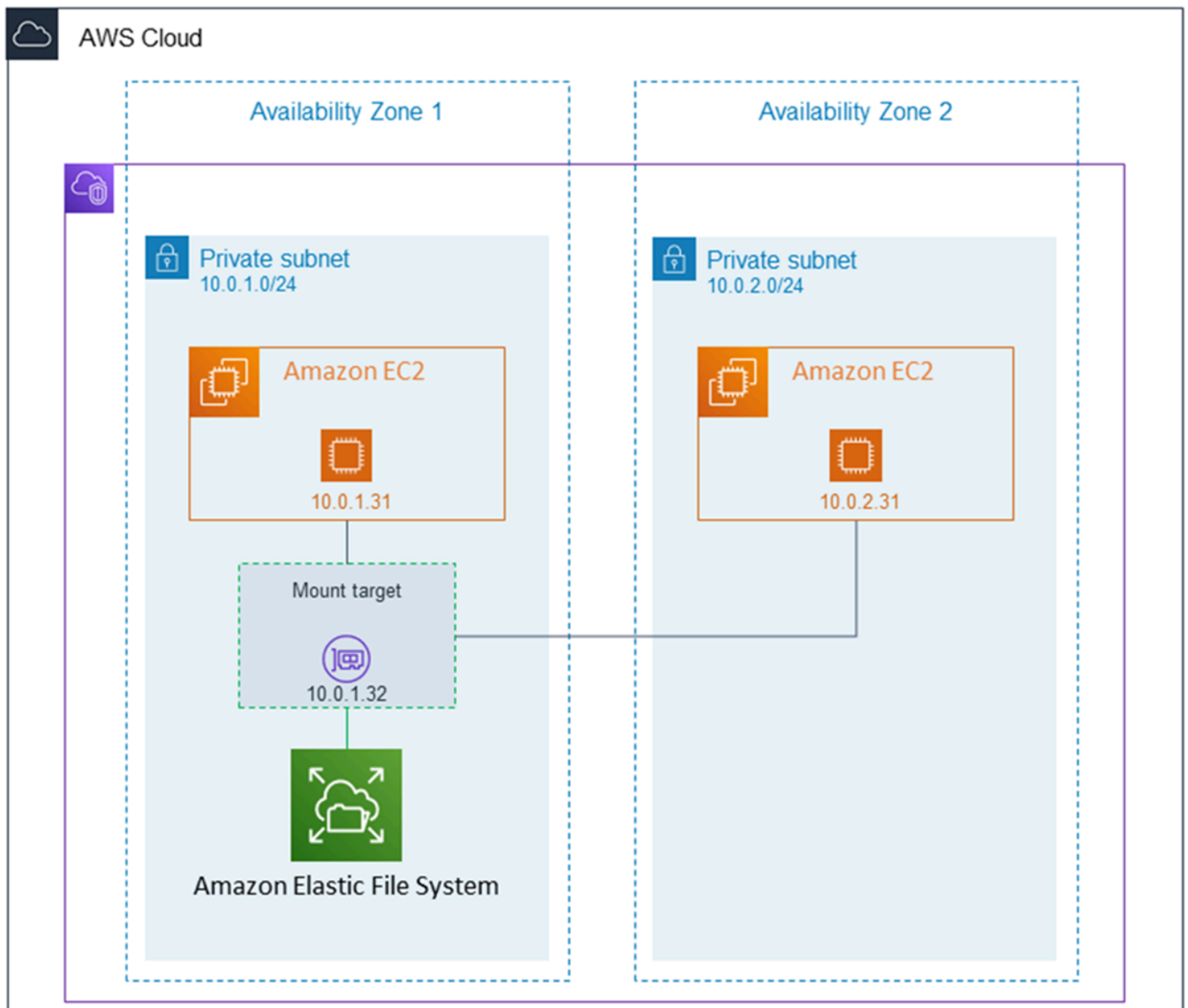
L'illustration suivante montre plusieurs EC2 instances accédant à un système de fichiers Amazon EFS configuré pour plusieurs zones de disponibilité dans un Région AWS.



Dans cette illustration, le cloud privé virtuel (VPC) comporte trois zones de disponibilité. Le système de fichiers étant régional, une cible de montage a été créée dans chaque zone de disponibilité. Nous recommandons que l'accès au système de fichiers s'effectue à partir d'une cible de montage dans la même zone de disponibilité pour des raisons de performance et de coût. L'une des zones de disponibilité comporte deux sous-réseaux. Toutefois, une cible de montage est créée dans un seul de ces sous-réseaux. Pour de plus amples informations, veuillez consulter [Montage de systèmes de fichiers EFS à l'aide de l'assistant de montage EFS](#).

Systèmes de fichiers EFS One Zone

L'illustration suivante montre plusieurs EC2 instances accédant à un système de fichiers One Zone à partir de différentes zones de disponibilité en une seule Région AWS.



Dans cette illustration, le VPC possède deux zones de disponibilité, chacune dotée d'un sous-réseau. Le type de système de fichiers étant One Zone, il ne peut avoir qu'une seule cible de montage. Pour améliorer les performances et les coûts, nous vous recommandons d'accéder au système de fichiers à partir d'une cible de montage située dans la même zone de disponibilité que l'EC2 instance sur laquelle vous le montez.

Dans cet exemple, l'EC2 instance de la zone de disponibilité us-west-2c paiera des frais d'accès aux EC2 données pour accéder à une cible de montage dans une autre zone de disponibilité. Pour de plus amples informations, veuillez consulter [Montage de systèmes de fichiers Zone unique](#).

Comment Amazon EFS fonctionne avec un AWS Direct Connect VPN AWS géré

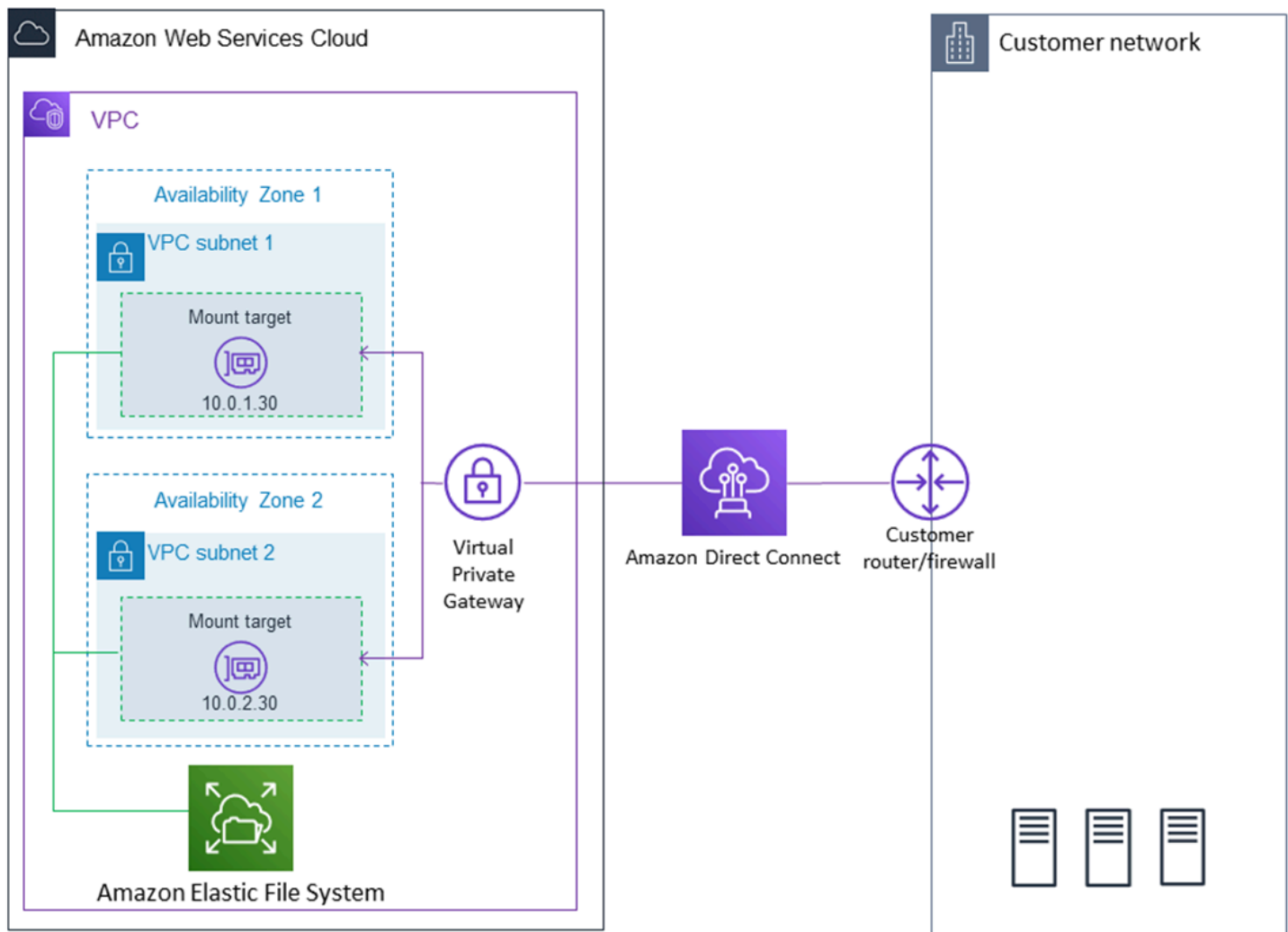
En utilisant un système de fichiers Amazon EFS monté sur un serveur sur site, vous pouvez migrer les données sur site vers le système de fichiers AWS Cloud hébergé dans un système de fichiers Amazon EFS. Vous pouvez également tirer parti de la transmission par rafales. En d'autres termes, vous pouvez transférer des données de vos serveurs sur site vers Amazon EFS et les analyser sur une flotte d' EC2 instances Amazon dans votre Amazon VPC. Vous pouvez ensuite stocker les résultats de façon permanente dans votre système de fichiers ou rapatrier les résultats sur votre serveur sur site.

Gardez les considérations suivantes à l'esprit lorsque vous utilisez Amazon EFS avec un serveur sur site :

- Votre serveur sur site doit disposer d'un système d'exploitation Linux. Nous recommandons un noyau Linux version 4.0 ou ultérieure.
- Dans un souci de simplicité, nous recommandons d'installer un système de fichiers Amazon EFS sur un serveur sur site en utilisant une adresse IP de montage cible au lieu d'un nom DNS.

Aucun coût supplémentaire n'est encouru pour l'accès à vos systèmes de fichiers Amazon EFS sur site. La AWS Direct Connect connexion à votre Amazon VPC vous est facturée. Pour en savoir plus, consultez [Pricing AWS Direct Connect](#) (Tarification).

L'illustration suivante présente un exemple d'accès à un système de fichiers Amazon EFS à partir de serveurs sur site (les serveurs sur site possèdent des systèmes de fichiers montés).



Vous pouvez utiliser n'importe quelle cible de montage dans votre VPC si vous pouvez atteindre le sous-réseau de cette cible de montage en utilisant une AWS Direct Connect connexion entre votre serveur local et votre VPC. Pour accéder à Amazon EFS à partir d'un serveur sur site, ajoutez une règle à votre groupe de sécurité de cible de montage afin d'autoriser le trafic entrant vers le port NFS (2049) à partir de votre serveur sur site. Pour plus d'informations, y compris les procédures détaillées, consultez [Prérequis](#).

Comment fonctionne Amazon EFS avec AWS Backup

Pour implémenter une sauvegarde complète de vos systèmes de fichiers, vous pouvez utiliser Amazon EFS avec AWS Backup. AWS Backup est un service de sauvegarde entièrement géré qui facilite la centralisation et l'automatisation de la sauvegarde des données entre les AWS services dans le cloud et sur site. Vous pouvez ainsi configurer de manière centralisée les politiques de sauvegarde et surveiller les activités de sauvegarde de vos AWS ressources. AWS Backup

Amazon EFS donne toujours la priorité aux opérations du système de fichiers par rapport aux opérations de sauvegarde. Pour en savoir plus sur la sauvegarde des systèmes de fichiers EFS à AWS Backup l'aide de [Sauvegarde des systèmes de fichiers EFS](#).

Fonctionnalités d'Amazon EFS

Voici les fonctionnalités d'Amazon EFS.

Rubriques

- [Authentification et contrôle d'accès](#)
- [Cohérence des données dans Amazon EFS](#)
- [Disponibilité et durabilité des systèmes de fichiers EFS](#)
- [Réplication](#)

Authentification et contrôle d'accès

Vous devez disposer d'informations d'identification valides pour utiliser la console de gestion Amazon EFS et pour effectuer des demandes d'API Amazon EFS, par exemple pour créer un système de fichiers. En outre, vous devez également être autorisé à créer ou à accéder à d'autres EFS et AWS ressources.

Les utilisateurs et les rôles que vous créez dans AWS Identity and Access Management (IAM) doivent être autorisés à créer des ressources ou à y accéder. Pour plus d'informations sur les autorisations, consultez [Gestion des identités et des accès pour Amazon EFS](#).

IAM pour les clients NFS est une option de sécurité supplémentaire pour Amazon EFS. Amazon EFS utilise IAM pour simplifier la gestion des accès pour les clients NFS (Network File System) à grande échelle. Avec l'autorisation IAM pour les clients NFS, vous pouvez utiliser IAM pour gérer l'accès à un système de fichiers EFS de manière intrinsèquement évolutive. L'autorisation IAM pour les clients NFS est également optimisée pour les environnements cloud. Pour plus d'informations sur l'utilisation d'une autorisation pour les clients NFS, veuillez consulter [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#).

Cohérence des données dans Amazon EFS

Amazon EFS fournit la sémantique de close-to-open cohérence que les applications attendent de NFS.

Sur Amazon EFS, les opérations d'écriture pour les systèmes de fichiers régionaux sont stockées durablement dans les zones de disponibilité dans ces situations :

- Une application effectue une opération d'écriture synchrone (par exemple, à l'aide de la commande Linux `open` avec l'indicateur `O_DIRECT`, ou à l'aide de la commande Linux `fsync`).
- Une application ferme un fichier.

Selon le modèle d'accès, Amazon EFS peut fournir de meilleures garanties de cohérence que la `close-to-open` sémantique. Les applications qui accèdent aux données de manière synchrone et effectuent des écritures sans ajout sont `read-after-write` cohérentes en matière d'accès aux données.

Verrouillage de fichiers

Les applications clientes NFS peuvent utiliser le verrouillage de fichiers NFS version 4 (y compris le verrouillage par plage d'octets) pour les opérations de lecture et d'écriture sur les fichiers Amazon EFS.

Notez ce qui suit concernant le verrouillage de fichiers Amazon EFS :

- Amazon EFS prend uniquement en charge le verrouillage consultatif et les `read/write` opérations ne vérifient pas la présence de verrous conflictuels avant de les exécuter. Par exemple, pour éviter les problèmes de synchronisation de fichiers liés aux opérations atomiques, votre application doit connaître la sémantique NFS (telle que `close-to-open` la cohérence).
- N'importe quel fichier peut avoir jusqu'à 512 verrous sur l'ensemble des instances connectées et des utilisateurs ayant accès au fichier.

Disponibilité et durabilité des systèmes de fichiers EFS

Cette section décrit les types de systèmes de fichiers et les options de classe de stockage pour les systèmes de fichiers Amazon Elastic File System (Amazon EFS).

Types de système de fichiers EFS

Amazon EFS propose des types de systèmes de fichiers régionaux et à zone unique.

- Régional — Les systèmes de fichiers régionaux (recommandé) stockent les données de manière redondante dans plusieurs zones de disponibilité séparées géographiquement au sein d'une même zone. Région AWS Le stockage des données dans plusieurs zones de disponibilité garantit la

disponibilité continue des données, même lorsqu'une ou plusieurs zones de disponibilité d'une zone Région AWS ne sont pas disponibles.

- Les systèmes de fichiers One Zone — One Zone stockent les données dans une seule zone de disponibilité. Le stockage des données dans une seule zone de disponibilité garantit la disponibilité continue des données. Dans le cas peu probable de perte ou d'endommagement de la totalité ou d'une partie de la zone de disponibilité, les données stockées dans ces types de systèmes de fichiers risquent d'être perdues.

Dans le cas peu probable de perte ou d'endommagement de la totalité ou d'une partie d'une zone de AWS disponibilité, les données d'une classe de stockage One Zone peuvent être perdues. Par exemple, des événements tels que le feu et les dégâts d'eau peuvent entraîner une perte de données. En dehors de ces types d'événements, nos classes de stockage de Zone unique utilisent des conceptions techniques similaires à celles de nos classes de stockage régionales pour protéger les objets contre les défaillances indépendantes au niveau du disque, de l'hôte et du rack, et chacune est conçue pour offrir une durabilité des données de 99,999999999 %.

Pour une protection accrue des données, Amazon EFS sauvegarde automatiquement les systèmes de fichiers One Zone avec AWS Backup. Vous pouvez restaurer les sauvegardes du système de fichiers dans n'importe quelle zone de disponibilité opérationnelle au sein d'un Région AWS, ou vous pouvez les restaurer dans une autre Région AWS. Les sauvegardes du système de fichiers EFS créées et gérées à l'aide de ce système AWS Backup sont répliquées dans trois zones de disponibilité et sont conçues pour durer. Pour plus d'informations, consultez [Resilience in AWS Backup](#).

 Note

Les systèmes de fichiers One Zone ne sont disponibles que pour certaines zones de disponibilité. Pour consulter un tableau répertoriant les zones de disponibilité dans lesquelles vous pouvez utiliser les systèmes de fichiers One Zone, consultez [Zones de disponibilité prises en charge pour les systèmes de fichiers One Zone](#).

Le tableau suivant compare les types de systèmes de fichiers, y compris leur disponibilité, leur durabilité et d'autres considérations.

Type de système de fichiers	Conçues pour	Durabilité (conçue pour)	Disponibilité	Zones de disponibilité	Autres considérations
Régional	Des données nécessitant une durabilité et une disponibilité maximales.	99,999999 999 % (11 9 s)	99,99 %	>=3	Aucun
Zone unique	Des données qui ne nécessitent pas une durabilité et une disponibilité optimales.	99,999999 999 % (11 9 s)	99,99 %	1	Inrésilient à la perte de la zone de disponibilité

Zones de disponibilité prises en charge pour les systèmes de fichiers One Zone

Les systèmes de fichiers One Zone ne sont disponibles que pour certaines zones de disponibilité. Le tableau suivant répertorie les zones de disponibilité Région AWS et IDs les zones de disponibilité dans lesquelles vous pouvez utiliser les systèmes de fichiers One Zone. Pour voir le mappage entre AZ et IDs les zones de disponibilité de votre compte, consultez [la section Zone de disponibilité IDs de vos AWS ressources](#) dans le guide de l'utilisateur de AWS Resource Access Manager.

Zones de disponibilité prenant en charge les systèmes de fichiers One Zone

Région AWS Nom	Région AWS Code	AZ pris en charge IDs
USA Est (Ohio)	us-east-2	use2-az1, use2-az2, use2-az3
USA Est (Virginie du Nord)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
USA Ouest (Californie du Nord)	us-west-1	usw1-az1, usw1-az3
USA Ouest (Oregon)	us-west-2	usw2-az1, usw2-az2, usw2-az3, usw2-az4

Région AWS Nom	Région AWS Code	AZ pris en charge IDs
Afrique (Le Cap)	af-south-1	afs1-az1, afs1-az2, afs1-az3
Asie-Pacifique (Hong Kong)	ap-east-1	ape1-az1, ape1-az2, ape1-az3
Asie-Pacifique (Mumbai)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
Asie-Pacifique (Osaka)	ap-northeast-3	apné3-az1, apné3-az2, apné3-az3
Asie-Pacifique (Séoul)	ap-northeast-2	apne2-az1, apne2-az2, apne2-az3
Asie-Pacifique (Singapour)	ap-southeast-1	apse1-az1, apse1-az2
Asie-Pacifique (Sydney)	ap-southeast-2	apse2-az1, apse2-az2, apse2-az3
Asie-Pacifique (Tokyo)	ap-northeast-1	apné1-az1, apné1-az4
Canada (Centre)	ca-central-1	cac1-az1, cac1-az2
Chine (Beijing)	cn-north-1	cnn1-az1, cnn1-az2
Chine (Ningxia)	cn-northwest-1	cnnw1-az1, cnnw1-az2, cnnw1-az3
Europe (Francfort)	eu-central-1	euc1-az1, euc1-az2, euc1-az3
Europe (Irlande)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europe (Londres)	eu-west-2	euw2-az1, euw2-az2
Europe (Milan)	eu-south-1	eus1-az1, eus1-az2, eus1-az3
Europe (Paris)	eu-west-3	euw3-az1, euw3-az3
Europe (Stockholm)	eu-north-1	eun1-az1, eun1-az2, eun1-az3

Région AWS Nom	Région AWS Code	AZ pris en charge IDs
Moyen-Orient (Bahreïn)	me-south-1	mes1-az1, mes1-az2, mes1-az3
Amérique du Sud (São Paulo)	sa-east-1	sae1-az1, sae1-az2, sae1-az3
AWS GovCloud (USA Est)	us-gov-east-1	usge1-az1, usge1-az2, usge1-az3
AWS GovCloud (US-Ouest)	us-gov-west-1	usgw1-az1, usgw1-az2, usgw1-az3

Classes de stockage EFS

Amazon EFS propose différentes classes de stockage conçues pour le stockage le plus efficace en fonction des cas d'utilisation.

- **EFS Standard** — La classe de stockage EFS Standard utilise le stockage sur disque SSD (Solid State Drive) pour fournir les niveaux de latence les plus faibles pour les fichiers fréquemment consultés. Les nouvelles données du système de fichiers sont d'abord écrites dans la classe de stockage EFS Standard, puis peuvent être hiérarchisées selon les classes de stockage EFS Infrequent Access et EFS Archive à l'aide de la gestion du cycle de vie.
- **Accès peu fréquent (IA) EFS** : classe de stockage optimisée en termes de coûts pour les données auxquelles on ne accède que quelques fois par trimestre.
- **Archive EFS** : classe de stockage optimisée en termes de coûts pour les données consultées plusieurs fois par an ou Moins.

La classe de stockage EFS Archive est prise en charge sur les systèmes de fichiers EFS dotés d'un débit élastique. Vous ne pouvez pas mettre à jour le débit de votre système de fichiers vers En rafales ou Alloué une fois que le système de fichiers contient des données dans la classe de stockage Archive.

Comparaison des classes de stockage

Le tableau suivant compare les classes de stockage. Pour plus d'informations sur les performances de chaque classe de stockage, consultez [Spécifications de performance d'Amazon EFS](#).

Classe de stockage	Conçues pour	Latence de lecture du premier octet	Durabilité (conçu pour) ¹	SLA de disponibilité	Zones de disponibilité	Frais de facturation minimaux par fichier ²	Durée minimale de stockage
Norme EFS	Données actives nécessitant une latence rapide inférieure à la milliseconde	Moins d'une milliseconde		99,99 % (régional) 99,9 % (une zone)	=>3 (Régional)	Ne s'applique pas	Ne s'applique pas
Accès peu fréquent à l'EFS	Données inactives auxquelles on ne accède que quelques fois par trimestre.	Des dizaines de millisecondes	99,999999 999 % (11 9)		1 (une zone)	128 KIB	Ne s'applique pas
Archive EFS	Données inactives consultées quelques fois par an ou moins	Des dizaines de millisecondes		99,9 % (régional)	=>3 (Régional)	128 KIB	90 jours

¹ Étant donné que les systèmes de fichiers One Zone stockent les données dans une seule zone de AWS disponibilité, les données stockées dans ces types de systèmes de fichiers peuvent être perdues en cas de sinistre ou de toute autre défaillance affectant toutes les copies des données au sein de la zone de disponibilité, ou en cas de destruction de la zone de disponibilité.

² Les politiques de cycle de vie mises à jour le 26 novembre 2023 ou après cette date permettront de classer les fichiers dont la taille est inférieure à 128 Ko dans la classe IA. Pour plus d'informations sur la façon dont Amazon EFS mesure et facture les fichiers individuels et les métadonnées, consultez [Comment Amazon EFS indique les tailles des systèmes de fichiers et des objets](#).

Facturation par classe de stockage

Vous êtes facturé pour le volume de données dans chaque classe de stockage. Des frais d'accès aux données vous sont également facturés lorsque des fichiers stockés dans IA ou Archive sont lus, ou pour les données qui passent d'une classe de stockage à l'autre à l'aide de la gestion du cycle de vie. La facture AWS affiche la capacité de chaque classe de stockage et l'accès mesuré pour la classe de stockage IA. Pour en savoir plus, consultez la page relative à la [Tarification Amazon EFS](#).

En outre, les classes de stockage Infrequent Access (IA) et Archive sont soumises à des frais de facturation minimaux de 128 KiB par fichier. Support pour les fichiers inférieurs à 128 KiB uniquement pour les politiques de cycle de vie mises à jour le 26 novembre 2023 à 12 h 00 (heure du Pacifique) ou après cette date. Pour plus d'informations sur la façon dont Amazon EFS mesure et facture les fichiers individuels et les métadonnées, consultez [Comment Amazon EFS indique les tailles des systèmes de fichiers et des objets](#).

D'autres considérations relatives à la facturation s'appliquent en fonction du mode de débit.

- Pour les systèmes de fichiers utilisant le débit élastique, le montant mensuel total de métadonnées et de données transférées pour vos systèmes de fichiers vous est facturé, indépendamment des frais de stockage.
- Pour les systèmes de fichiers utilisant le mode Débit alloué, vous êtes facturé pour le débit alloué dépassant celui qui vous est fourni en fonction de la quantité de données stockées dans la classe de stockage Standard.
- Pour les systèmes de fichiers utilisant le débit en rafales, le débit autorisé est déterminé en fonction de la quantité de données stockées dans la classe de stockage Standard uniquement.

Pour plus d'informations sur les modes de débit EFS, consultez [Modes de débit](#).

Note

Vous n'avez pas à payer de frais d'accès aux données lorsque vous les utilisez AWS Backup pour sauvegarder des systèmes de fichiers EFS compatibles avec la gestion du cycle de vie. Pour en savoir plus sur AWS Backup Amazon EFS, consultez [Sauvegarde des systèmes de fichiers EFS](#).

Gestion des cycles de vie

Pour gérer vos systèmes de fichiers afin qu'ils soient stockés de manière rentable tout au long de leur cycle de vie, utilisez la gestion du cycle de vie. La gestion du cycle de vie permet de transférer automatiquement les données entre les classes de stockage conformément à la configuration du cycle de vie définie pour le système de fichiers. La configuration du cycle de vie est un ensemble de politiques de cycle de vie qui définissent le moment où il convient de transférer les données du système de fichiers vers une autre classe de stockage. Pour de plus amples informations, veuillez consulter [Gestion du cycle de vie du stockage](#).

Réplication

Vous pouvez créer une réplique de votre système de fichiers Amazon EFS comme vous le souhaitez à l'aide Région AWS de la réplication. La réplication réplique automatiquement et de manière transparente les données et les métadonnées de votre système de fichiers EFS vers un nouveau système de fichiers EFS de destination créé dans le système de votre Région AWS choix. EFS synchronise automatiquement les systèmes de fichiers source et de destination. La réplication est continue et conçue pour fournir un objectif de point de reprise (RPO) et un objectif de délai de reprise (RTO) de quelques minutes. Ces fonctionnalités vous aident à atteindre vos objectifs de conformité et de continuité des activités. Pour de plus amples informations, veuillez consulter [Réplication de systèmes de fichiers EFS](#).

Commencer à utiliser Amazon EFS

Si vous utilisez Amazon Elastic File System (Amazon EFS) pour la première fois, suivez les étapes ci-dessous pour démarrer avec votre premier système de fichiers EFS.

1. [Passez en revue les conditions préalables pour démarrer](#)
2. [Créez votre système de fichiers EFS et lancez votre EC2 instance](#)
3. [Transférez des fichiers vers votre système de fichiers EFS à l'aide de AWS DataSync](#)
4. [Nettoyez les ressources et protégez votre AWS compte](#)

Prérequis

Avant de terminer les étapes de mise en route, assurez-vous de remplir les conditions suivantes :

- Vous êtes familiarisé avec Amazon EC2 et vous êtes habitué au lancement d' EC2 instances. Vous avez besoin d'un Compte AWS, d'un utilisateur disposant d'un accès administratif, d'une paire de clés et d'un groupe de sécurité. Pour plus d'informations, consultez la section [Commencer avec Amazon EC2](#) dans le guide de EC2 l'utilisateur Amazon.
- Vos ressources Amazon Virtual Private Cloud (Amazon VPC) et EFS sont toutes identiques Région AWS et vous disposez d'un VPC par défaut dans la région. EC2 Si vous n'avez pas de VPC par défaut ou si vous souhaitez monter votre système de fichiers à partir d'un nouveau VPC avec des groupes de sécurité nouveaux ou existants, consultez. [Utilisation de groupes de sécurité VPC](#)
- Vous n'avez pas Modifié la règle d'accès entrante par défaut pour le groupe de sécurité par défaut.

Vous pouvez également effectuer un exercice de démarrage similaire en utilisant les commandes AWS Command Line Interface (AWS CLI) pour effectuer les appels d'API EFS. Pour de plus amples informations, veuillez consulter [Tutoriel : créer un système de fichiers EFS et le monter sur une EC2 instance à l'aide du AWS CLI](#).

Créez votre système de fichiers EFS et lancez votre EC2 instance

Après avoir vérifié que vous disposez des conditions requises pour cet exercice de démarrage, vous pouvez créer votre système de fichiers EFS et lancer votre EC2 instance. Le moyen le plus rapide de réaliser toutes les étapes nécessaires pour démarrer avec votre premier système de fichiers EFS consiste à utiliser le EC2 nouvel assistant de lancement lors du lancement de l'instance.

 Note

Vous ne pouvez pas utiliser Amazon EFS avec des instances basées sur Microsoft Windows EC2 .

Pour créer votre système de fichiers EFS et lancer votre EC2 instance à l'aide de l'assistant de EC2 lancement

Pour obtenir des instructions sur la création et le montage de votre système de fichiers EFS lors de la création d'un lancement d' EC2 instance, consultez la section [Utiliser Amazon EFS avec Amazon EC2](#) dans le guide de EC2 l'utilisateur Amazon.

Voici les étapes que vous allez effectuer lors de la création d'un système de fichiers EFS lors du lancement de l'instance.

1. Créez une EC2 instance exécutée sur un système d'exploitation Linux à l'aide de la paire de clés et des paramètres réseau de votre choix.
2. Créez un système de fichiers EFS partagé doté des paramètres recommandés et monté automatiquement sur l' EC2 instance.
3. Lancez l' EC2 instance afin que le système de fichiers EFS soit facilement disponible pour les transferts de fichiers.

Dans la console Amazon EFS, vous pouvez également créer des systèmes de fichiers avec des paramètres recommandés ou des paramètres personnalisés. Vous pouvez également utiliser la AWS CLI et l'API pour créer des systèmes de fichiers. Pour plus d'informations sur toutes les options de création d'un système de fichiers, consultez [Création de systèmes de fichiers EFS](#).

Transférez des fichiers vers votre système de fichiers EFS à l'aide de AWS DataSync

Après avoir créé un système de fichiers EFS, vous pouvez y transférer des fichiers à partir d'un système de fichiers existant en utilisant AWS DataSync. DataSync est un service de transfert de données qui simplifie, automatise et accélère le déplacement et la réplication des données entre les systèmes de stockage sur site et les services AWS de stockage via Internet ou. AWS Direct Connect DataSync peut transférer les données de vos fichiers, ainsi que les métadonnées du système de fichiers telles que la propriété, les horodatages et les autorisations d'accès.

Pour plus d'informations sur DataSync, consultez [AWS DataSync](#).

Prérequis

Avant de transférer des fichiers vers le système de fichiers EFS, assurez-vous de disposer des éléments suivants :

- Un système de fichiers NFS source à partir duquel vous pouvez transférer des fichiers. Ce système source doit être accessible via NFS version 3, 4 ou 4.1. Les exemples de systèmes de fichiers incluent ceux situés dans un centre de données sur site, les systèmes de fichiers autogérés dans le cloud et les systèmes de fichiers EFS.
- Vous êtes configuré pour utiliser DataSync. Pour en savoir plus, consultez la section [Mise en route AWS DataSync](#) dans le guide de AWS DataSync l'utilisateur.

Pour transférer des fichiers vers votre système de fichiers EFS à l'aide de AWS DataSync

Pour obtenir des instructions sur le transfert DataSync de fichiers vers un système de fichiers EFS, reportez-vous à la section [Transfert de vos données AWS DataSync](#) dans le guide de AWS DataSync l'utilisateur.

Voici les étapes que vous allez effectuer lors du transfert de fichiers vers le système de fichiers EFS à l'aide de DataSync.

1. Connectez-vous à votre EC2 instance. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Téléchargez, déployez et activez un agent dans votre environnement.
3. Créez et configurez un emplacement source et de destination.
4. Créez et configurez une tâche.
5. Exécutez la tâche pour transférer les fichiers depuis la source vers la destination.

Nettoyez les ressources et protégez votre AWS compte

Lorsque vous aurez terminé cet exercice de mise en route, effectuez les étapes suivantes pour nettoyer vos ressources et protéger vos Compte AWS.

Pour nettoyer les ressources et protéger votre compte

1. Connectez-vous à votre EC2 instance. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Démontez le système de fichiers EFS à l'aide de la commande suivante.

```
$ sudo umount efs
```

3. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
4. Supprimez le système de fichiers EFS que vous avez créé lors de la première étape de l'exercice de démarrage.
 - a. Choisissez le système de fichiers &EFS;. que vous souhaitez supprimer dans la liste des systèmes de fichiers.
 - b. Dans Actions, choisissez Supprimer le système de fichiers.
 - c. Dans la boîte de dialogue Supprimer définitivement le système de fichiers, saisissez l'ID du système de fichiers EFS que vous voulez supprimer, puis sélectionnez Supprimer le système de fichiers.
5. Mettez fin à l' EC2 instance que vous avez lancée pour cet exercice de démarrage. Pour obtenir des instructions, consultez la section [Résiliation d' EC2instances Amazon](#) dans le guide de AWS IAM Identity Center l'utilisateur.
6. Si vous avez créé un groupe de sécurité pour cet exercice de démarrage, supprimez-le. Pour obtenir des instructions, voir [Supprimer un groupe de sécurité](#) dans le guide de AWS IAM Identity Center l'utilisateur.

Warning

Ne supprimez pas le groupe de sécurité par défaut pour votre VPC.

Installation du client Amazon EFS

Nous vous recommandons d'installer le client Amazon EFS (`amazon-efs-utils`), un ensemble d'outils open source pour Amazon EFS. Le client Amazon EFS inclut un assistant de montage, un programme qui permet de simplifier le montage des systèmes de fichiers EFS. Le client permet également d'utiliser Amazon CloudWatch pour surveiller l'état de montage d'un système de fichiers EFS, et il inclut des outils qui facilitent le chiffrement des données en transit pour les systèmes de fichiers Amazon EFS.

Vous pouvez installer manuellement le client Amazon EFS sur les instances Amazon EC2 (EC2) exécutant des [distributions prises en charge](#). Pour certains systèmes d'exploitation pris en charge, vous pouvez également configurer AWS Systems Manager pour installer ou mettre à jour automatiquement le package. Pour obtenir la liste des distributions que vous pouvez utiliser AWS Systems Manager, consultez [Systèmes d'exploitation pris en charge par Systems Manager](#).

Important

Nous vous recommandons de toujours utiliser la version la plus récente de `amazon-efs-utils` afin de garantir l'accès à toutes ses fonctionnalités. Par exemple, le montage avec des IPv6 adresses est pris en charge dans les versions 2.3 ou ultérieures, mais pas dans les versions antérieures.

Rubriques

- [Dépendances pour les outils EFS](#)
- [Distributions prises en charge :](#)
- [Installation manuelle du client Amazon EFS](#)
- [Installation ou mise à jour automatique du client Amazon EFS à l'aide de AWS Systems Manager](#)
- [Installation et mise à niveau botocore](#)
- [Mise à niveau d'stunnel](#)
- [Activation du mode FIPS](#)

Dépendances pour les outils EFS

Les dépendances suivantes existent pour `amazon-efs-utils` et sont installées lors de l'installation du package `amazon-efs-utils` :

- Client NFS
 - `nfs-utils` pour les distributions RHEL, CentOS, Amazon Linux et Fedora
 - `nfs-common` pour les distributions Debian et Ubuntu
- Relais réseau (package `stunnel`, version 4.56 ou suivante)
- Python (version 3.4 ou suivante)
- OpenSSL 1.0.2 ou version plus récente

Note

Par défaut, lorsque vous utilisez l'assistant de montage EFS avec Transport Layer Security (TLS), l'assistant de montage applique la vérification du nom d'hôte du certificat. L'assistant de montage EFS utilise le `stunnel` programme pour ses fonctionnalités TLS. Certaines versions de Linux n'incluent pas une version de `stunnel` prenant en charge ces fonctionnalités TLS par défaut. Lorsque vous utilisez l'une de ces versions de Linux, le montage d'un système de fichiers EFS à l'aide du protocole TLS échoue.

Après avoir installé le `amazon-efs-utils` package, mettez à niveau `Stunnel`. Consultez [Mise à niveau d'`stunnel`](#).

Vous pouvez l'utiliser AWS Systems Manager pour gérer les clients Amazon EFS et automatiser les tâches requises pour installer ou mettre à jour le `amazon-efs-utils` package sur vos EC2 instances. Pour de plus amples informations, veuillez consulter [Installation ou mise à jour automatique du client Amazon EFS à l'aide de AWS Systems Manager](#).

Pour tout problème lié au chiffrement, consultez [Résolution des problèmes de chiffrement](#).

Distributions prises en charge :

Le client Amazon EFS a été vérifié par rapport aux distributions Linux et Mac suivantes :

Distribution	Type de package	Système init
Amazon Linux 2023 (AL2023)	rpm	systemd
Amazon Linux (2AL2)	rpm	systemd
CentOS 8	rpm	systemd
Amazon Linux (1AL1) 09/2017	rpm	upstart
 Note AL1 L'AMI a atteint son niveau le 31 end-of-life décembre 2023 et n'est pas pris en charge pour les amazon-efs-utils packages publiés en avril 2024 ou ultérieurement (version 2.0 et ultérieure).		
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
Oracle 8	rpm	systemd
Red Hat Enterprise Linux (RHEL) 7, 8, 9	rpm	systemd

Distribution	Type de package	Système init
SUSE Linux Enterprise Server (SLES) 12, 15	rpm	systemd
Ubuntu 16,04 LTS, 18,04 LTS, 20,04 LTS, 22,04 LTS	deb	systemd

Pour une liste complète des distributions prises en charge par rapport auxquelles le package a été vérifié, consultez le site `amazon-efs-utils` [README](#) sur Github.

Installation manuelle du client Amazon EFS

Vous pouvez installer manuellement le client Amazon EFS sur les instances Amazon EC2 (EC2) Linux et sur les instances EC2 Mac exécutant macOS Big Sur, macOS Monterey et macOS Ventura. Pour obtenir la liste des distributions compatibles avec le client Amazon EFS, consultez [Distributions prises en charge](#) :

Les procédures d'installation des systèmes d'exploitation pris en charge sont décrites dans les sections suivantes.

Rubriques

- [Installation du client Amazon EFS sur les instances Amazon EC2 Linux](#)
- [Pour installer le client Amazon EFS sur d'autres distributions Linux](#)
- [Installation du client Amazon EFS sur des instances EC2 Mac exécutant macOS Big Sur, macOS Monterey ou macOS Ventura](#)

Installation du client Amazon EFS sur les instances Amazon EC2 Linux

Le `amazon-efs-utils` package à installer sur les instances Amazon EC2 Linux à partir des emplacements suivants :

- Les référentiels de packages Amazon Machine Images (AMI) pour Amazon Linux. Les instructions suivantes concernent l'installation du `amazon-efs-utils` package à partir des référentiels de packages de l'AMI.

- Le AWS [efs-utils](#) GitHub référentiel. Pour plus d'informations sur l'installation amazon-efs-utils du package depuis GitHub, consultez [Pour installer le client Amazon EFS sur d'autres distributions Linux](#).

Note

- Si vous utilisez AWS Direct Connect, vous trouverez les instructions d'installation dans [Prérequis](#).
- L'AMI Amazon Linux 1 (AL1) a atteint sa limite end-of-life le 31 décembre 2023 et n'est pas prise en charge pour les amazon-efs-utils packages publiés en avril 2024 et versions ultérieures (versions 2.0 et ultérieures). Nous vous recommandons de mettre à niveau les applications vers Amazon Linux 2023 (AL2023), qui inclut un support à long terme jusqu'en 2028.

Pour installer le **amazon-efs-utils** package depuis le référentiel de packages AMI sur les instances EC2 Linux

1. Assurez-vous d'avoir créé une EC2 instance AL2 023 ou Amazon Linux (2AL2). Pour plus d'informations sur la procédure à suivre, consultez [Étape 1 : Lancer une instance](#).
2. Accédez au terminal pour votre instance via Secure Shell (SSH) et connectez-vous avec le nom d'utilisateur approprié. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
3. Pour installer le package amazon-efs-utils, exécutez la commande suivante :

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

Pour installer le client Amazon EFS sur d'autres distributions Linux

Si vous ne souhaitez pas obtenir le amazon-efs-utils package depuis les référentiels de packages de l'AMI Amazon Linux, il est également disponible sur GitHub.

Une fois que vous avez cloné le package, vous pouvez générer et installer amazon-efs-utils en utilisant l'une des méthodes suivantes, selon le type de package pris en charge par votre distribution Linux :

- RPM — Ce type de package est pris en charge par AL2 023, Amazon Linux 2, Red Hat Linux, CentOS, etc.
- DEB - Ce type de package est pris en charge par Ubuntu, Debian et d'autres systèmes similaires.

Pour obtenir des instructions sur l'installation `amazon-efs-utils` du package pour d'autres distributions Linux, voir [Sur les autres distributions Linux](#) dans le `amazon-efs-utils` fichier README sur Github.

Installation du client Amazon EFS sur des instances EC2 Mac exécutant macOS Big Sur, macOS Monterey ou macOS Ventura

Le `amazon-efs-utils` package peut être installé sur des instances EC2 Mac exécutant macOS Big Sur, macOS Monterey ou macOS Ventura.

Pour obtenir des instructions sur l'installation du `amazon-efs-utils` package sur des instances Mac, consultez la section [Sur macOS Big Sur, macOS Monterey, macOS Sonoma et macOS Ventura](#) dans le `amazon-efs-utils` fichier README sur Github.

Étapes suivantes

Après les installations `amazon-efs-utils` sur votre EC2 instance, passez aux étapes suivantes pour monter votre système de fichiers :

- [Installez-le botocore](#) afin de pouvoir utiliser Amazon CloudWatch pour surveiller l'état de montage de votre système de fichiers.
- [Passez à la dernière version de stunnel](#) pour activer le chiffrement des données en transit.
- [Monter votre système de fichiers](#) à l'aide de l'assistant de montage EFS

Installation ou mise à jour automatique du client Amazon EFS à l'aide de AWS Systems Manager

Vous pouvez l'utiliser AWS Systems Manager pour simplifier la gestion du client Amazon EFS (`amazon-efs-utils`). AWS Systems Manager est un AWS service que vous pouvez utiliser pour visualiser et contrôler votre infrastructure AWS. AWS Systems Manager Vous pouvez ainsi automatiser les tâches nécessaires à l'installation ou à la mise à jour `amazon-efs-utils` du

package sur vos instances Amazon EC2 (EC2). Les fonctionnalités de Systems Manager, telles que Distributor et State Manager, vous permettent d'automatiser les processus suivants :

- Maintien du contrôle de version sur le client Amazon EFS.
- Stockage centralisé et distribution systématique du client Amazon EFS sur vos EC2 instances Amazon.
- Automatisez le processus de maintien de vos EC2 instances dans un état défini.

Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Systems Manager](#).

Ce que fait le client Amazon EFS lors de l'installation

Vous utilisez le client Amazon EFS pour automatiser la surveillance des CloudWatch journaux Amazon pour connaître l'état de montage du système de fichiers et effectuer la mise `stunnel` à niveau vers la dernière version pour certaines distributions Linux. Lorsque vous installez le client Amazon EFS sur vos EC2 instances Amazon à l'aide de Systems Manager, celui-ci effectue les actions suivantes :

- Installe le package `botocore` en suivant les mêmes étapes que celles décrites dans [Installation et mise à niveau botocore](#). Le client Amazon EFS utilise `botocore` pour surveiller l'état de montage du système de fichiers EFS.
- Permet de surveiller l'état de montage du système de fichiers EFS dans les CloudWatch journaux par le biais d'une mise à jour `efs-utils.conf`. Pour de plus amples informations, veuillez consulter [Surveillance des réussites et des échecs des tentatives de montage](#).
- Pour les EC2 instances en cours d'exécution RHEL7 ou CentOS7, le client Amazon EFS est automatiquement mis à niveau `stunnel` comme décrit dans [Mise à niveau d'stunnel](#). La mise à niveau de `stunnel` est nécessaire pour monter correctement un système de fichiers EFS avec le protocole TLS, et la `stunnel` version est livrée avec le client Amazon EFS RHEL7 mais CentOS7 ne le prend pas en charge (`amazon-efs-utils`).

Systèmes d'exploitation pris en charge par Systems Manager

Vos EC2 instances doivent exécuter l'un des systèmes d'exploitation suivants pour pouvoir être utilisées pour mettre AWS Systems Manager à jour ou installer automatiquement le client Amazon EFS.

Plateforme	Version de plateforme	Architecture
Amazon Linux 2023 (AL2023)	AL2023	x86_64, arm64 (processeurs Graviton2 ou ultérieurs)
Amazon Linux (2AL2)	2.0	x86_64, arm64 (Amazon Linux 2, types d'instances A1)
Amazon Linux (1AL1)	2017,09, 2018,03	x86_64
 Note L'AMI Amazon Linux 1 (AL1) a atteint son niveau le 31 end-of-life décembre 2023 et n'est pas prise en charge pour les amazon-efs-utils packages publiés en avril 2024 et versions ultérieures (versions 2.0 et ultérieures). Nous vous recommandons de mettre à niveau les applications vers Amazon Linux 2023 (AL2023), qui inclut un support à long terme jusqu'en 2028.		
CentOS	7, 8	x86_64
Red Hat Enterprise Linux (RHEL)	7, 8	x86_64, arm64 (RHEL 7.6 et versions ultérieures, types d'instances A1)

Plateforme	Version de plateforme	Architecture
SUSE Linux Enterprise Server (SLES)	12, 15	x86_64
Ubuntu Server	16,04, 18,04, 20,04	x86_64, arm64 (Ubuntu Server 16 et versions ultérieures, types d'instances A1)

Configuration AWS Systems Manager pour installer le client EFS

Deux configurations uniques sont nécessaires pour configurer Systems Manager afin d'installer ou de mettre à jour automatiquement le `amazon-efs-utils` package.

1. Configurez un profil d'instance AWS Identity and Access Management (IAM) avec les autorisations requises.
2. Configurez une association (y compris le calendrier) utilisée pour l'installation ou les mises à jour par le State Manager.

Étape 1 : Configurez un profil d'instance (IAM) avec les autorisations requises.

Par défaut, AWS Systems Manager n'est pas autorisé à gérer vos clients Amazon EFS ni à installer ou à mettre à jour le `amazon-efs-utils` package. Vous devez accorder l'accès au gestionnaire de systèmes en utilisant un profil d'instance (IAM) AWS Identity and Access Management . Un profil d'instance est un conteneur qui transmet les informations de rôle IAM à une instance Amazon EC2 (EC2) lors du lancement.

Utilisez la politique d'autorisation `AmazonElasticFileSystemsUtils` AWS gérée pour attribuer les autorisations appropriées aux rôles. Vous pouvez créer un rôle pour votre profil d'instance ou ajouter la politique d'autorisation `AmazonElasticFileSystemsUtils` à un rôle existant. Vous devez ensuite utiliser ce profil d'instance pour lancer vos EC2 instances. Pour plus d'informations, consultez la section [Configurer des autorisations d'instance requises pour Systems Manager](#).

Étape 2 : Configuration d'une association utilisée par State Manager

Le `amazon-efs-utils` package est inclus avec le distributeur et est prêt à être déployé sur des EC2 instances gérées. Pour voir la dernière version disponible pour l'installation, vous pouvez utiliser

la AWS Systems Manager console ou votre outil de ligne de commande préféré. `amazon-efs-utils` Pour accéder à Distributor, ouvrez le <https://console.aws.amazon.com/systems-manager/> et choisissez Distributor dans le volet de navigation de gauche. Localisez Amazon EFSUtils dans la section Owned by Amazon. Choisissez Amazon EFSUtils pour voir les détails du colis. Pour plus d'informations, consultez [Voir package](#).

À l'aide de State Manager, vous pouvez installer ou mettre à jour le `amazon-efs-utils` package sur vos EC2 instances gérées immédiatement ou selon un calendrier. En outre, vous pouvez vous assurer qu'`amazon-efs-utils` est automatiquement installé sur les nouvelles EC2 instances. Pour plus d'informations sur l'installation ou la mise à jour de packages à l'aide de Distributor et State Manager, consultez la section [Travailler avec le distributeur](#).

Pour installer ou mettre à jour automatiquement le `amazon-efs-utils` package sur les instances à l'aide de la console Systems Manager, consultez la section [Planification de l'installation ou de la mise à jour d'un package \(console\)](#). Cela vous invite à créer une association pour State Manager, qui définit l'état que vous souhaitez appliquer à un ensemble d'instances. Utilisez les entrées suivantes lors de la création de votre association :

- Pour les paramètres, choisissez Action > Installation et type d'installation > Mise à jour sur place.
- Pour les cibles, le paramètre recommandé est Choisir toutes les instances pour enregistrer toutes les EC2 instances nouvelles et existantes en tant que cibles afin d'installer ou de mettre à jour automatiquement Amazon EFSUtils. Vous pouvez également spécifier des balises d'instance, sélectionner des instances manuellement ou choisir un groupe de ressources pour appliquer l'association à un sous-ensemble d'instances. Si vous spécifiez des balises d'instance, vous devez lancer vos EC2 instances avec ces balises pour permettre à AWS Systems Manager d'installer ou de mettre à jour automatiquement le client Amazon EFS.
- Pour Spécifier le calendrier, le paramètre recommandé pour Amazon EFSUtils est tous les 30 jours. Vous pouvez utiliser les contrôles pour créer un cron ou un calendrier pour l'association.

À utiliser AWS Systems Manager pour monter des systèmes de fichiers EFS sur plusieurs EC2 instances, voir [Montage d'EFS sur plusieurs EC2 instances](#).

Installation et mise à niveau **botocore**

Le client Amazon EFS est utilisé `botocore` pour interagir avec d'autres AWS services. Cela est nécessaire si vous souhaitez contrôler le succès ou l'échec des tentatives de montage de vos

systèmes de fichiers EFS dans CloudWatch Logs. Pour de plus amples informations, veuillez consulter [Surveillance des réussites et des échecs des tentatives de montage](#).

Pour obtenir des instructions sur l'installation et la mise à niveau de `botocore`, consultez la section [Installation de `botocore`](#) dans le fichier README sur Github.

Mise à niveau d'`stunnel`

Le chiffrement des données en transit avec l'assistant de montage EFS nécessite la OpenSSL version 1.0.2 ou une version ultérieure, `stunnel` dont une version prend en charge à la fois le protocole OCSP (Online Certificate Status Protocol) et la vérification du nom d'hôte du certificat. L'assistant de montage EFS utilise le `stunnel` programme pour ses fonctionnalités TLS. Notez que certaines versions de Linux n'incluent pas une version de `stunnel` prenant en charge ces fonctionnalités TLS par défaut. Lorsque vous utilisez l'une de ces distributions Linux, le montage d'un système de fichiers EFS à l'aide du protocole TLS échoue.

Après avoir installé l'assistant de montage EFS, vous pouvez mettre à niveau la version de `Stunnel` de votre système en suivant les instructions suivantes.

Pour effectuer une mise à niveau **`stunnel`** sur Amazon Linux, Amazon Linux 2 et d'autres distributions Linux prises en charge (à l'exception de [SLES 12](#))

1. Dans un navigateur Web, accédez à la page des `stunnel` téléchargements <https://stunnel.org/downloads.html>.
2. Localisez la dernière version `stunnel` disponible dans le format `tar.gz`. Notez le nom du fichier, car vous en aurez besoin dans la procédure suivante.
3. Ouvrez un terminal sur votre client Linux et exécutez les commandes suivantes dans l'ordre.

- a. Pour RPM :

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

Pour DEB :

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

- b. *latest-stunnel-version* Remplacez-le par le nom du fichier que vous avez noté précédemment à l'étape 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. Le stunnel package actuel est installé dans `bin/stunnel`. Pour que la nouvelle version puisse être installée, supprimez ce répertoire à l'aide de la commande suivante :

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

h. Installer la dernière version

```
sudo make install
```

i. Créer un lien symbolique

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

Pour mettre à jour Stunnel sur macOS

- Ouvrez un terminal sur votre instance EC2 Mac et exécutez la commande suivante pour effectuer la mise à niveau vers la dernière version de Stunnel.

```
brew upgrade stunnel
```

Mise à niveau de Stunnel pour SLES 12

- Exécutez les commandes suivantes et suivez les instructions du gestionnaire de packages zypper pour mettre à niveau Stunnel sur votre instance de calcul en cours d'exécution. 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
```

Une fois que vous avez installé une version de stunnel avec les fonctionnalités requises, vous pouvez monter votre système de fichiers à l'aide de TLS en utilisant les paramètres recommandés pour Amazon EFS.

Résolution des problèmes liés à l'installation de Stunnel

Si vous ne parvenez pas à installer Stunnel, essayez de désactiver la vérification du nom d'hôte du certificat. En outre, offrez le niveau de sécurité le plus élevé possible en activant le protocole OCSP (Online Certificate Status Protocol).

Rubriques

- [Désactivation de la vérification du nom d'hôte du certificat](#)
- [Activation du protocole de vérification en ligne de certificat \(OCSP\)](#)

Désactivation de la vérification du nom d'hôte du certificat

Si vous ne pouvez pas installer les dépendances requises, vous pouvez désactiver la vérification du nom d'hôte du certificat dans la configuration d'assistant de montage Amazon EFS. Nous vous déconseillons de désactiver cette fonction dans les environnements de production. Pour désactiver la vérification du nom d'hôte du certificat, procédez comme suit :

1. Dans l'éditeur de texte de votre choix, ouvrez le fichier `/etc/amazon/efs/efs-utils.conf`.
2. Définissez la valeur de `stunnel_check_cert_hostname` sur `false`.
3. Enregistrez les modifications du fichier, puis fermez-le.

Pour plus d'informations sur l'utilisation du chiffrement des données en transit, consultez [Montage des systèmes de fichiers EFS](#).

Activation du protocole de vérification en ligne de certificat (OCSP)

Afin de maximiser la disponibilité du système de fichiers si l'autorité de certification n'est pas accessible depuis votre VPC, le protocole OCSP (Online Certificate Status Protocol) n'est pas activé par défaut lorsque vous choisissez de chiffrer les données en transit. Amazon EFS utilise une [autorité de certification \(CA\) Amazon](#) pour émettre et signer ses certificats TLS, et l'autorité de certification demande au client d'utiliser le protocole OCSP pour vérifier les certificats révoqués. Le point de terminaison OCSP doit être accessible via Internet à partir de votre Virtual Private Cloud afin de vérifier le statut d'un certificat. Au sein du service, Amazon EFS surveille en permanence l'état des certificats et émet de nouveaux certificats pour remplacer les certificats révoqués détectés.

Afin de vous assurer de la meilleure sécurité possible, vous pouvez activer OCSP de sorte que vos clients Linux puissent vérifier les certificats révoqués. OCSP protège contre l'utilisation malveillante des certificats révoqués, ce qui est peu probable dans votre VPC. En cas de révocation d'un certificat EFS TLS, Amazon publie un bulletin de sécurité et publie une nouvelle version de l'assistant de montage EFS qui rejette le certificat révoqué.

Pour activer OCSP sur votre client Linux pour toutes les futures connexions TLS à EFS

1. Ouvrez un terminal sur votre client Linux.
2. Dans l'éditeur de texte de votre choix, ouvrez le fichier `/etc/amazon/efs/efs-utils.conf`.
3. Définissez la valeur de `stunnel_check_cert_validity` sur `true`.
4. Enregistrez les modifications du fichier, puis fermez-le.

Pour activer OCSP dans le cadre de la commande **mount**

- Utilisez la commande mount suivante pour activer OCSP lors du montage du système de fichiers.

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

Activation du mode FIPS

Si votre système d'exploitation utilise des points de terminaison FIPS (Federal Information Processing Standards) lors du montage de votre système de fichiers, vous devez activer le mode FIPS dans le

client Amazon EFS. L'activation du mode FIPS implique de modifier le `efs-utils.conf` fichier sur le système d'exploitation.

 Note

Le mode FIPS nécessite que la version installée d'OpenSSL soit compilée avec FIPS. [Pour plus d'informations sur la configuration d'OpenSSL avec FIPS, consultez le fichier README d'OpenSSL FIPS.](#)

Pour activer le mode FIPS dans le client Amazon EFS

1. Accédez au terminal de votre EC2 instance Amazon via Secure Shell (SSH) et connectez-vous avec le nom d'utilisateur approprié. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.
2. Dans l'éditeur de texte de votre choix, ouvrez le fichier `/etc/amazon/efs/efs-utils.conf`.
3. Trouvez la ligne contenant le texte suivant :

```
"fips_mode_enabled = false"
```

4. Modifiez le texte comme suit :

```
"fips_mode_enabled = true"
```

5. Enregistrez vos modifications.

Création et gestion des ressources EFS

Amazon EFS fournit un service de stockage de fichiers élastique et partagé qui est compatible POSIX. Le système de fichiers que vous créez prend en charge l'accès simultané en lecture et en écriture à partir de plusieurs EC2 instances Amazon. Le système de fichiers est également accessible depuis toutes les zones de disponibilité dans Région AWS lesquelles il a été créé.

Vous pouvez monter un système de fichiers Amazon EFS sur des EC2 instances de votre cloud privé virtuel (VPC) basé sur Amazon VPC en utilisant le protocole Network File System versions 4.0 et 4.1 (). NFSv4 Pour de plus amples informations, veuillez consulter [Comment fonctionne Amazon EFS](#).

Par exemple, supposons qu'une ou plusieurs EC2 instances soient lancées dans votre VPC. A présent, vous voulez créer et utiliser un système de fichiers sur ces instances. Voici les étapes classiques que vous devez suivre pour utiliser les systèmes de fichiers Amazon EFS dans le VPC :

- Créer un système de fichiers Amazon EFS : lors de la création d'un système de fichiers, nous vous recommandons d'utiliser la balise Nom. La valeur de la balise Nom apparaît dans la console et facilite l'identification du système de fichiers. Vous pouvez également ajouter d'autres balises facultatives au système de fichiers.
- Création de cibles de montage pour le système de fichiers — Pour accéder au système de fichiers de votre VPC et monter le système de fichiers sur votre EC2 instance Amazon, vous devez créer des cibles de montage dans les sous-réseaux VPC.
- Création de groupes de sécurité : des groupes de sécurité doivent être associés à une EC2 instance Amazon et à une cible de montage. Ces groupes de sécurité font office de pare-feu virtuel contrôlant le trafic entre elles. Vous pouvez utiliser le groupe de sécurité que vous avez associé à la cible de montage pour contrôler le trafic entrant vers votre système de fichiers. Pour ce faire, ajoutez une règle entrante au groupe de sécurité cible de montage qui autorise l'accès depuis une EC2 instance spécifique. Vous pouvez ensuite monter le système de fichiers uniquement sur cette EC2 instance.

Rubriques

- [Récapitulatif de l'implémentation](#)
- [Ressource IDs](#)
- [Jeton de création et idempotence](#)
- [Création de systèmes de fichiers EFS](#)

- [Suppression de systèmes de fichiers EFS](#)
- [Création de politiques de système de fichiers](#)
- [Création de points d'accès](#)
- [Supprimer des points d'accès](#)
- [Marquage des ressources EFS](#)
- [Tutoriel : Création de sous-répertoires accessibles en écriture par utilisateur](#)

Récapitulatif de l'implémentation

Dans Amazon EFS, un système de fichiers est la ressource principale. Chaque système de fichiers possède des propriétés telles que l'identifiant, le jeton de création, l'heure de création, la taille du système de fichiers en octets, le nombre de cibles de montage créées pour le système de fichiers et les politiques de cycle de vie du système de fichiers.

Amazon EFS prend également en charge d'autres ressources pour configurer la ressource principale. Celles-ci comprennent des cibles de montage et des points d'accès :

- Cible de montage – Pour accéder à votre système de fichiers, vous devez créer des cibles de montage dans votre VPC. Chaque cible de montage a les propriétés suivantes : ID de la cible de montage, ID du sous-réseau dans lequel elle a été créée, ID du système de fichiers pour lequel elle a été créée, adresse IP à laquelle le système de fichiers peut être monté, groupes de sécurité de VPC et état de la cible de montage. Vous pouvez utiliser l'adresse IP ou le nom DNS dans votre commande mount.

Chaque système de fichiers a un nom DNS utilisant la forme suivante.

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

Vous pouvez spécifier ce nom DNS dans votre commande mount pour monter le système de fichiers Amazon EFS. Supposons que vous créiez un `efs-mount-point` sous-répertoire à partir de votre répertoire de base sur votre EC2 instance ou sur votre serveur local. Ensuite, vous pouvez utiliser la commande mount pour monter le système de fichiers. Par exemple, sur une AMI Amazon Linux, vous pouvez utiliser la commande mount suivante.

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

Pour de plus amples informations, veuillez consulter [Gérer des cibles de Montage](#).

- Points d'accès – Un point d'accès applique un utilisateur, un groupe et un chemin d'accès du système de fichiers pour système d'exploitation à toute demande de système de fichiers effectuée à l'aide du point d'accès. L'utilisateur et le groupe du système d'exploitation du point d'accès remplacent toutes les informations d'identité fournies par le client NFS. Le chemin d'accès du système de fichiers est exposé au client en tant que répertoire racine du point d'accès. Cela garantit que chaque application utilise toujours l'identité correcte du système d'exploitation et le bon répertoire lors de l'accès à des ensembles de données basés sur des fichiers partagés. Les applications utilisant le point d'accès peuvent uniquement accéder aux données dans leur propre répertoire et en dessous. Pour de plus amples informations, veuillez consulter [Utilisation des points d'accès](#).

Les cibles de montage et les balises sont des sous-ressources associées à un système de fichiers. Vous ne pouvez les créer que dans le contexte d'un système de fichiers existant.

Amazon EFS fournit des opérations d'API qui vous permettent de créer et de gérer ces ressources. En plus des opérations de création et de suppression pour chaque ressource, Amazon EFS prend également en charge une opération de description qui vous permet d'extraire des informations de ressource. Vous disposez des options suivantes pour créer et gérer ces ressources :

- Utilisez la console Amazon EFS – Pour un exemple, consultez [Premiers pas](#).
- Utilisez l'interface de ligne de commande (CLI). Pour obtenir un exemple, consultez [Tutoriel : créer un système de fichiers EFS et le monter sur une EC2 instance à l'aide du AWS CLI](#).
- Vous pouvez également gérer ces ressources par programmation comme suit :
 - Utilisez le AWS SDKs — AWS SDKs Simplifiez vos tâches de programmation en encapsulant l'API Amazon EFS sous-jacente. Les clients SDK peuvent également authentifier vos requêtes à l'aide de clés d'accès que vous fournissez. Pour plus d'informations, consultez [Exemples de code et de bibliothèques](#).
 - Appelez l'API Amazon EFS directement depuis votre application : si SDKs pour une raison ou une autre, vous ne pouvez pas l'utiliser, vous pouvez effectuer des appels d'API Amazon EFS directement depuis votre application. Cependant, vous devez écrire le code nécessaire pour

authentifier vos requêtes si vous utilisez cette option. Pour en savoir plus sur l'API Amazon EFS, consultez [API Amazon EFS](#).

Ressource IDs

Amazon EFS attribue des identifiants de ressource uniques (IDs) à toutes les ressources EFS lors de leur création. Toutes les ressources EFS IDs se composent d'un identifiant de ressource et d'une combinaison de chiffres de 0 à 9 et de lettres minuscules de a à f.

Avant octobre 2021, les ressources cibles IDs attribuées au système de fichiers et au montage nouvellement créés utilisaient 8 caractères après le tiret (par exemple, `fs-12345678`). De mai 2021 à octobre 2021, nous avons modifié ces types IDs de ressources pour utiliser 17 caractères après le tiret (par exemple, `fs-1234567890abcdef0`). Selon la date de création de votre compte, il se peut que vous ayez un système de fichiers et que vous montiez des ressources cibles avec des raccourcis IDs, bien que les nouvelles ressources de ce type soient plus longues IDs. L'ID de ressource ne change jamais.

Jeton de création et idempotence

L'idempotence garantit qu'une requête d'API n'est exécutée qu'une seule fois. Avec les demandes idempotentes, si la demande d'origine se termine avec succès, les demandes suivantes n'ont aucun effet supplémentaire. Cela s'avère utile pour empêcher la création de tâches dupliquées lorsque vous interagissez avec l'API Amazon EFS.

L'API Amazon EFS prend en charge l'idempotence avec les jetons de demande du client. Un jeton de demande client est une chaîne unique que vous spécifiez lorsque vous créez une demande de création de tâche.

Un jeton de demande client peut être n'importe quelle chaîne qui comprend jusqu'à 64 caractères ASCII. Si vous réutilisez un jeton de demande client dans la minute qui suit le succès d'une demande, l'API renvoie les détails de la tâche de la demande initiale.

Si vous utilisez la console, elle génère le jeton à votre place. Si vous utilisez le flux Création personnalisée dans la console, le jeton de création généré pour vous a le format suivant :

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

Si vous utilisez Quick Create pour créer un système de fichiers avec les paramètres recommandés par le service, le jeton de création a le format suivant :

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

Création de systèmes de fichiers EFS

Vous pouvez créer un système de fichiers lorsque vous créez une nouvelle instance de EC2 lancement, comme expliqué dans l'[exercice de démarrage](#). Toutefois, vous pouvez également créer des systèmes de fichiers à l'aide de la console Amazon EFS, du AWS Command Line Interface (AWS CLI) ou de l'API Amazon EFS.

Lorsque vous créez le système de fichiers à l'aide de la console Amazon EFS, différentes options s'offrent à vous, selon que vous souhaitez que le système de fichiers utilise les paramètres recommandés ou que vous souhaitiez personnaliser les paramètres.

- Vous pouvez utiliser la création rapide pour créer rapidement un système de fichiers avec les paramètres recommandés suivants.
 - Disponibilité par région
 - Politiques de cycle de vie visant à faire passer le système de fichiers au stockage EFS Infrequent Access (IA) après 30 jours, au stockage des archives EFS après 90 jours, et à ne pas passer au stockage standard EFS
 - Chiffrement des données au repos activé
 - Mode de débit élastique
 - Mode de performance à usage général
 - Les cibles de montage sont configurées dans chaque zone de disponibilité Région AWS dans laquelle le système de fichiers est créé à l'aide d'un fichier disponible IPv4 sur le sous-réseau spécifié
- Vous pouvez utiliser Personnaliser pour créer un système de fichiers avec les paramètres de votre choix.

Pour consulter un tableau répertoriant les paramètres du système de fichiers et les valeurs recommandées, consultez [Options de configuration pour les systèmes de fichiers](#).

Autorisations IAM requises pour créer des systèmes de fichiers

Pour créer des ressources EFS, telles qu'un système de fichiers et des points d'accès, vous devez disposer des autorisations AWS Identity and Access Management (IAM) pour l'opération et la ressource d'API correspondantes.

Créez des utilisateurs IAM et accordez-leur des autorisations pour les actions Amazon EFS avec des stratégies utilisateur. Vous pouvez également utiliser des rôles pour accorder des autorisations sur des comptes. Amazon Elastic File System utilise également un rôle lié au service IAM qui inclut les autorisations requises pour appeler d'autres personnes en votre Services AWS nom. Pour plus d'informations sur la gestion des autorisations relatives aux opérations d'API, consultez [Gestion des identités et des accès pour Amazon EFS](#).

Options de configuration pour les systèmes de fichiers

Les systèmes de fichiers EFS sont configurés avec les paramètres répertoriés dans le tableau suivant.

- Si vous utilisez la création rapide pour créer le système de fichiers, celui-ci est créé avec la valeur recommandée indiquée pour le paramètre.
- Si vous utilisez Personnaliser pour créer un système de fichiers personnalisé, vous pouvez modifier la valeur recommandée pour le paramètre.

Après avoir créé le système de fichiers, vous pouvez personnaliser les paramètres du système de fichiers, à l'exception du type de système de fichiers, du chiffrement et du mode de performance.

Paramètres du système de fichiers EFS

Paramètre	Description
Type de système de fichiers	Recommandé : régional Le type de système de fichiers détermine la disponibilité et la durabilité avec lesquelles un système de fichiers EFS stocke les données dans un Région AWS. • Les systèmes de fichiers régionaux stockent les données et les métadonnées de manière

Paramètre	Description
	redondante dans toutes les zones de disponibilité d'une Région AWS. Vous pouvez aussi créer des cibles de montage dans chaque zone de disponibilité de la Région AWS. Régional offre les niveaux les plus élevés de disponibilité et de durabilité. Les systèmes de fichiers One Zone stockent les données et les métadonnées de manière redondante au sein d'une seule zone de disponibilité. Les systèmes de fichiers One Zone ne peuvent avoir qu'une seule cible de montage. Cette cible de montage doit se trouver dans la même zone de disponibilité que celle dans laquelle le système de fichiers est créé.  Note Les systèmes de fichiers One Zone ne sont disponibles que pour certaines zones de disponibilité. Pour plus d'informations sur les types de systèmes de fichiers, consultez Disponibilité et durabilité des systèmes de fichiers EFS.

Paramètre	Description
Gestion du cycle de vie	Recommandé : transition vers le stockage IA après 30 jours et vers le stockage Archive après 90 jours. Ne passez pas au stockage standard. La gestion du cycle de vie utilise des politiques de cycle de vie pour déplacer automatiquement les fichiers vers et hors de la classe de stockage à accès peu fréquent (IA) à moindre coût en fonction des modèles d'accès. Lorsque vous créez un système de fichiers à l'aide du AWS Management Console, la politique de cycle de vie du système de fichiers est configurée avec les paramètres par défaut suivants : • Transition vers IA définie sur 30 jours depuis le dernier accès. • Le délai de transition vers l'archivage est fixé à 90 jours depuis le dernier accès. • Transition vers Standard définie sur Aucun. Lorsque vous créez un système de fichiers à l'aide de l' AWS CLI API Amazon EFS ou AWS SDKs, vous ne pouvez pas définir de politique de cycle de vie en même temps. Il faut attendre que le système de fichiers soit créé, puis utiliser l'opération d'API PutLifecycleConfiguration pour mettre à jour la politique de cycle de vie. Pour plus d'informations sur la gestion du cycle de vie, consultez Gestion du cycle de vie du stockage.

Paramètre	Description
Chiffrement au repos	Recommandé : activé Amazon EFS utilise votre AWS Key Management Service (AWS KMS) clé de service EFS (aws/elasticfilesystem) pour chiffrer les données au repos par défaut. Avec le chiffrement, toutes les données et métadonnées qui y sont stockées sont cryptées. Une fois que vous avez créé un système de fichiers EFS, vous ne pouvez pas modifier ses paramètres de chiffrement. Cela signifie que vous ne pouvez pas modifier un système de fichiers non chiffré pour le chiffrer. À la place, vous devez créer un système de fichiers chiffré. Pour plus d'informations sur le chiffrement Amazon EFS, consultez Chiffrement des données dans Amazon EFS.

Paramètre	Description
Mode débit	Recommandé : élastique Vous pouvez choisir l'un des modes de débit suivants : • Élastique : fournit un débit qui augmente ou diminue automatiquement en temps réel, afin de répondre aux besoins de performance de votre charge de travail. • Provisionné : spécifiez le débit souhaité, indépendamment de la taille du système de fichiers. • En rafale : il fournit un débit qui s'adapte à la quantité de données dans le stockage Standard.  Note Des frais supplémentaires sont associés à l'utilisation des débits Élastique et Provisionné. Pour de plus amples informations, consultez la tarification Amazon EFS. Pour plus d'informations sur les modes de débit, consultez Modes de débit.

Paramètre	Description
Mode performance	Recommandé : Usage général Le mode de performance General Purpose présente la latence par opération la plus faible et est recommandé pour tous les systèmes de fichiers. Les E/S maximales sont un type de performance de génération précédente conçu pour les charges de travail hautement parallélisées qui peuvent tolérer des latences supérieures à celles du mode General Purpose. Le I/O mode Max n'est pas pris en charge pour les systèmes de fichiers One Zone ou les systèmes de fichiers qui utilisent le débit élastique.  Important En raison des latences par opération plus élevées avec Max E/S, nous recommandons d'utiliser le mode de performance Usage général pour tous les systèmes de fichiers. Pour de plus amples informations, veuillez consulter Modes de performances.

Paramètre	Description
Accès réseau	Recommandé : cible de montage créée dans chaque zone de disponibilité dans laquelle le système de fichiers est disponible Les paramètres de la cible de montage sont les suivants : • VPC — Vous pouvez créer des cibles de montage pour le système de fichiers dans un VPC à la fois. Par défaut, le sous-réseau par défaut de l' EC2 instance est sélectionné. Modifiez le VPC si vous devez accéder au système de fichiers depuis un autre VPC. Si vous souhaitez modifier le VPC après avoir créé le système de fichiers d'après, vous devez d'abord supprimer les cibles de montage du VPC actuel. Pour de plus amples informations, veuillez consulter Modification du VPC cible de montage. • Zone de disponibilité et ID de sous-réseau : vous pouvez modifier la zone de disponibilité ou le sous-réseau de la cible de montage. • Type d'adresse IP — Par défaut, Amazon EFS utilise une IPv4 adresse à laquelle créer la cible de montage. Vous pouvez également choisir de IPv6 ne prendre en charge que les IPv6 adresses ou de Dual-Stack pour prendre en charge à la fois les IPv6 adresses IPv4 et les adresses.  Note Le type d'adresse IP doit correspondre au type IP du sous-réseau. En

Paramètre	Description
	outre, le type d'adresse IP remplace l'attribut d'adressage IP de votre sous-réseau. Par exemple, si le type d'adresse IP est IPv4 -only et que l'attribut d' IPv6 adressage est activé pour votre sous-réseau, les interfaces réseau créées dans le sous-réseau reçoivent une IPv4 adresse provenant de la plage du sous-réseau. Pour plus d'informations, consultez Modifier les attributs d'adressage IP de votre sous-réseau. • Adresse IP — Par défaut, Amazon EFS crée la cible de montage à une adresse disponible sur le sous-réseau spécifié. Vous pouvez également spécifier l'adresse IP de la cible de montage. Vous ne pouvez pas modifier l'adresse IP d'une cible de montage une fois qu'elle a été créée. Vous devez supprimer la cible de montage et en créer une nouvelle avec la nouvelle adresse. • Groupe de sécurité : le groupe de sécurité attribué à la cible VPC est utilisé par défaut. Vous pouvez ajouter ou supprimer des groupes de sécurité. Pour plus d'informations sur les groupes de sécurité, consultez Modification des groupes de sécurité cibles de montage. Lorsque vous créez un système de fichiers à l'AWS CLI aide de l'API Amazon EFS ou AWS SDKs, vous ne pouvez pas créer de cible de

Paramètre	Description
	montage en même temps. Vous devez attendre que le système de fichiers soit créé, puis utiliser l'opération CreateMountTarget d'API pour créer les cibles de montage. Pour plus d'informations sur les cibles de montage, consultez Gérer des cibles de Montage.

Création rapide à l'aide de la console

Utilisez la console Amazon EFS pour créer un système de fichiers Amazon EFS doté des paramètres recommandés. Si vous souhaitez créer un système de fichiers avec une configuration intégrée, consultez [Création personnalisée à l'aide de la console](#).

Pour créer rapidement un système de fichiers Amazon EFS doté des paramètres recommandés

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/efs/>.
2. Choisissez Créer un système de fichiers pour ouvrir l'assistant de création de système de fichiers.
3. (Facultatif) Entrez un Nom pour votre système de fichiers.
4. Pour cloud privé virtuel (VPC), choisissez votre VPC, ou conservez-le comme VPC par défaut.
5. Choisissez Créer pour créer un système de fichiers utilisant les paramètres recommandés par le service suivants :
 - Disponibilité par région
 - Politiques de cycle de vie visant à faire passer le système de fichiers au stockage EFS Infrequent Access (IA) après 30 jours, au stockage des archives EFS après 90 jours, et à ne pas passer au stockage standard EFS
 - Chiffrement des données au repos activé
 - Mode de débit élastique
 - Mode de performance à usage général

- Montez les cibles configurées dans chaque zone de disponibilité Région AWS dans laquelle le système de fichiers est créé, en utilisant un IPv4

La page Systèmes de fichiers apparaît avec une bannière en haut indiquant l'état du système de fichiers que vous avez créé. Un lien permettant d'accéder à la page de détails du système de fichiers apparaît dans la bannière lorsque ce dernier est disponible.

Pour plus d'informations sur les états d'un système de fichiers, consultez [Comprendre l'état du système de fichiers](#).

Création personnalisée à l'aide de la console

Cette section décrit le processus d'utilisation de la console Amazon EFS pour créer un système de fichiers EFS avec des paramètres personnalisés au lieu d'utiliser les paramètres recommandés par le service. Pour plus d'informations sur la création d'un système de fichiers à l'aide des paramètres recommandés, consultez [Création rapide à l'aide de la console](#).

La création d'un système de fichiers EFS avec des paramètres personnalisés à l'aide de la console s'effectue en quatre étapes :

- Étape 1 : configurez les paramètres généraux du système de fichiers, notamment la classe de stockage et le mode de débit.
- Étape 2 : configurez les paramètres réseau du système de fichiers, notamment le cloud privé virtuel (VPC) et les cibles de montage. Pour chaque cible de montage, définissez la zone de disponibilité, le sous-réseau, l'adresse IP et les groupes de sécurité.
- Étape 3 : (facultative) créez une politique de système de fichiers pour contrôler l'accès des clients NFS à ce dernier.
- Étape 4 : passez en revue les paramètres du système de fichiers, apportez les modifications nécessaires, puis créez le système de fichiers.

Étape 1 : configurez les paramètres du système de fichiers

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/efs/>.
2. Choisissez Créer un système de fichiers pour ouvrir l'assistant de création de système de fichiers.

3. Choisissez Personnaliser pour créer un système de fichiers personnalisé au lieu de créer un système de fichiers en utilisant les paramètres recommandés. La page des Paramètres du système de fichiers s'ouvre.
4. Sous les paramètres Généraux, effectuez les opérations suivantes :
 - a. (Facultatif) Saisissez un Nom pour le système de fichiers.
 - b. Pour le type de système de fichiers, Régional est sélectionné par défaut. Choisissez One Zone si vous souhaitez créer un système de fichiers qui stocke les données et les métadonnées du système de fichiers de manière redondante au sein d'une seule zone de disponibilité. Si vous choisissez One Zone, choisissez la Zone de disponibilité dans laquelle vous souhaitez créer le système de fichiers ou conservez la valeur par défaut.
 - c. Pour la Gestion du cycle de vie, modifiez les politiques de cycle de vie, si nécessaire.
 - Transition vers IA : sélectionnez le moment où vous souhaitez transférer les fichiers vers la classe de stockage Infrequent Access (IA), en fonction du temps écoulé depuis leur dernier accès dans le stockage standard.
 - Transition vers l'archivage : sélectionnez à quel moment les fichiers doivent être transférés vers la classe de stockage Archive, en fonction du temps écoulé depuis la dernière consultation dans le stockage Standard.
 - Transition vers Standard : indiquez si vous souhaitez transférer le système de fichiers vers la classe de stockage.

Pour plus d'informations sur les politiques de cycle de vie, consultez [Gestion du cycle de vie du stockage](#).

- d. Amazon EFS utilise votre AWS Key Management Service (AWS KMS) clé de service EFS (aws/elasticfilesystem) pour chiffrer les données au repos par défaut. Pour choisir une clé KMS différente pour le chiffrement, ouvrez les Paramètres personnalisés de chiffrement et choisissez une clé dans la liste. Vous pouvez également saisir un ID de clé KMS ou un nom de ressource Amazon (ARN) pour la clé KMS que vous souhaitez utiliser.

Si vous devez créer une nouvelle clé, choisissez Create an AWS KMS key pour lancer la AWS KMS console et créer une nouvelle clé.

Vous pouvez désactiver le chiffrement des données au repos en décochant la case.

Vous ne pouvez pas modifier le paramètre de chiffrement une fois le système de fichiers créé. Pour de plus amples informations, veuillez consulter [Chiffrement des données dans Amazon EFS](#).

5. Pour les paramètres de Performance, procédez comme suit :

- a. Le Mode de débit Élastique est sélectionné par défaut.
 - Pour utiliser le débit provisionné, choisissez Provisionnée et dans Débit provisionné (Mio/s), saisissez le débit à allouer pour les demandes du système de fichiers. La valeur du Débit de lecture maximal affichée est trois fois supérieure à celle du débit saisi.
 - Pour utiliser le débit en rafale, choisissez Bursting.

Une fois que vous avez choisi le mode de débit, une estimation du coût mensuel du système de fichiers s'affiche. Vous pouvez modifier le mode de débit une fois que le système de fichiers est disponible.

Pour plus d'informations sur le choix du mode de débit adapté à vos besoins en termes de performances, consultez [Chiffrement des données dans Amazon EFS](#).

- b. Pour le Mode de performance, l'option par défaut est Usage général. Pour modifier le mode de performance, ouvrez les Paramètres supplémentaires, puis choisissez E/S max.

Vous ne pouvez pas modifier le mode de performance une fois que le système de fichiers est disponible. Pour de plus amples informations, veuillez consulter [Modes de performances](#).

 Important

En raison des latences par opération plus élevées avec E/S max, nous recommandons d'utiliser le mode de performance Usage général pour tous les systèmes de fichiers.

6. (Facultatif) Ajoutez des paires clé-valeur de balise à votre système de fichiers.
7. Choisissez Suivant pour configurer l'accès réseau pour le système de fichiers.

Étape 2 : configurer l'accès réseau

À l'étape 2, vous configurez les paramètres réseau du système de fichiers, notamment le VPC et les cibles de montage.

1. Choisissez le Virtual Private Cloud (VPC) dans lequel vous souhaitez que les EC2 instances se connectent à votre système de fichiers. Pour de plus amples informations, veuillez consulter [Gérer des cibles de Montage](#).
2. Pour les Cibles de montage, vous en créez une ou plusieurs pour votre système de fichiers. Pour chaque cible de montage, définissez les propriétés suivantes :
 - Zone de disponibilité : par défaut, une cible de montage est configurée dans chaque zone de disponibilité d'une Région AWS. Si vous ne souhaitez pas de cible de montage dans une zone de disponibilité particulière, choisissez Supprimer pour supprimer la cible de montage pour cette zone. Créez une cible de montage dans chaque zone de disponibilité à partir de laquelle vous prévoyez d'accéder à votre système de fichiers, sans frais.
 - ID de sous-réseau : choisissez l'un des sous-réseaux disponibles dans une zone de disponibilité. Le sous-réseau par défaut est présélectionné.
 - Type d'adresse IP — Choisissez de IPv4 ne prendre en charge que IPv4 les adresses, IPv6 uniquement pour prendre en charge IPv6 les adresses, ou de Dual-Stack pour prendre en charge IPv4 les deux IPv6 adresses.
 - IPv4 ou IPv6 adresse : si vous connaissez l'adresse IP sur laquelle vous souhaitez placer la cible de montage, saisissez-la dans le champ d'adresse IP correspondant au type d'adresse IP. Si vous ne spécifiez aucune valeur, Amazon EFS sélectionne une adresse IP non utilisée dans le sous-réseau spécifié.
 - Groupes de sécurité : par défaut, Amazon EFS choisit le groupe de sécurité par défaut pour le VPC. Pour modifier le groupe de sécurité, supprimez le groupe attribué, puis choisissez-le dans la liste Choisir les groupes de sécurité. Vous pouvez spécifier un ou plusieurs groupes de sécurité pour la cible de montage. Pour de plus amples informations, veuillez consulter [Utilisation de groupes de sécurité VPC](#).
3. Choisissez Ajouter une cible de montage pour créer une cible de montage pour une zone de disponibilité qui n'en possède pas. Si une cible de montage est configurée pour chaque zone de disponibilité, ce choix n'est pas disponible.
4. Choisissez Suivant pour enregistrer la stratégie de système de fichiers.

Étape 3 : créer une politique de système de fichiers (facultatif)

Vous pouvez également créer une politique de système de fichiers pour votre système de fichiers. Une politique de système de fichiers EFS est une politique de ressource IAM utilisée pour contrôler l'accès NFS au système de fichiers. Pour de plus amples informations, veuillez consulter [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#).

1. Dans les Options de politique, vous pouvez choisir n'importe quelle combinaison de politiques de système de fichiers préconfigurées :
 - Empêcher l'accès à la racine par défaut : cette option supprime `ClientRootAccess` de l'ensemble des actions EFS autorisées.
 - Appliquer l'accès en lecture seule par défaut : cette option supprime `ClientWriteAccess` de l'ensemble des actions EFS autorisées.
 - Empêcher l'accès anonyme : cette option supprime `ClientMount` de l'ensemble des actions EFS autorisées.
 - Appliquer le chiffrement en transit à tous les clients : cette option refuse l'accès aux clients non chiffrés.

Lorsque vous choisissez une politique préconfigurée, l'objet JSON de la politique s'affiche dans le volet de l'Éditeur de politiques.

2. Utilisez l'option Accorder des autorisations supplémentaires pour accorder des autorisations de système de fichiers à d'autres principaux IAM, y compris à un autre. Compte AWS Choisissez Ajouter, puis saisissez l'ARN principal de l'entité à laquelle vous accordez des autorisations. Choisissez les Autorisations que vous souhaitez accorder. Les autorisations supplémentaires sont affichées dans l'Éditeur de politiques.
3. Vous pouvez utiliser l'Éditeur de politiques pour personnaliser une politique préconfigurée ou pour créer votre propre politique de système de fichiers. Lorsque vous utilisez l'éditeur, les options de politique préconfigurées ne sont plus disponibles. Pour effacer la politique actuelle du système de fichiers et commencer à en créer une nouvelle, choisissez Effacer.
4. Choisissez Suivant pour vérifier et créer le système de fichiers.

Étape 4 : vérifier et créer

1. Examinez chacun des groupes de configuration de système de fichiers. Vous pouvez alors apporter des modifications à chaque groupe en choisissant Modifier.

2. Choisissez **Créer un système de fichiers** pour créer votre système de fichiers et revenez à la page **Systèmes de fichiers**.

Une bannière située en haut indique que le nouveau système de fichiers est en cours de création. Un lien permettant d'accéder à la page de détails du nouveau système de fichiers apparaît dans la bannière lorsque ce dernier est disponible.

Créez à l'aide du AWS CLI

Lorsque vous utilisez le AWS CLI, vous créez ces ressources dans l'ordre. Tout d'abord, vous créez un système de fichiers. Vous pouvez ensuite créer des cibles de montage et des balises facultatives supplémentaires pour le système de fichiers à l'aide des AWS CLI commandes correspondantes.

Les exemples suivants utilisent `adminuser` comme valeurs des paramètres `--profile`. Vous devez utiliser un profil utilisateur approprié pour fournir vos informations d'identification. Pour plus d'informations, reportez-vous à la section [Conditions requises pour utiliser le AWS CLI dans le Guide de l'AWS Command Line Interface utilisateur](#).

- Pour créer un système de fichiers chiffré avec les sauvegardes automatiques activées, utilisez la commande Amazon EFS `create-file-system` CLI (l'opération correspondante est [CreateFileSystem](#)), comme indiqué ci-dessous.

```
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
```

Par exemple, la `create-file-system` commande suivante crée un système de fichiers utilisant le débit élastique dans le `us-west-2` Région AWS. La commande spécifie `MyFirstFS` comme jeton de création. Pour obtenir une liste des Régions AWS endroits où vous pouvez créer un système de fichiers Amazon EFS, consultez la section [Points de terminaison et quotas Amazon EFS](#) dans le Référence générale d'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
```

Une fois le système de fichiers créé, Amazon EFS renvoie la description du système de fichiers au format JSON, comme illustré dans l'exemple suivant.

```
{  
  "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'exemple suivant crée un système de fichiers qui utilise le débit en rafale dans la zone de us-west-2a disponibilité à l'aide de la `availability-zone-name` propriété.

```
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
```

Une fois le système de fichiers créé, Amazon EFS renvoie la description du système de fichiers au format JSON, comme illustré dans l'exemple suivant.

```
{  
  "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 fournit également la commande d'interface de ligne de commande `describe-file-systems` (l'opération d'API correspondante est [DescribeFileSystems](#)) que vous pouvez utiliser pour extraire la liste des systèmes de fichiers de votre compte, comme illustré ci-après :

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

Amazon EFS renvoie une liste des systèmes de fichiers que vous Compte AWS avez créés dans la région spécifiée.

Suppression de systèmes de fichiers EFS

La suppression d'un système de fichiers est une action destructrice que vous ne pouvez pas annuler. Vous perdez le système de fichiers ainsi que les données qu'il contient. Les données que vous supprimez d'un système de fichiers sont détruites et vous ne pouvez pas les restaurer. Lorsque les utilisateurs suppriment des données d'un système de fichiers, ces données sont immédiatement rendues inutilisables. EFS force le remplacement des données à terme.

Note

Vous ne pouvez pas supprimer un système de fichiers faisant partie d'une configuration de réplication. Vous devez d'abord supprimer la configuration de réplication. Pour de plus amples informations, veuillez consulter [Supprimer des configuration de réplication](#).

Important

Vous devez toujours démonter un système de fichiers avant de le supprimer.

Utilisation de la console

Pour supprimer un système de fichiers

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Choisissez le système de fichiers . que vous souhaitez supprimer dans la liste des systèmes de fichiers.
3. Sélectionnez Delete (Supprimer).

4. Dans la boîte de dialogue Supprimer le système de fichiers, entrez l'ID du système de fichiers affiché, puis choisissez Confirmer pour confirmer la suppression.

La console simplifie la suppression du système de fichiers pour vous. Tout d'abord, elle supprime les cibles de montage associées, puis elle supprime le système de fichiers.

En utilisant le AWS CLI

Avant de pouvoir utiliser la AWS CLI commande pour supprimer un système de fichiers, vous devez supprimer toutes les cibles de montage et tous les points d'accès créés pour le système de fichiers.

Pour des exemples de AWS CLI commandes, voir [Étape 4 : nettoyer](#).

Création de politiques de système de fichiers

Vous pouvez créer une politique de système de fichiers à l'aide de la console Amazon EFS ou de l'AWS CLI. Vous pouvez également créer une politique de système de fichiers par programmation en utilisant directement l'AWS SDKs API Amazon EFS. Les politiques du système de fichiers EFS sont limitées à 20 000 caractères. Pour plus d'informations sur l'utilisation d'une politique de système de fichiers EFS et pour des exemples, consultez [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#).

Note

Les modifications d'une politique de système de fichiers Amazon EFS peuvent prendre plusieurs minutes pour entrer en vigueur.

Utilisation de la console

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Choisissez Systèmes de fichiers.
3. Sur la page Système de fichiers, choisissez le système de fichiers pour lequel vous souhaitez modifier ou créer une politique de système de fichiers.
4. Choisissez Politique du système de fichiers, puis Modifier.
5. Dans les Options de politique, vous pouvez choisir n'importe quelle combinaison de politiques de système de fichiers préconfigurées :

- Empêcher l'accès à la racine par défaut : cette option supprime `ClientRootAccess` de l'ensemble des actions EFS autorisées.
- Appliquer l'accès en lecture seule par défaut : cette option supprime `ClientWriteAccess` de l'ensemble des actions EFS autorisées.
- Empêcher l'accès anonyme : cette option supprime `ClientMount` de l'ensemble des actions EFS autorisées.
- Appliquer le chiffrement en transit à tous les clients : cette option refuse l'accès aux clients non chiffrés.

Lorsque vous choisissez une politique préconfigurée, l'objet JSON de la politique s'affiche dans le volet de l'Éditeur de politiques.

6. Utilisez l'option `Accorder des autorisations supplémentaires` pour accorder des autorisations de système de fichiers à d'autres principaux IAM, y compris à un autre. Compte AWS Choisissez `Ajouter`, puis saisissez l'ARN principal de l'entité à laquelle vous accordez des autorisations. Choisissez les Autorisations que vous souhaitez accorder. Les autorisations supplémentaires sont affichées dans l'Éditeur de politiques.
7. Vous pouvez utiliser l'Éditeur de politiques pour personnaliser une politique préconfigurée ou pour créer votre propre politique de système de fichiers. Lorsque vous utilisez l'éditeur, les options de politique préconfigurées ne sont plus disponibles. Pour effacer la politique actuelle du système de fichiers et commencer à en créer une nouvelle, choisissez `Effacer`.

Lorsque vous effacez la politique dans l'éditeur, les politiques préconfigurées sont de nouveau disponibles.

8. Une fois que vous avez terminé de modifier la politique, choisissez `Enregistrer`.

En utilisant le AWS CLI

Dans l'exemple suivant, la commande [put-file-system-policy](#) CLI crée une politique de système de fichiers qui autorise l'accès en Compte AWS lecture seule spécifié au système de fichiers EFS. La commande API équivalente est [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\"
      }
    ]
  }
}

```

Création de points d'accès

Vous pouvez créer et supprimer des points d'accès Amazon EFS à l'aide de AWS Management Console, the AWS Command Line Interface (AWS CLI) et de l'API Amazon EFS et SDKs. Vous ne pouvez pas modifier un point d'accès une fois qu'il a été créé. Un système de fichiers peut avoir un maximum de 10 000 points d'accès, sauf si vous demandez une augmentation.

 Note

Si plusieurs demandes de création de points d'accès sur le même système de fichiers sont envoyées en succession rapide et que le système de fichiers approche de la limite de points d'accès, il est possible que la réponse à ces demandes soit limitée. Cela permet de garantir que le système de fichiers ne dépasse pas le quota de points d'accès indiqué.

Pour plus d'informations sur les points d'accès EFS, consultez [Utilisation des points d'accès](#).

Utilisation de la console

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Choisissez Points d'accès pour ouvrir la fenêtre Points d'accès.
3. Choisissez Créer un point d'accès pour accéder à la page Créer un point d'accès.

Vous pouvez également ouvrir la page Créer un point d'accès en choisissant Systèmes de fichiers. Choisissez un Nom de système de fichiers ou un ID de système de fichiers, puis choisissez Points d'accès et Créer un point d'accès pour créer un point d'accès pour ce système de fichiers.

- a. Sur la page des Détails, saisissez les informations suivantes :
 - Système de fichiers : saisissez un nom ou un ID de système de fichiers et choisissez le système de fichiers correspondant. Vous pouvez également choisir le système de fichiers dans la liste qui apparaît lorsque vous choisissez le champ de saisie.
 - (Facultatif) Nom : saisissez un nom pour le point d'accès.
 - (Facultatif) Chemin du répertoire racine : vous pouvez spécifier un répertoire racine pour le point d'accès ; la racine du point d'accès par défaut est /. Pour saisir un chemin du répertoire racine, utilisez le format /foo/bar. Pour de plus amples informations, veuillez consulter [Application forcée d'un répertoire racine avec un point d'accès](#).
- b. (Facultatif) Dans le panneau Utilisateur POSIX, vous pouvez spécifier l'identité POSIX complète à utiliser pour appliquer les informations d'utilisateur et de groupe pour toutes les opérations de fichier réalisées par des clients NFS qui utilisent le point d'accès. Pour de plus amples informations, veuillez consulter [Application forcée d'une identité utilisateur à l'aide d'un point d'accès](#).
 - ID utilisateur : saisissez un ID d'utilisateur POSIX numérique pour l'utilisateur.

- ID de groupe : saisissez un ID de groupe POSIX numérique pour l'utilisateur.
 - Groupe secondaire IDs — Entrez une liste facultative de groupes secondaires séparés par des virgules. IDs
- c. (Facultatif) Pour les autorisations de création de répertoire racine, vous pouvez spécifier les autorisations à utiliser lorsqu'Amazon EFS crée le chemin du répertoire racine, si cela est spécifié et si le répertoire racine n'existe pas déjà. Pour de plus amples informations, veuillez consulter [Application forcée d'un répertoire racine avec un point d'accès](#).

 Note

Si vous ne spécifiez pas la propriété et les autorisations du répertoire racine et que ce dernier n'existe pas encore, EFS ne le créera pas. Toute tentative de montage du système de fichiers à l'aide du point d'accès échouera.

- ID d'utilisateur propriétaire : saisissez l'ID d'utilisateur POSIX numérique à utiliser en tant que propriétaire du répertoire racine.
 - ID de groupe propriétaire : saisissez l'ID de groupe POSIX numérique à utiliser en tant qu'utilisateur propriétaire du répertoire racine.
 - Autorisations : saisissez le mode Unix du répertoire. Une configuration commune est 755. Assurez-vous que le bit d'exécution est défini pour l'utilisateur du point d'accès afin qu'il puisse être monté.
4. Choisissez Créer un point d'accès pour créer le point d'accès à l'aide de cette configuration.

En utilisant le AWS CLI

L'exemple de commande d'interface de ligne de commande `create-access-point` suivant montre la création d'un point d'accès pour un système de fichiers EFS. La commande API équivalente est [CreateAccessPoint](#).

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

Si la demande aboutit, l'interface de ligne de commande répond avec la description du point d'accès.

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

Note

Si plusieurs demandes de création de points d'accès sur le même système de fichiers sont envoyées en succession rapide et que le système de fichiers approche de la limite de points d'accès, il est possible que la réponse à ces demandes soit limitée. Cela permet de garantir que le système de fichiers ne dépasse pas le quota de points d'accès indiqué.

Supprimer des points d'accès

Lorsque vous supprimez un point d'accès, tous les clients qui l'utilisent perdent l'accès au système de fichiers Amazon EFS pour lequel il est configuré.

Utilisation de la console

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Dans le volet de navigation de gauche, choisissez Points d'accès pour ouvrir la page Points d'accès.
3. Sélectionnez le point d'accès à supprimer.
4. Sélectionnez Delete (Supprimer).
5. Choisissez Confirmer pour confirmer l'action et supprimer le point d'accès.

En utilisant le AWS CLI

Dans l'exemple suivant, la commande d'interface de ligne de commande `delete-access-point` supprime le point d'accès spécifié. La commande API équivalente est [DeleteAccessPoint](#). Si la commande aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

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

Marquage des ressources EFS

Pour vous aider à gérer vos ressources EFS, vous pouvez attribuer vos propres métadonnées à chaque ressource sous forme de balises. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire ou de leur environnement. Cette classification est utile lorsque vous avez de nombreuses ressources de même type. Elle vous permet d'identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées. Cette rubrique décrit les identifications et explique comment les créer.

Principes de base des étiquettes

Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez.

Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Par exemple, vous pouvez définir un ensemble de balises pour les systèmes de fichiers Amazon EFS de votre compte qui vous permet de suivre chaque propriétaire de système de fichiers.

Nous vous recommandons de concevoir un ensemble de clés d'étiquette répondant à vos besoins pour chaque type de ressource. L'utilisation d'un ensemble de clés de balise cohérent facilite la gestion de vos ressources. Vous pouvez rechercher et filtrer les ressources en fonction des étiquettes que vous ajoutez.

Les balises n'ont pas de signification sémantique pour Amazon EFS et sont interprétées strictement comme des chaînes de caractères. De plus, les étiquettes ne sont pas automatiquement affectées à vos ressources. Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises d'une ressource à tout moment. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur. Si vous supprimez une ressource, ses balises sont également supprimées.

Restrictions liées aux balises

Les restrictions de base suivantes s'appliquent aux balises :

- Nombre maximal de balises par ressource : 50
- Pour chaque ressource, chaque clé de balise doit être unique, et chaque clé de balise peut avoir une seule valeur.
- Longueur de clé maximale : 128 caractères Unicode en UTF-8
- Longueur de valeur maximale : 256 caractères Unicode en UTF-8
- Amazon EFS permet d'utiliser n'importe quel caractère dans ses balises, mais d'autres services sont plus restrictifs. Les caractères autorisés pour les services sont les lettres, les chiffres et les espaces représentables en UTF-8, ainsi que les caractères suivants : + - = . _ : / @.
- Les clés et valeurs de balise sont sensibles à la casse.
- Le aws : préfixe est réservé à l' AWS usage. Lorsque la balise possède une clé de balise avec ce préfixe, vous ne pouvez pas modifier ou supprimer sa clé ou sa valeur. Les balises avec le préfixe aws : ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Vous ne pouvez pas mettre à jour ou supprimer une ressource uniquement en fonction de ses balises ; vous devez spécifier l'identificateur de ressource. Par exemple, pour supprimer des systèmes de fichiers que vous avez balisés avec une clé de balise appelée DeleteMe, vous devez utiliser l'action DeleteFileSystem avec les identificateurs de ressource du système de fichiers, tels que fs-1234567890abcdef0.

Lorsque vous balisez des ressources publiques ou partagées, les balises que vous attribuez ne sont disponibles que pour votre Compte AWS. Aucun autre Compte AWS utilisateur n'aura accès à ces tags. Pour le contrôle d'accès basé sur des balises aux ressources partagées, chacun Compte AWS doit attribuer son propre ensemble de balises pour contrôler l'accès à la ressource.

Vous pouvez baliser les ressources du système de fichiers et des points d'accès Amazon EFS.

Utilisation de balises pour le contrôle d'accès

Vous pouvez utiliser des balises pour contrôler l'accès aux ressources Amazon EFS et pour implémenter le contrôle d'accès basé sur les attributs (ABAC).

Note

La réplication EFS ne prend pas en charge l'utilisation de balises pour le Contrôle d'accès par attributs (ABAC).

Baliser vos ressources

Vous pouvez baliser les ressources du système de fichiers et des points d'accès Amazon EFS qui existent déjà dans votre compte.

Utilisation de la console

- Vous pouvez utiliser la console Amazon EFS pour appliquer des balises aux ressources existantes en utilisant l'onglet Balises dans l'écran des détails des ressources. Dans la console Amazon EFS, vous pouvez spécifier des balises pour une ressource lorsque vous la créez. Par exemple, vous pouvez ajouter une balise avec une clé de Name et une valeur que vous spécifiez.

Dans la plupart des cas, la console applique les balises immédiatement après la création de la ressource (plutôt qu'au cours de la création de ressources). La console organise des ressources en fonction de la balise Name, mais cette balise n'a pas de signification sémantique pour le service Amazon EFS.

En utilisant le AWS CLI

- Si vous utilisez l'API Amazon EFS, le ou un AWS SDK AWS CLI, vous pouvez utiliser l'action d'API `TagResource` EFS pour appliquer des balises aux ressources existantes. En outre,

certaines actions de création de ressources vous permettent de spécifier des étiquettes pour une ressource lors de la création de cette dernière.

Les AWS CLI commandes de gestion des balises, ainsi que les actions d'API Amazon EFS équivalentes, sont répertoriées dans le tableau suivant.

Commande de la CLI	Description	Opération d'API équivalente
tag-resource	Ajouter de nouvelles balises ou mettre à jour des balises existantes	TagResource
list-tags-for-resource	Récupérer des balises existantes	ListTagsForResource
untag-resource	Supprimer des balises existantes	UntagResource

Tutoriel : Création de sous-répertoires accessibles en écriture par utilisateur

Une fois que vous avez créé un système de fichiers EFS et que vous l'avez monté localement sur votre instance Amazon EC2 (EC2), il expose un répertoire vide appelé. *file system root* L'un des cas d'utilisation courants de ce répertoire racine du système de fichiers consiste à créer un sous-répertoire « accessible en écriture » pour chaque utilisateur que vous créez sur l' EC2 instance et à monter le sous-répertoire dans le répertoire personnel de l'utilisateur. Tous les fichiers et sous-répertoires créés par l'utilisateur dans son répertoire personnel sont ensuite créés dans le système de fichiers EFS.

Note

Vous pouvez suivre l'[Premiers pas](#) exercice pour créer et monter un système de fichiers EFS sur votre EC2 instance.

Dans les étapes suivantes, vous créez un utilisateur, créez un sous-répertoire pour l'utilisateur, faites de l'utilisateur le propriétaire du sous-répertoire, puis montez le sous-répertoire Amazon EFS dans le répertoire personnel de l'utilisateur.

1. Créez l'utilisateur mike :

- Connectez-vous à votre EC2 instance. À l'aide des privilèges root (dans ce cas, à l'aide de la `sudo` commande), créez l'utilisateur et attribuez un mot de passe.

Par exemple, la commande suivante crée l'utilisateur `mike`.

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

Un répertoire personnel est également créé pour l'utilisateur. Par exemple, `/home/mike`.

2. Créez un sous-répertoire `EFStoot` pour l'utilisateur sous.

Par exemple, la commande suivante crée un sous-répertoire `mike` sous `EFStoot`.

```
$ sudo mkdir /EFStoot/mike
```

Vous devrez le remplacer `EFStoot` par le nom de votre répertoire local.

3. L'utilisateur root et le groupe root sont les propriétaires du sous-répertoire (vous pouvez le vérifier à l'aide de la `ls -l` commande). Pour accorder des autorisations complètes à l'utilisateur sur ce sous-répertoire, accordez-lui la propriété du répertoire.

Par exemple :

```
$ sudo chown mike:mike /EFStoot/mike
```

4. Utilisez la `mount` commande pour monter le sous-répertoire dans le répertoire personnel de l'utilisateur.

Par exemple :

```
$ sudo mount -t nfs -o
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-DNS:/mike /home/mike
```

L'*mount-target-DNS* adresse identifie la racine du système de fichiers EFS distant.

Si vous démontez cette cible de montage, l'utilisateur ne peut pas accéder au répertoire sans le remonter, ce qui nécessite des autorisations root.

Montage des systèmes de fichiers EFS

Pour monter des systèmes de fichiers EFS, nous vous recommandons d'utiliser l'assistant de montage EFS. L'assistant de montage EFS vous aide à monter vos systèmes de fichiers EFS sur des instances EC2 Linux et Mac exécutant les distributions prises en charge. L'assistant de montage fait partie de la collection d'outils open source qui est installée lorsque vous installez le client Amazon EFS (`amazon-efs-utils`). Pour plus d'informations sur le client Amazon EFS et les distributions prises en charge, consultez [Installation du client Amazon EFS](#).

Vous pouvez également monter manuellement les systèmes de fichiers EFS à l'aide du client NFS Linux standard. Amazon EFS prend en charge les protocoles Network File System versions 4.0 et 4.1 (NFSv4) lors du montage de vos systèmes de fichiers sur des EC2 instances Amazon.

En outre, vous pouvez utiliser l'assistant de montage EFS ou NFS pour configurer une EC2 instance afin de monter automatiquement un système de fichiers EFS au démarrage de l'instance.

Rubriques

- [Considérations relatives au montage pour Linux](#)
- [Montage de systèmes de fichiers EFS à l'aide de l'assistant de montage EFS](#)
- [Utilisation du système de fichiers réseau pour monter des systèmes de fichiers EFS](#)
- [Montage automatique des systèmes de fichiers EFS](#)
- [Démontage des systèmes de fichiers](#)
- [Tutoriel : créer un système de fichiers EFS et le monter sur une EC2 instance à l'aide du AWS CLI](#)
- [Tutoriel : Montage avec des clients Linux locaux](#)
- [Tutoriel : monter un système de fichiers à partir d'un autre VPC](#)
- [Résolution des problèmes de montage](#)

Considérations relatives au montage pour Linux

Nous vous recommandons d'utiliser les valeurs suivantes pour les options de Montage sous Linux :

- `rsize=1048576` – Définit le nombre maximal d'octets de données que le client NFS peut recevoir pour chaque demande READ du réseau. Cette valeur s'applique lors de la lecture des données à partir d'un fichier sur un système de fichiers EFS. Nous vous recommandons d'utiliser la plus grande taille possible (jusqu'à 1048576) afin d'éviter une baisse de performances.

- `wsiz=1048576` – Définit le nombre maximal d'octets de données que le client NFS peut envoyer pour chaque demande `WRITE` du réseau. Cette valeur s'applique lors de l'écriture de données sur un fichier d'un système de fichiers EFS. Nous vous recommandons d'utiliser la plus grande taille possible (jusqu'à 1048576) afin d'éviter une baisse de performances.
- `hard` – Définit le comportement de récupération du client NFS après qu'une demande NFS a expiré, de sorte que les demandes NFS sont relancées indéfiniment jusqu'à ce que le serveur réponde. Nous vous recommandons d'utiliser l'option de Montage physique (`hard`) pour garantir l'intégrité des données. Si vous utilisez un Montage `soft`, définissez le paramètre `timeo` sur au Moins 150 décisecondes (15 secondes). Vous minimiserez ainsi le risque de corruption des données inhérent aux Montages logiciels.
- `timeo=600` – Définit la valeur de délai d'expiration que le client NFS utilise pour attendre une réponse avant de relancer une demande NFS sur 600 décisecondes (60 secondes). Si vous devez Modifier le paramètre de délai (`timeo`), nous vous recommandons d'utiliser une valeur d'au Moins 150, ce qui équivaut à 15 secondes. Vous éviterez ainsi une baisse de performances.
- `retrans=2` – Définit sur 2 le nombre de fois que le client NFS essaie une demande avant de tenter une action de récupération.
- `noresvport` – Indique au client NFS d'utiliser un nouveau port source TCP (Transmission Control Protocol) non privilégié lorsqu'une connexion réseau est rétablie. Cette utilisation permet de s'assurer que le système de fichiers EFS a une disponibilité ininterrompue après un événement de récupération du réseau.
- `_netdev` – Lorsque cette option est présente dans `/etc/fstab`, elle empêche le client d'essayer de Monter le système de fichiers EFS tant que le réseau n'a pas été activé.

En général, évitez de définir d'autres options de Montage différentes des valeurs par défaut, ce qui peut entraîner une réduction des performances et d'autres problèmes. Si vous n'utilisez pas les valeurs par défaut précédentes, vous devez être conscient des points suivants :

- La Modification des tailles tampon de lecture ou d'écriture, ou la désactivation de la mise en cache d'attribut, peuvent entraîner une réduction des performances.
- Amazon EFS ignore les ports source. Si vous Modifiez les ports source Amazon EFS, cela n'a aucun effet.
- Amazon EFS ne prend en charge aucune des variantes sécurité Kerberos. Par exemple, la commande de Montage suivante échoue.

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

- Nous vous recommandons de Monter votre système de fichiers à l'aide de son nom DNS. Amazon EFS convertit ce nom en adresse IP de la cible de montage EFS dans la même zone de disponibilité que votre EC2 instance Amazon sans faire appel à des ressources externes. Si vous utilisez une cible de montage dans une zone de disponibilité différente de celle de votre EC2 instance, vous devez payer des EC2 frais standard pour les données envoyées entre les zones de disponibilité. De même, vous pouvez constater des latences accrues pour les opérations de système de fichiers.
- Pour plus d'options de montage et des explications détaillées sur les valeurs par défaut, consultez la documentation Linux.

Note

Si votre EC2 instance doit démarrer quel que soit le statut de votre système de fichiers EFS monté, ajoutez `l'nofail` option à l'entrée de votre système de fichiers dans votre `/etc/fstab` fichier.

Montage de systèmes de fichiers EFS à l'aide de l'assistant de montage EFS

Après avoir installé le client Amazon EFS (`amazon-efs-utils`), vous pouvez utiliser l'assistant de montage EFS pour monter des systèmes de fichiers EFS sur vos instances EC2 Linux et Mac exécutant des [distributions prises en charge](#). Amazon EFS ne prend pas en charge le montage à partir d'instances EC2 Windows.

Important

Nous vous recommandons de toujours utiliser la version la plus récente de `amazon-efs-utils` pour garantir un montage réussi. Par exemple, les versions `amazon-efs-utils` antérieures à 2.3 ne prennent pas en charge le montage avec des IPv6 adresses.

Lors du montage d'un système de fichiers, l'assistant de montage définit un nouveau type de système de fichiers `reseauefs`, appelé, qui est entièrement compatible avec la `mount` commande standard sous Linux. L'assistant de montage prend également en charge le montage automatique d'un

système de fichiers EFS au moment du démarrage de l'instance en utilisant les entrées du fichier `/etc/fstab` de configuration sur les instances EC2 Linux.

 Warning

Utilisez l'option `_netdev`, utilisée pour identifier les systèmes de fichiers réseau lors du Montage automatique de votre système de fichiers. Si elle `_netdev` est absente, il est possible que votre EC2 instance cesse de répondre. Cela s'explique par le fait que les systèmes de fichiers réseau doivent être initialisés après le démarrage de la mise en réseau de l'instance de calcul. Pour de plus amples informations, veuillez consulter [Le montage automatique échoue et l'instance ne répond pas](#).

Vous pouvez Monter un système de fichiers en spécifiant l'une des propriétés suivantes :

- Nom DNS du système de fichiers – Si vous utilisez le nom DNS du système de fichiers et que l'assistant de Montage ne parvient pas à le résoudre, par exemple lorsque vous Montez un système de fichiers dans un autre VPC, il utilisera à nouveau l'adresse IP cible de Montage. Pour de plus amples informations, veuillez consulter [Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC](#).
- ID du système de fichiers – Si vous utilisez l'identifiant du système de fichiers, l'assistant de Montage le convertit en adresse IP locale de l'Interface réseau Elastic (ENI) cible du Montage sans faire appel à des ressources externes.
- adresse IP cible de Montage – Vous pouvez utiliser l'adresse IP de l'une des cibles de Montage du système de fichiers.

Vous pouvez trouver la valeur de toutes ces propriétés dans la console Amazon EFS. Le nom DNS du système de fichiers se trouve dans l'écran Joindre.

Lorsque le chiffrement des données en transit est déclaré comme option de montage pour votre système de fichiers EFS, l'assistant de montage initialise un `stunnel` processus client et un processus superviseur est appelé. `amazon-efs-mount-watchdog` Le processus `amazon-efs-mount-watchdog` surveille l'état des Montages TLS et démarre automatiquement la première fois qu'un système de fichiers EFS est Monté sur TLS. Si votre client fonctionne sous Linux, ce processus est géré par votre distribution Linux `upstart` ou `systemd` en fonction de celle-ci. Pour les clients exécutant un macOS compatible, il est géré par `launchd`.

Stunnel est un relais réseau multifonctionnel en open source. Le processus client stunnel écoute le trafic entrant sur un port local et l'assistant de Montage redirige le trafic client NFS vers ce port.

L'assistant de Montage utilise la version 1.2 de TLS pour communiquer avec votre système de fichiers. L'utilisation de TLS nécessite des certificats, et ces certificats sont signés par une autorité de certification Amazon de confiance. Pour plus d'informations sur le fonctionnement du chiffrement, consultez [Chiffrement des données dans Amazon EFS](#).

Rubriques

- [Paramètres de montage utilisés par l'assistant de montage EFS](#)
- [Obtention de journaux de support](#)
- [Conditions préalables à l'utilisation de l'assistant de Montage EFS](#)
- [Montage sur des instances EC2 Linux à l'aide de l'assistant de montage EFS](#)
- [Montage sur des instances EC2 Mac à l'aide de l'assistant de montage EFS](#)
- [Montage de systèmes de fichiers EFS à partir d'un autre Région AWS](#)
- [Montage de systèmes de fichiers Zone unique](#)
- [Montage avec autorisation IAM](#)
- [Montage avec points d'accès EFS](#)
- [Montage d'EFS sur plusieurs EC2 instances](#)
- [Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC](#)

Paramètres de montage utilisés par l'assistant de montage EFS

Le client d'assistance au Montage Amazon EFS utilise les options de Montage suivantes, optimisées pour Amazon EFS :

- `nfsvers=4.1`— utilisé lors du montage sur des instances EC2 Linux
- `nfsvers=4.0`— utilisé lors du montage sur des instances EC2 Mac compatibles exécutant macOS Big Sur, Monterey et Ventura
- `rsize=1048576` – Définit le nombre maximum d'octets de données que le client NFS peut recevoir pour chaque requête READ du réseau à 1048576, le plus grand disponible, pour éviter une diminution des performances.

- `wsiz=1048576` – Définit le nombre maximum d'octets de données que le client NFS peut envoyer pour chaque requête WRITE du réseau à 1048576, le plus grand disponible, pour éviter une diminution des performances.
- `hard` – Définit le comportement de récupération du client NFS en cas de dépassement du délai d'une requête NFS, de manière à ce que les requêtes NFS soient relancées indéfiniment jusqu'à ce que le serveur réponde, pour garantir l'intégrité des données.
- `timeo=600` – Définit la valeur de délai d'expiration que le client NFS utilise pour attendre une réponse avant de relancer une demande NFS sur 600 décisecondes (60 secondes) pour éviter une diminution des performances..
- `retrans=2` – Définit sur 2 le nombre de fois que le client NFS essaie une demande avant de tenter une action de récupération.
- `noresvport` – Indique au client NFS d'utiliser un nouveau port source TCP (Transmission Control Protocol) non privilégié lorsqu'une connexion réseau est rétablie. L'utilisation de l'option `noresvport` permet de garantir la disponibilité ininterrompue de votre système de fichiers EFS après une reconnexion ou un événement de restauration du réseau.
- `mountport=2049`— uniquement utilisé lors du montage sur des instances EC2 Mac exécutant macOS Big Sur, Monterey et Ventura.

Obtention de journaux de support

L'assistant de montage EFS intègre la journalisation de votre système de fichiers EFS. Vous pouvez partager ces journaux avec le AWS Support à des fins de résolution des problèmes. Vous pouvez trouver les journaux stockés dans `/var/log/amazon/efs` sur les clients à l'aide de l'assistant de Montage EFS. Ces journaux concernent l'aide au Montage EFS, le processus stunnel (désactivé par défaut) et le processus `amazon-efs-mount-watchdog` qui surveille le processus stunnel.

Note

Le `amazon-efs-mount-watchdog` processus garantit que le processus Stunnel de chaque montage est en cours d'exécution et arrête le processus Stunnel lorsque le système de fichiers EFS est démonté. Si, pour une raison quelconque, un processus stunnel est interrompu de manière inattendue, le processus de surveillance le redémarre.

Vous pouvez Modifier la configuration de vos journaux dans `/etc/amazon/efs/efs-utils.conf`. Pour que les modifications du journal soient prises en compte, vous devez démonter et remonter le

système de fichiers à l'aide de l'assistant de montage EFS. La capacité de journalisation destinée à l'assistant de Montage et aux journaux de surveillance est limitée à 20 MiB. Les journaux destinés au processus stunnel sont désactivés par défaut.

Important

Vous pouvez activer la journalisation pour les journaux du processus stunnel. Cependant, sachez que cette activation risque d'utiliser une quantité d'espace non négligeable sur votre système de fichiers.

Conditions préalables à l'utilisation de l'assistant de Montage EFS

Vous pouvez monter un système de fichiers EFS sur une EC2 instance Amazon à l'aide de l'assistant de montage Amazon EFS. Pour utiliser l'assistant de Montage, vous avez besoin des éléments suivants :

- ID du système de fichiers à Monter – L'aide au Montage EFS permet de résoudre l'ID du système de fichiers en fonction de l'adresse IP locale de l'Interface réseau Elastic (ENI) de la cible de Montage, sans faire appel à des ressources externes.
- Une cible de montage EFS : vous créez des cibles de montage dans votre cloud privé virtuel (VPC). Si vous créez votre système de fichiers dans la console en utilisant les paramètres recommandés par le service, une cible de montage est créée dans chaque zone de disponibilité dans Région AWS laquelle se trouve le système de fichiers. Pour les instructions relatives à la création de cibles de Montage, consultez [Gérer des cibles de Montage](#).

Note

Nous vous recommandons d'attendre 60 secondes après que l'état du cycle de vie de la cible de Montage nouvellement créée soit disponible avant de Monter le système de fichiers via DNS. Cette attente permet aux enregistrements DNS de se propager entièrement Région AWS là où réside le système de fichiers.

Si vous utilisez une cible de montage dans une zone de disponibilité différente de celle de votre EC2 instance, vous devez payer des EC2 frais standard pour les données envoyées entre les zones de disponibilité. De même, vous pouvez constater des latences accrues pour les opérations de système de fichiers.

- Pour Monter des systèmes de fichiers Zone unique à partir d'une Zone de disponibilité différente :
 - Nom de la zone de disponibilité du système de fichiers : si vous montez un système de fichiers EFS One Zone situé dans une zone de disponibilité différente de celle de l' EC2 instance.
 - Nom DNS de la cible de Montage – Vous pouvez également spécifier le nom DNS de la cible de Montage au lieu de la Zone de disponibilité.
- Une EC2 instance exécutant l'une des distributions Linux ou macOS prises en charge — Les distributions prises en charge pour le montage de votre système de fichiers avec l'assistant de montage sont les suivantes :
 - Amazon Linux 2
 - Amazon Linux 2023
 - Amazon Linux 2017.09 et versions ultérieures
 - macOS Big Sur
 - Red Hat Enterprise Linux (et dérivés telles que CentOS) version 7 et versions ultérieures
 - Ubuntu 16.04 LTS et les versions plus récentes

 Note

EC2 Les instances Mac exécutant macOS Big Sur sont compatibles avec NFS 4.0 uniquement.

- L'assistant de montage EFS est installé sur l' EC2instance : l'assistant de montage est un outil inclus dans le `amazon-efs-utils` package d'utilitaires. Pour plus d'informations sur l'installation `amazon-efs-utils`, consultez [Installation du client Amazon EFS](#).
- L' EC2 instance se trouve dans un VPC : l' EC2 instance de connexion doit se trouver dans un cloud privé virtuel (VPC) basé sur le service Amazon VPC. Il doit également être configuré pour utiliser le serveur DNS fourni par AWS. Pour plus d'informations sur le serveur DNS Amazon, consultez les [ensembles d'options DHCP dans Amazon VPC](#) dans le guide de l'utilisateur Amazon VPC.
- Les noms d'hôte DNS sont activés sur le VPC : les noms d'hôte DNS doivent être activés sur le VPC de l' EC2 instance de connexion. Pour plus d'informations, consultez la section [Attributs DNS de votre VPC](#) dans le guide de l'utilisateur Amazon VPC.
- Pour EC2 des instances et des systèmes de fichiers différents Régions AWS : si l' EC2 instance et le système de fichiers que vous montez sont situés dans des endroits différents Régions AWS, vous devez modifier la `region` propriété dans le `efs-utils.conf` fichier. Pour de plus amples

informations, veuillez consulter [Montage de systèmes de fichiers EFS à partir d'un autre Région AWS](#).

Montage sur des instances EC2 Linux à l'aide de l'assistant de montage EFS

Ce processus nécessite les éléments suivants :

- Vous avez installé le `amazon-efs-utils` package sur l' EC2instance Amazon. Pour de plus amples informations, veuillez consulter [Installation manuelle du client Amazon EFS](#).
- Vous avez créé des cibles de Montage pour le système de fichiers. Pour de plus amples informations, veuillez consulter [Gérer des cibles de Montage](#).

Pour monter votre système de fichiers EFS à l'aide de l'assistant de montage sur les instances EC2 Linux

1. Ouvrez une fenêtre de terminal sur votre EC2 instance via Secure Shell (SSH) et connectez-vous avec le nom d'utilisateur approprié. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Créez un répertoire `efs` que vous utiliserez comme point de Montage du système de fichiers à l'aide de la commande suivante :

```
sudo mkdir efs
```

3. Exécutez les commandes suivantes pour Monter votre système de fichiers.

Note

Si l' EC2 instance et le système de fichiers que vous montez se trouvent dans des emplacements différents Région AWS, reportez-vous [Montage de systèmes de fichiers EFS à partir d'un autre Région AWS](#) à la section pour modifier la `region` propriété dans le `efs-utils.conf` fichier.

- Pour Monter le système de fichiers avec l'ID de système de fichiers :

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

Utilisez l'ID du système de fichiers que vous installez à la place *file-system-id* et efs à la place du système de fichiers *efs-mount-point*.

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

Sinon, si vous souhaitez utiliser le chiffrement des données en transit, vous pouvez Monter votre système de fichiers avec la commande suivante.

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

- Pour effectuer le Montage à l'aide du nom DNS du système de fichiers :

```
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/
```

- Pour effectuer un Montage à l'aide de l'adresse IP cible du Montage :

```
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/
```

Vous pouvez afficher et copier les commandes exactes pour Monter votre système de fichiers dans la boîte de dialogue Attacher.

- a. Dans la console Amazon EFS, choisissez le système de fichiers que vous souhaitez Monter pour afficher sa page de détails.
- b. Pour afficher les commandes de Montage à utiliser pour ce système de fichiers, choisissez Attacher en haut à droite.

L'écran Joindre affiche les commandes exactes à utiliser pour Monter le système de fichiers de la manière suivante :

- (Montage via DNS) En utilisant le nom DNS du système de fichiers avec l'assistant de Montage EFS ou un client NFS.
- (Montage via IP) Utilisation de l'adresse IP cible du Montage dans la Zone de disponibilité sélectionnée avec un client NFS.

Montage sur des instances EC2 Mac à l'aide de l'assistant de montage EFS

Ce processus nécessite les éléments suivants :

- Vous avez installé le `amazon-efs-utils` package sur l'instance Amazon EC2 Mac. Pour de plus amples informations, veuillez consulter [Installation du client Amazon EFS sur des instances EC2 Mac exécutant macOS Big Sur, macOS Monterey ou macOS Ventura](#).
- Vous avez créé des cibles de Montage pour le système de fichiers. Vous pouvez créer des cibles de Montage lors de la création du système de fichiers et les ajouter aux systèmes de fichiers existants. Pour de plus amples informations, veuillez consulter [Gérer des cibles de Montage](#).
- Vous montez le système de fichiers sur une instance EC2 Mac exécutant macOS Big Sur, Monterey ou Ventura. Les autres versions de macOS ne sont pas prises en charge.

Note

Seules les instances EC2 Mac exécutant macOS Big Sur, Monterey et Ventura sont prises en charge. Les autres versions de macOS ne sont pas compatibles avec Amazon EFS.

Pour monter votre système de fichiers EFS à l'aide de l'assistant de montage EFS sur des instances EC2 Mac exécutant macOS Big Sur, Monterey ou Ventura

1. Ouvrez une fenêtre de terminal sur votre instance EC2 Mac via Secure Shell (SSH) et connectez-vous avec le nom d'utilisateur approprié. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Créez un répertoire que vous utiliserez comme point de Montage du système de fichiers à l'aide de la commande suivante :

```
sudo mkdir efs
```

3. Exécutez la commande suivante pour Monter votre système de fichiers.

 Note

Par défaut, l'assistant de montage EFS utilise le chiffrement en transit lors du montage sur des instances EC2 Mac, que vous utilisiez ou non l'`tls` option dans la commande de montage.

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

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

Vous pouvez également utiliser l'option `tls` lors du Montage.

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

Pour monter un système de fichiers sur une instance EC2 Mac sans utiliser le chiffrement en transit, utilisez l'`notls` option, comme indiqué dans la commande suivante.

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

Vous pouvez afficher et copier les commandes exactes pour Monter votre système de fichiers dans la boîte de dialogue Joindre de la console de gestion, décrite comme suit.

- a. Dans la console Amazon EFS, choisissez le système de fichiers que vous souhaitez Monter pour afficher sa page de détails.
- b. Pour afficher les commandes de Montage à utiliser pour ce système de fichiers, choisissez Attacher en haut à droite.

L'écran Joindre affiche les commandes exactes à utiliser pour Monter le système de fichiers de la manière suivante :

- (Montage via DNS) En utilisant le nom DNS du système de fichiers avec l'assistant de Montage EFS ou un client NFS.
- (Montage via IP) Utilisation de l'adresse IP cible du Montage dans la Zone de disponibilité sélectionnée avec un client NFS.

Montage de systèmes de fichiers EFS à partir d'un autre Région AWS

Pour monter votre système de fichiers EFS à partir d'une EC2 instance située dans un autre système de fichiers Région AWS que le système de fichiers, vous devez modifier la valeur de `region` propriété dans le `efs-utils.conf` fichier.

Pour modifier la **region** propriété dans **efs-utils.conf**

1. Accédez au terminal de votre EC2 instance via Secure Shell (SSH) et connectez-vous avec le nom d'utilisateur approprié. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Localisez le fichier `efs-utils.conf` et ouvrez-le à l'aide de votre éditeur préféré.
3. Recherchez la ligne suivante :

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

- a. Décommentez la ligne.
 - b. Si le système de fichiers ne se trouve pas dans la région `us-east-1`, remplacez-le `us-east-1` par l'ID de la région dans laquelle se trouve le système de fichiers.
 - c. Enregistrez les Modifications.
4. Ajoutez une entrée d'hôte pour le Montage interrégional. Pour en savoir plus à ce sujet, consultez [Étape 3 : ajouter une entrée d'hôte pour la cible de montage](#).
 5. Montez le système de fichiers à l'aide de l'assistant de Montage EFS pour les instances [Linux](#) ou [Mac](#).

Montage de systèmes de fichiers Zone unique

Les systèmes de fichiers EFS One Zone ne prennent en charge qu'une seule cible de montage située dans la même zone de disponibilité que le système de fichiers. Vous ne pouvez pas ajouter de cibles de Montage supplémentaires. Cette section décrit les éléments à prendre en compte lors du Montage de systèmes de fichiers Zone unique.

Vous pouvez éviter les frais de transfert de données entre les zones de disponibilité et améliorer les performances en accédant à un système de fichiers EFS à l'aide d'une instance de EC2 calcul Amazon située dans la même zone de disponibilité que celle de la cible de montage du système de fichiers.

Les procédures de la présente section requièrent les éléments suivants :

- Vous l'avez installé `amazon-efs-utils` package sur l' EC2 instance. Pour de plus amples informations, veuillez consulter [Installation du client Amazon EFS](#).
- Vous avez créé une cible de Montage pour le système de fichiers. Pour de plus amples informations, veuillez consulter [Gérer des cibles de Montage](#).

Montage de systèmes de fichiers One Zone EC2 dans une autre zone de disponibilité

Si vous montez un système de fichiers One Zone sur une EC2 instance Amazon située dans une autre zone de disponibilité, vous devez spécifier le nom de la zone de disponibilité du système de fichiers ou le nom DNS de la cible de montage du système de fichiers dans la commande `mount helper mount`.

Créez un répertoire appelé `efs` que vous utiliserez comme point de Montage du système de fichiers à l'aide de la commande suivante :

```
sudo mkdir efs
```

Utilisez la commande suivante pour Monter le système de fichiers à l'aide de l'assistant de Montage EFS. La commande indique le nom de la Zone de disponibilité du système de fichiers.

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

Voici la commande avec des exemples de valeurs :

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

La commande suivante Monte le système de fichiers en spécifiant le nom DNS de la cible de Montage du système de fichiers.

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

Il s'agit de la commande avec un exemple de nom DNS de la cible de Montage.

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

Montage automatique de systèmes de fichiers Zone unique dans une Zone de disponibilité différente avec l'assistant de Montage EFS

Si vous `/etc/fstab` souhaitez monter un système de fichiers EFS One Zone sur une EC2 instance située dans une autre zone de disponibilité, vous devez spécifier le nom de la zone de disponibilité du système de fichiers ou le nom DNS de la cible de montage du système de fichiers dans l'`/etc/fstab` entrée.

```
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
```

Montage automatique de systèmes de fichiers Zone unique avec NFS

Si vous souhaitez monter un système de fichiers EFS `/etc/fstab` à l'aide du stockage One Zone sur une EC2 instance située dans une autre zone de disponibilité, vous devez spécifier le nom de la zone de disponibilité du système de fichiers avec le nom DNS du système de fichiers dans l'`/etc/fstab` entrée.

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

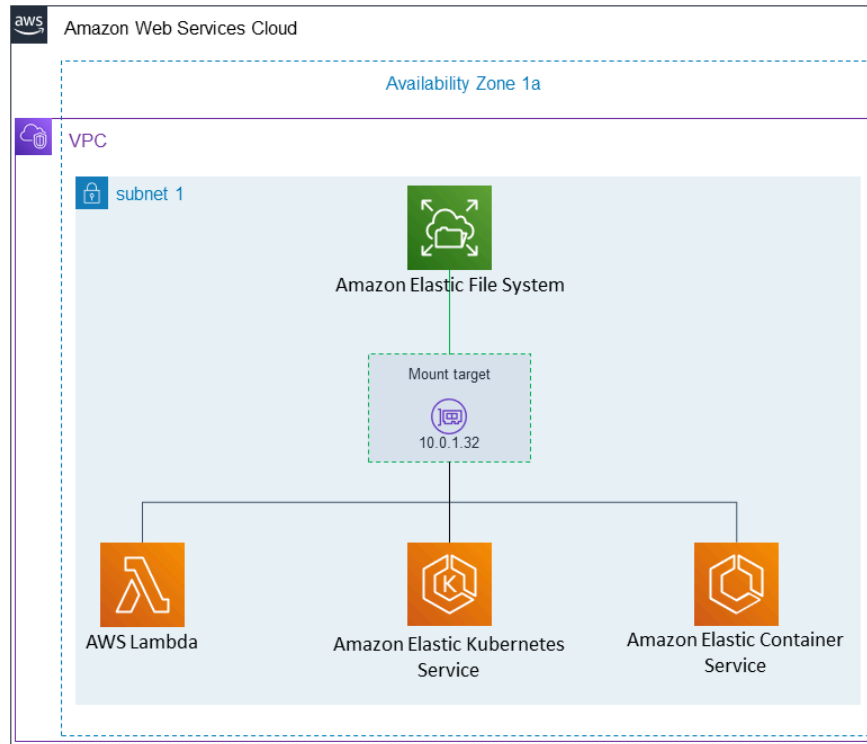
```
us-east-1a.fs-abc123def456a7890.efs.us-east-1.amazonaws.com:/ efs-one-zone nfs4  
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0  
0
```

Pour plus d'informations sur la façon de Modifier le fichier `/etc/fstab` et sur les valeurs utilisées dans cette commande, consultez [Montage automatique des systèmes de fichiers EFS](#).

Montage de systèmes de fichiers dotés d'un système de fichiers One Zone sur d'autres instances AWS de calcul

Lorsque vous utilisez un système de fichiers One Zone avec Amazon Elastic Container Service, Amazon Elastic Kubernetes Service AWS Lambda ou, vous devez configurer le service pour utiliser

la même zone de disponibilité que celle dans laquelle se trouve le système de fichiers EFS, comme illustré ci-dessous et décrit dans les sections suivantes.



Connexion depuis Amazon Elastic Container Service

Vous pouvez utiliser les systèmes de fichiers EFS avec Amazon ECS pour partager les données du système de fichiers entre votre flotte d'instances de conteneurs afin que vos tâches aient accès au même stockage persistant, quelle que soit l'instance sur laquelle elles aboutissent. Pour utiliser les systèmes de fichiers EFS One Zone avec Amazon ECS, vous devez choisir uniquement des sous-réseaux situés dans la même zone de disponibilité que votre système de fichiers lors du lancement de votre tâche. Pour plus d'informations, veuillez consulter la rubrique [Volumes Amazon EFS](#) dans le Guide du développeur Amazon Elastic Container Service.

Connexion depuis Amazon Elastic Kubernetes Service

Lorsque vous montez un système de fichiers One Zone à partir d'Amazon EKS, vous pouvez utiliser le pilote Amazon EFS [Container Storage Interface](#) (CSI), qui prend en charge les points d'accès EFS, pour partager un système de fichiers entre plusieurs pods d'un cluster Amazon EKS ou Kubernetes autogéré. Le pilote Amazon EFS CSI est installé dans la pile Fargate. Lorsque vous utilisez le pilote Amazon EFS CSI avec les systèmes de fichiers EFS One Zone, vous pouvez utiliser `nodeSelector`

cette option lors du lancement de votre pod pour vous assurer qu'il est planifié dans la même zone de disponibilité que votre système de fichiers.

Connexion depuis AWS Lambda

Vous pouvez utiliser Amazon EFS AWS Lambda pour partager des données entre des invocations de fonctions, lire de gros fichiers de données de référence et écrire le résultat d'une fonction dans un magasin persistant et partagé. Lambda connecte de manière sécurisée les instances de fonction aux cibles de montage EFS situées dans la même zone de disponibilité et le même sous-réseau. Lorsque vous utilisez Lambda avec des systèmes de fichiers Zone unique, configurez votre fonction pour lancer des invocations dans des sous-réseaux situés dans la même Zone de disponibilité que votre système de fichiers.

Montage avec autorisation IAM

Pour monter votre système de fichiers EFS sur des instances Linux à l'aide de l'autorisation AWS Identity and Access Management (IAM), utilisez l'assistant de montage EFS. Pour plus d'informations sur l'utilisation d'une autorisation IAM pour les clients NFS, consultez [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#).

Vous devez créer un répertoire à utiliser comme point de montage du système de fichiers dans les sections suivantes. Vous pouvez utiliser la commande suivante pour créer un répertoire `efs` de points de Montage :

```
sudo mkdir efs
```

Vous pouvez ensuite remplacer les instances de *efs-mount-point* par `efs`.

Montage avec IAM à l'aide d'un profil d' EC2 instance

Si vous effectuez un montage avec une autorisation IAM sur une EC2 instance Amazon dotée d'un profil d'instance, utilisez les options de `iam` montage `tls` et indiquées ci-dessous.

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

Pour effectuer un montage automatique avec l'autorisation IAM sur une EC2 instance dotée d'un profil d'instance, ajoutez la ligne suivante au `/etc/fstab` fichier de l' EC2 instance.

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

Montage avec IAM à l'aide d'un profil nommé

Vous pouvez effectuer le montage avec l'autorisation IAM à l'aide des informations d'identification IAM situées dans le fichier AWS CLI d'informations d'identification ou dans le fichier `~/.aws/credentials` de AWS CLI configuration. `~/.aws/config` Si "awsprofile" n'est pas spécifié, le profil par défaut (« default ») est utilisé.

Pour procéder à un Montage avec autorisation IAM sur une instance Linux à l'aide d'un fichier d'informations d'identification, utilisez les options de Montage `tls`, `awsprofile`, and `iam`, présentées ci-dessous.

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

Pour effectuer un montage automatique avec l'autorisation IAM sur une instance Linux à l'aide d'un fichier d'informations d'identification, ajoutez la ligne suivante au `/etc/fstab` fichier de l' EC2 instance.

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

Montage avec points d'accès EFS

Vous ne pouvez Monter un système de fichiers EFS avec un point d'accès EFS qu'en utilisant l'aide au Montage EFS.

Note

Vous devez configurer une ou plusieurs cibles de Montage pour votre système de fichiers lorsque vous Montez un système de fichiers à l'aide de points d'accès EFS.

Lorsque vous Montez un système de fichiers à l'aide d'un point d'accès, la commande Mount inclut l'option de Montage `access-point-id` et `tls`, en plus des options de Montage standard. Voici un exemple ci-dessous.

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

Pour monter automatiquement un système de fichiers à l'aide d'un point d'accès, ajoutez la ligne suivante au `/etc/fstab` fichier de l' EC2 instance.

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

Pour plus d'informations sur les points d'accès EFS, consultez [Utilisation des points d'accès](#).

Montage d'EFS sur plusieurs EC2 instances

Vous pouvez monter des systèmes de fichiers EFS sur plusieurs EC2 instances Amazon à distance et en toute sécurité sans avoir à vous connecter aux instances à l'aide de la commande AWS Systems Manager Run. Pour plus d'informations sur AWS Systems Manager Run Command, voir [AWS Systems Manager Run Command](#) dans le Guide de AWS Systems Manager l'utilisateur. Les conditions préalables suivantes sont requises avant de Monter des systèmes de fichiers EFS à l'aide de cette méthode :

1. Les EC2 instances sont lancées avec un profil d'instance qui inclut la politique AmazonElasticFileSystemsUtils d'autorisations. Pour de plus amples informations, veuillez consulter [Étape 1 : Configurez un profil d'instance \(IAM\) avec les autorisations requises](#).
2. La version 1.28.1 ou ultérieure du client Amazon EFS (amazon-efs-utils package) est installée sur les EC2 instances. Vous pouvez utiliser AWS Systems Manager pour installer automatiquement le package sur vos instances. Pour de plus amples informations, veuillez consulter [Étape 2 : Configuration d'une association utilisée par State Manager](#).

Pour monter plusieurs systèmes de fichiers EFS sur plusieurs EC2 instances à l'aide de la console

1. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
2. Dans le panneau de navigation, choisissez Fonctionnalité Exécuter la commande.
3. Choisissez Run a Command.
4. Entrez **AWS-RunShellScript** dans le champ de recherche des Commandes.
5. Sélectionnez AWS- RunShellScript.
6. Dans Paramètres de commande, entrez la commande de Montage à utiliser pour chaque système de fichiers EFS que vous souhaitez Monter. Par exemple :

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

Pour plus d'informations sur les commandes de Montage EFS à l'aide du client Amazon EFS, consultez [Montage sur des instances EC2 Linux à l'aide de l'assistant de montage EFS](#) ou [Montage sur des instances EC2 Mac à l'aide de l'assistant de montage EFS](#).

7. Sélectionnez les EC2 instances AWS Systems Manager gérées cibles sur lesquelles vous souhaitez exécuter la commande.
8. Effectuez les autres réglages supplémentaires que vous souhaitez. Choisissez ensuite Exécuter pour exécuter la commande et Monter les systèmes de fichiers EFS spécifiés dans la commande.

Au Moment de l'exécution de la commande, vous pouvez consulter son état dans l'historique des commandes.

Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC

Vous pouvez monter votre système de fichiers EFS à l'aide de l'autorisation IAM pour les clients NFS et les points d'accès EFS à l'aide de l'assistant de montage EFS. Par défaut, l'assistant de Montage EFS utilise le service de nom de domaine (DNS) pour résoudre l'adresse IP de votre cible de Montage EFS. Si vous Montez le système de fichiers à partir d'un autre compte ou d'un autre VPC, vous devez résoudre manuellement la cible de Montage EFS.

Vous trouverez ci-dessous des instructions permettant de déterminer l'adresse IP appropriée à la cible de Montage EFS à utiliser pour votre client NFS. Vous trouverez également des instructions permettant de configurer le client de sorte à Monter le système de fichiers EFS à l'aide de cette adresse IP.

Rubriques

- [Montage de systèmes de fichiers EFS depuis un autre Compte AWS](#)
- [Montage de systèmes de fichiers EFS depuis un autre VPC](#)

Montage de systèmes de fichiers EFS depuis un autre Compte AWS

Grâce au partage VPCs, vous pouvez monter un système de fichiers EFS appartenant à l'un Compte AWS d'entre eux à partir d' EC2 instances Amazon appartenant à un autre Compte AWS. Pour plus d'informations sur la configuration d'un VPC partagé, consultez [Partager votre VPC avec d'autres comptes dans le guide de peering](#) Amazon VPC.

Après avoir configuré le partage VPC, les EC2 instances peuvent monter le système de fichiers EFS à l'aide de la résolution des noms du système de noms de domaine (DNS) ou de l'assistant de montage EFS. Nous vous recommandons d'utiliser l'assistant de Montage EFS pour Monter vos systèmes de fichiers EFS.

Montage de systèmes de fichiers EFS depuis un autre VPC

Lorsque vous utilisez une connexion d'appairage VPC ou une passerelle de transit pour vous connecter, les EC2 instances VPCs Amazon situées dans un VPC peuvent accéder aux systèmes de fichiers EFS d'un autre VPC, même s'ils appartiennent à des comptes différents. VPCs

Vous ne pouvez pas utiliser la résolution de noms DNS pour les points de montage EFS d'un autre VPC. Pour monter votre système de fichiers EFS, utilisez l'adresse IP des points de montage dans la zone de disponibilité correspondante.

Vous pouvez également utiliser Amazon Route 53 comme service DNS. Dans Route 53, vous pouvez résoudre les adresses IP cibles du montage EFS à partir d'un autre VPC en créant une zone hébergée privée et un ensemble d'enregistrements de ressources. Pour plus d'informations sur la procédure à suivre, consultez la section [Travailler avec des zones hébergées privées](#) dans le manuel Amazon Route 53 Developer Guide.

Prérequis

Avant d'utiliser la procédure suivante, procédez comme suit :

- Installez le client Amazon EFS, qui fait partie de l'ensemble d'utilitaires `amazon-efs-utils` de l'instance de calcul sur laquelle vous Montez le système de fichiers EFS. Vous utilisez l'assistant de Montage EFS, inclus dans `amazon-efs-utils`, pour Monter le système de fichiers. Pour obtenir des instructions sur l'installation de l'ensemble d'outils `amazon-efs-utils`, veuillez consulter [Installation du client Amazon EFS](#).
- Autorisez l'action `ec2:DescribeAvailabilityZones` dans la politique IAM pour le rôle IAM que vous avez attaché à l'instance. Nous vous recommandons d'associer la politique AWS gérée `AmazonElasticFileSystemsUtils` à une entité IAM afin de fournir les autorisations nécessaires à l'entité.
- Lors du montage depuis un autre Compte AWS, mettez à jour la politique de ressources du système de fichiers pour autoriser `elasticfilesystem:DescribeMountTargetaction` pour l'ARN principal de l'autre Compte AWS. Par exemple :

```
{
```

```
"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"
  }
]
```

Pour plus d'informations sur les stratégies de ressources de système de fichiers EFS, consultez [Politiques basées sur les ressources au sein d'Amazon EFS](#).

- Installez botocore. Le client EFS utilise botocore pour récupérer l'adresse IP cible du Montage lorsque le nom DNS du système de fichiers ne peut pas être résolu lors du Montage d'un système de fichiers dans un autre VPC. Pour plus d'informations, consultez [Installer botocore](#) dans le amazon-efs-utils fichier README.
- Configurez une connexion d'appairage de VPC ou une passerelle de transit de VPC.

Vous connectez le VPC du client et le VPC de votre système de fichiers EFS à l'aide d'une connexion d'appairage de VPC ou d'une passerelle de transit de VPC. Lorsque vous utilisez une connexion d'appairage VPC ou une passerelle de transit pour vous connecter, les EC2 instances VPCs Amazon situées dans un VPC peuvent accéder aux systèmes de fichiers EFS d'un autre VPC, même s'ils appartiennent à des comptes différents. VPCs

Une passerelle de transit est un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations sur l'utilisation des passerelles de transit de VPC, consultez [Démarrez avec les passerelles de transit](#) dans le Guide des passerelles de transit Amazon VPC.

Une connexion d'appairage VPC est une connexion réseau entre deux VPCs. Ce type de connexion vous permet d'acheminer le trafic entre eux à l'aide d'adresses privées du protocole Internet version 4 (IPv4) ou du protocole Internet version 6 (IPv6). Vous pouvez utiliser le peering VPC pour vous connecter au VPCs sein d'un même Région AWS système ou entre les deux. Régions AWS Pour plus d'informations sur l'appairage VPC, consultez [Qu'est-ce que l'appairage VPC ?](#) dans le Guide d'appairage Amazon VPC.

Pour garantir la haute disponibilité de votre système de fichiers, nous vous recommandons de toujours utiliser une adresse IP de cible de Montage EFS qui se trouve dans la même Zone de disponibilité que votre client NFS. Si vous Montez un système de fichiers EFS qui se trouve dans un autre compte, assurez-vous que le client NFS et la cible de Montage EFS possèdent le même ID de Zone de disponibilité. Ce critère s'applique car les noms d'AZ peuvent différer d'un compte à l'autre.

Pour Monter un système de fichiers EFS dans un autre VPC à l'aide d'IAM ou d'un point d'accès

1. Connectez-vous à votre EC2 instance. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Créez un répertoire dans lequel Monter le système de fichiers à l'aide de la commande suivante.

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

3. Pour Monter le système de fichiers avec une autorisation IAM, utilisez la commande suivante :

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

Pour de plus amples informations sur l'utilisation d'une autorisation IAM avec EFS, veuillez consulter [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#).

Pour Monter le système de fichiers à l'aide d'un point d'accès EFS, utilisez la commande suivante :

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

Pour plus d'informations sur les points d'accès EFS, consultez [Utilisation des points d'accès](#).

Montage de systèmes de fichiers EFS à partir d'un autre Région AWS

Si vous montez votre système de fichiers EFS à partir d'un autre VPC situé dans un autre système de fichiers Région AWS que le système de fichiers, vous devez modifier le `efs-utils.conf` fichier. Dans `/dist/efs-utils.conf`, recherchez la ligne suivante :

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

Décommentez la ligne et remplacez la valeur de l'ID de la région dans laquelle se trouve le système de fichiers, si ce n'est pas dans `us-east-1`.

Utilisation du système de fichiers réseau pour monter des systèmes de fichiers EFS

Découvrez ci-dessous comment installer le client NFS (Network File System) et comment monter votre système de fichiers Amazon EFS sur une EC2 instance Amazon. Vous trouverez également une explication de la commande `mount` et les options disponibles pour spécifier le nom DNS (Domain Name System) de votre système de fichiers dans la commande `mount`. En outre, vous découvrirez comment utiliser le fichier `fstab` pour remonter automatiquement votre système de fichiers après un redémarrage du système.

Note

Dans cette section, vous découvrirez comment monter votre système de fichiers Amazon EFS sans le `amazon-efs-utils` package. Pour utiliser le chiffrement des données en transit avec votre système de fichiers, vous devez monter votre système de fichiers avec le protocole TLS (Transport Layer Security). Pour ce faire, nous vous recommandons d'utiliser le `amazon-efs-utils` package. Pour de plus amples informations, veuillez consulter [Installation du client Amazon EFS](#).

Rubriques

- [Prérequis](#)
- [NFS Support](#)
- [Installation du client NFS](#)
- [Paramètres de montage NFS recommandés](#)
- [Montage sur Amazon EC2 avec un nom DNS](#)
- [Montage avec une adresse IP](#)

Prérequis

Avant de monter un système de fichiers, assurez-vous que vous répondez aux exigences suivantes :

- Créez, configurez et lancez vos AWS ressources connexes. Pour obtenir des instructions, veuillez consulter [Commencer à utiliser Amazon EFS](#).
- Créez des groupes de sécurité VPC pour vos EC2 instances Amazon et montez des cibles avec l'accès entrant et sortant requis. Pour de plus amples informations, veuillez consulter [Utilisation de groupes de sécurité VPC](#).

NFS Support

Amazon EFS prend en charge les protocoles Network File System versions 4.0 et 4.1 (NFSv4) lors du montage de vos systèmes de fichiers sur des EC2 instances Amazon. Bien que la NFSv4 version 2.0 soit prise en charge, nous vous recommandons d'utiliser la version NFSv4 .1. Le montage de votre système de fichiers Amazon EFS sur votre EC2 instance Amazon nécessite également un client NFS compatible avec le NFSv4 protocole que vous avez choisi. Les instances Amazon EC2 Mac exécutant macOS Big Sur ne prennent en charge que NFS v4.0.

Amazon EFS ne prend pas en charge l'option de Montage nconnect.

Note

Pour les versions 5.4.* du noyau Linux, le client NFS Linux utilise une valeur `read_ahead_kb` par défaut de 128 Ko. Nous recommandons d'augmenter cette valeur jusqu'à 15 Mo. Pour de plus amples informations, veuillez consulter [Optimisation de la taille NFS read_ahead_kb](#).

Afin d'obtenir des performances optimales et éviter divers bogues identifiés du client NFS, nous vous recommandons d'utiliser un noyau Linux récent. Si vous utilisez une distribution Linux d'entreprise, nous vous recommandons de procéder comme suit :

- Amazon Linux 2
- Amazon Linux 2017.09 ou version ultérieure
- Red Hat Enterprise Linux (et dérivés telles que CentOS) version 7 et versions ultérieures
- Ubuntu 16.04 LTS et les versions plus récentes
- SLES 12 Sp2 ou version ultérieure

Si vous utilisez une autre distribution ou un noyau personnalisé, nous recommandons la version 4.3 ou version ultérieure. Pour résoudre les problèmes liés à certaines versions d'AMI ou de noyau lors de l'utilisation d'Amazon EFS à partir d'une EC2 instance, consultez [Résolution des problèmes d'AMI et de noyau](#).

 Note

Le montage de systèmes de fichiers EFS avec EC2 des instances Amazon exécutant Microsoft Windows n'est pas pris en charge.

Installation du client NFS

Pour monter votre système de fichiers EFS sur votre EC2 instance Amazon, vous devez d'abord installer un client NFS. Pour vous connecter à votre EC2 instance et installer un client NFS, vous avez besoin du nom DNS public de l' EC2 instance et d'un nom d'utilisateur pour vous connecter. Le nom d'utilisateur de votre instance est généralement `ec2-user`.

Pour connecter votre EC2 instance et installer le client NFS

1. Connectez-vous à votre EC2 instance. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.

Le fichier de clé ne peut pas être visible publiquement pour SSH. Vous pouvez utiliser la commande `chmod 400 filename.pem` pour définir ces autorisations. Pour plus d'informations, consultez [Créer une paire de clés pour votre EC2 instance Amazon](#).

2. (Facultatif) Obtenez les mises à jour et redémarrez.

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

3. Après le redémarrage, reconnectez-vous à votre EC2 instance.
4. Installez le client NFS.

Si vous utilisez une AMI Amazon Linux ou Red Hat Linux, installez le client NFS avec la commande suivante.

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

Si vous utilisez une EC2 AMI Amazon Ubuntu, installez le client NFS à l'aide de la commande suivante.

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

5. Démarrez le service NFS à l'aide des commandes suivantes. Pour RHEL 7 :

```
$ sudo service nfs start
```

Pour RHEL 8 :

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

6. Vérifiez que le service NFS a démarré, comme suit.

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

Si vous utilisez un noyau personnalisé (c'est-à-dire si vous créez une AMI personnalisée), vous devez inclure au minimum le module noyau client NFSv4 .1 et l'assistant de montage en NFS4 espace utilisateur approprié.

Note

Si vous choisissez Amazon Linux AMI 2016.03.0 ou Amazon Linux AMI 2016.09.0 lors du lancement de votre instance EC2 Amazon, vous n'avez pas besoin de l'`nfs-utils` installer car elle est déjà incluse dans l'AMI par défaut.

Ensuite : Montage de votre système de fichiers

Utilisez l'une des procédures suivantes pour monter votre système de fichiers.

- [Montage sur Amazon EC2 avec un nom DNS](#)
- [Montage avec une adresse IP](#)
- [Montage automatique des systèmes de fichiers EFS](#)

Paramètres de montage NFS recommandés

Nous vous recommandons d'utiliser les valeurs suivantes pour les options de montage sous Linux :

- `noresvport` – Indique au client NFS d'utiliser un nouveau port source TCP (Transmission Control Protocol) non privilégié lorsqu'une connexion réseau est rétablie. Les logiciels clients NFS inclus dans les anciennes versions du noyau Linux (versions v5.4 et antérieures) ont un comportement qui fait que les clients NFS tentent de se reconnecter sur le même port source TCP en cas de déconnexion. Ce comportement n'est pas conforme à la spécification RFC TCP et peut empêcher ces clients de rétablir rapidement les connexions à un système de fichiers EFS.

L'utilisation de l'option `noresvport` permet de garantir que les clients NFS se reconnectent de manière transparente à votre système de fichiers EFS, tout en maintenant une disponibilité ininterrompue lors de la reconnexion après un événement de restauration du réseau.

Important

Nous vous recommandons vivement d'utiliser l'option de montage `noresvport` pour garantir la disponibilité ininterrompue de votre système de fichiers EFS après une reconnexion ou un événement de restauration du réseau.

Envisagez de monter votre système de fichiers à l'aide de l'[assistant de montage EFS](#). L'assistant de montage EFS utilise des options de montage NFS optimisées pour les systèmes de fichiers Amazon EFS.

- `rsz=1048576` – Définit le nombre maximal d'octets de données que le client NFS peut recevoir pour chaque demande READ du réseau. Cette valeur s'applique lors de la lecture des données à partir d'un fichier sur un système de fichiers EFS. Nous vous recommandons d'utiliser la plus grande taille possible (jusqu'à 1048576) afin d'éviter une baisse de performances.
- `wsz=1048576` – Définit le nombre maximal d'octets de données que le client NFS peut envoyer pour chaque demande WRITE du réseau. Cette valeur s'applique lors de l'écriture de données sur

un fichier d'un système de fichiers EFS. Nous vous recommandons d'utiliser la plus grande taille possible (jusqu'à 1048576) afin d'éviter une baisse de performances.

- **hard** – Définit le comportement de récupération du client NFS après qu'une demande NFS a expiré, de sorte que les demandes NFS sont relancées indéfiniment jusqu'à ce que le serveur réponde. Nous vous recommandons d'utiliser l'option de Montage physique (**hard**) pour garantir l'intégrité des données. Si vous utilisez un Montage **soft**, définissez le paramètre **timeo** sur au Moins 150 décisecondes (15 secondes). Vous minimiserez ainsi le risque de corruption des données inhérent aux Montages logiciels.
- **timeo=600** – Définit la valeur de délai d'expiration que le client NFS utilise pour attendre une réponse avant de relancer une demande NFS sur 600 décisecondes (60 secondes). Si vous devez Modifier le paramètre de délai (**timeo**), nous vous recommandons d'utiliser une valeur d'au Moins 150, ce qui équivaut à 15 secondes. Vous éviterez ainsi une baisse de performances.
- **retrans=2** – Définit sur 2 le nombre de fois que le client NFS essaie une demande avant de tenter une action de récupération.
- **_netdev** – Lorsque cette option est présente dans `/etc/fstab`, elle empêche le client d'essayer de monter le système de fichiers EFS tant que le réseau n'a pas été activé.
- **nofail**— Si votre EC2 instance doit démarrer quel que soit l'état de votre système de fichiers EFS monté, ajoutez l'**nofail**option à l'entrée de votre système de fichiers dans votre `/etc/fstab` fichier.

Si vous n'utilisez pas les valeurs par défaut précédentes, vous devez être conscient des points suivants :

- En général, évitez de définir d'autres options de montage différentes des valeurs par défaut, ce qui peut entraîner une réduction des performances et d'autres problèmes. Par exemple, la modification des tailles tampon de lecture ou d'écriture, ou la désactivation de la mise en cache d'attribut, peuvent entraîner une réduction des performances.
- Amazon EFS ignore les ports source. Si vous modifiez les ports source Amazon EFS, cela n'a aucun effet.
- Amazon EFS ne prend pas en charge l'option de montage **nconnect**.
- Amazon EFS ne prend en charge aucune des variantes sécurité Kerberos. Par exemple, la commande de Montage suivante échoue.

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

- Nous vous recommandons de Monter votre système de fichiers à l'aide de son nom DNS. Ce nom correspond à l'adresse IP de la cible de montage Amazon EFS située dans la même zone de disponibilité que votre EC2 instance Amazon. Si vous utilisez une cible de montage dans une zone de disponibilité différente de celle de votre EC2 instance Amazon, vous devez payer des EC2 frais standard pour les données envoyées entre les zones de disponibilité. De même, vous pouvez constater des latences accrues pour les opérations de système de fichiers.
- Pour plus d'options de montage et des explications détaillées sur les valeurs par défaut, consultez la documentation Linux.

Montage sur Amazon EC2 avec un nom DNS

Note

Avant de monter votre système de fichiers, vous devez ajouter une règle au groupe de sécurité cible de montage qui autorise l'accès NFS entrant depuis le groupe de EC2 sécurité. Pour de plus amples informations, veuillez consulter [Utilisation de groupes de sécurité VPC](#).

- Nom DNS du système de fichiers – Le nom DNS du système de fichiers constitue votre option de montage la plus simple. Le nom DNS du système de fichiers correspond automatiquement à l'adresse IP de la cible de montage dans la zone de disponibilité de l' EC2 instance Amazon connectée. Vous pouvez obtenir le nom DNS à partir de la console, ou si vous avez l'ID du système de fichiers, vous pouvez le construire selon la convention suivante.

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

Note

La résolution DNS pour les noms DNS du système de fichiers nécessite que le système de fichiers Amazon EFS comporte une cible de montage dans la même zone de disponibilité que l'instance client.

- À l'aide du nom DNS du système de fichiers, vous pouvez monter un système de fichiers sur votre instance Amazon EC2 Linux à l'aide de la commande suivante.

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

- À l'aide du nom DNS du système de fichiers, vous pouvez monter un système de fichiers sur votre instance Amazon EC2 Mac exécutant une version compatible de macOS (Big Sur, Monterey, Ventura) à l'aide de la commande suivante.

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

Important

Pour vous connecter correctement `mountport=2049` au système de fichiers EFS lors du montage sur EC2 Mac, vous devez utiliser des instances exécutant des versions compatibles de macOS.

- Nom DNS de la cible de montage – En décembre 2016, nous avons introduit les noms DNS pour les systèmes de fichiers. Nous continuons à fournir un nom DNS pour chaque cible de montage de zone de disponibilité à des fins de compatibilité descendante. La forme générique du nom DNS de la cible de montage est la suivante.

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

Note

La résolution des noms DNS de la cible de montage dans les zones de disponibilité est prise en charge.

Dans certains cas, il se peut que vous supprimiez une cible de montage, puis en créiez une nouvelle dans la même zone de disponibilité. Dans ce cas, le nom DNS de cette nouvelle cible de montage de cette zone de disponibilité est le même que le nom DNS de l'ancienne cible de montage.

Vous pouvez afficher et copier les commandes exactes pour monter votre système de fichiers dans la boîte de dialogue Attacher.

Pour afficher les commandes de montage de votre système de fichiers

1. Dans la console Amazon EFS, choisissez le système de fichiers que vous souhaitez monter pour afficher sa page de détails.
2. Pour afficher les commandes de Montage à utiliser pour ce système de fichiers, choisissez Attacher en haut à droite.

L'écran Attacher affiche les commandes exactes à utiliser pour monter le système de fichiers.

3. La vue Montage via DNS par défaut montre la commande permettant de monter le système de fichiers en utilisant le nom DNS du système de fichiers lors du montage avec l'assistant de montage EFS ou un client NFS.

Pour obtenir la liste des Région AWS systèmes compatibles avec Amazon EFS, consultez [Amazon Elastic File System](#) dans le Références générales AWS.

Pour utiliser un nom DNS dans la commande mount, les conditions suivantes doivent être vérifiées :

- L' EC2 instance de connexion doit se trouver dans un VPC et doit être configurée pour utiliser le serveur DNS fourni par Amazon. Pour plus d'informations sur le serveur DNS Amazon, consultez les [ensembles d'options DHCP dans Amazon VPC](#) dans le guide de l'utilisateur Amazon VPC.
- La résolution DNS et les noms d'hôte DNS doivent être activés sur le VPC de l' EC2 instance de connexion. Pour plus d'informations, consultez la section [Attributs DNS de votre VPC](#) dans le guide de l'utilisateur Amazon VPC.
- L' EC2 instance de connexion doit se trouver dans le même VPC que le système de fichiers EFS. Pour plus d'informations sur l'accès et le montage d'un système de fichiers à partir d'un autre emplacement ou d'un autre VPC, consultez [Prérequis](#) et [Tutoriel : monter un système de fichiers à partir d'un autre VPC](#) .

 Note

Nous vous recommandons d'attendre 90 secondes après la création d'une cible de montage pour monter votre système de fichiers. Cette attente permet aux enregistrements DNS de se propager entièrement Région AWS là où se trouve le système de fichiers.

Montage avec une adresse IP

Au lieu de monter votre système de fichiers Amazon EFS avec le nom DNS, les EC2 instances Amazon peuvent monter un système de fichiers en utilisant l'adresse IP d'une cible de montage. Le montage par adresse IP fonctionne dans les environnements où le DNS est désactivé, par exemple lorsque les noms VPCs d'hôte DNS sont désactivés.

Il est aussi possible de configurer le montage d'un système de fichiers à l'aide de l'adresse IP de la cible de montage comme option de secours pour les applications configurées pour le montage de système de fichiers à l'aide de son nom DNS par défaut. Lorsque vous vous connectez à une adresse IP cible de montage, EC2 les instances doivent être montées en utilisant l'adresse IP cible de montage dans la même zone de disponibilité que l'instance de connexion.

Vous pouvez afficher et copier les commandes exactes pour Monter votre système de fichiers dans la boîte de dialogue Attacher.

Note

Avant de monter votre système de fichiers, vous devez ajouter une règle pour le groupe de sécurité cible de montage afin d'autoriser l'accès NFS entrant depuis le groupe de EC2 sécurité. Pour de plus amples informations, veuillez consulter [Utilisation de groupes de sécurité VPC](#).

Pour afficher et copier les commandes exactes pour monter votre système de fichiers EFS à l'aide de l'adresse IP d'une cible du montage

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Dans la console Amazon EFS, choisissez le système de fichiers que vous souhaitez Monter pour afficher sa page de détails.
3. Pour afficher les commandes de Montage à utiliser pour ce système de fichiers, choisissez Attacher en haut à droite.
4. L'écran Attacher affiche les commandes exactes à utiliser pour monter le système de fichiers.

Choisissez Monter via IP pour afficher la commande permettant de monter le système de fichiers à l'aide de l'adresse IP d'une cible du montage dans la zone de disponibilité sélectionnée avec un client NFS.

- En utilisant l'adresse IP d'une cible de montage dans la mount commande, vous pouvez monter un système de fichiers sur votre instance Amazon EC2 Linux à l'aide de la commande suivante.

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

- En utilisant l'adresse IP d'une cible de montage dans la mount commande, vous pouvez monter un système de fichiers sur votre instance Amazon EC2 Mac exécutant macOS Big Sur à l'aide de la commande suivante.

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

Important

Vous devez utiliser mountport=2049 afin de vous connecter correctement au système de fichiers EFS lors du montage sur des instances EC2 Mac exécutant macOS Big Sur.

Montage avec une adresse IP dans AWS CloudFormation

Vous pouvez également monter votre système de fichiers à l'aide d'une adresse IP dans un AWS CloudFormation modèle. Pour plus d'informations, consultez [storage-efs-mountfilesystem-ip-addr.config](#) dans le référentiel `awsdocs/elastic-beanstalk-samples` pour les fichiers de configuration fournis par la communauté sur GitHub

Montage automatique des systèmes de fichiers EFS

Vous pouvez utiliser l'assistant de montage EFS ou NFS pour configurer une EC2 instance Amazon afin de monter automatiquement un système de fichiers EFS au démarrage de l'instance.

- Utilisation de l'assistant de Montage EFS
 - Joignez un système de fichiers EFS lorsque vous créez une nouvelle instance EC2 Linux à l'aide de l'assistant de EC2 lancement d'instance.
 - Mettez à jour le EC2 `/etc/fstab` fichier avec une entrée pour le système de fichiers EFS.

- Utilisation de [NFS sans l'assistant de montage EFS pour mettre à jour](#) le EC2 `/etc/fstab` fichier, pour les instances EC2 Linux et Mac.

 Note

L'assistant de montage EFS ne prend pas en charge le montage automatique sur les instances EC2 Mac exécutant macOS Big Sur ou Monterey. Vous pouvez plutôt utiliser [NFS pour configurer le fichier `/etc/fstab` sur une instance EC2 Mac afin de monter automatiquement un système de fichiers](#) EFS.

Rubriques

- [Activation du montage automatique sur les nouvelles instances EC2 Linux](#)
- [Activation du montage automatique sur les instances EC2 Linux existantes](#)
- [Activation du montage automatique sur des instances EC2 Linux ou Mac à l'aide de NFS](#)

Activation du montage automatique sur les nouvelles instances EC2 Linux

Lorsque vous créez une nouvelle instance EC2 Linux à l'aide de l'assistant de EC2 lancement d'instance Amazon, vous pouvez la configurer pour monter automatiquement votre système de fichiers Amazon EFS. L' EC2 instance monte le système de fichiers automatiquement dès le lancement de l'instance et également chaque fois qu'elle redémarre.

Cette méthode utilise l'assistant de montage EFS pour monter le système de fichiers et mettre à jour le fichier `/etc/fstab` sur l'instance. EC2 L'assistant de Montage fait partie de l'ensemble d'outils [amazon-efs-utils](#).

 Note

Les systèmes de fichiers EFS ne prennent pas en charge le montage sur des instances EC2 Mac exécutant macOS Big Sur ou Monterey au lancement de l'instance.

 Note

Vous ne pouvez pas utiliser Amazon EFS avec des instances basées sur Microsoft Windows EC2.

Avant de lancer et de vous connecter à une EC2 instance, vous devez créer une paire de clés. Pour plus d'informations, consultez les [sections paires de EC2 clés Amazon et EC2 instances Amazon](#) dans le guide de EC2 l'utilisateur Amazon pour créer une paire de clés.

Pour configurer votre EC2 instance afin de monter automatiquement un système de fichiers EFS au lancement

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Launch Instances (Lancer les instances).
3. Dans Étape 1 : Sélectionnez un Amazon Machine Image (AMI) (Étape 1 : Choisir une Amazon Machine Image (AMI)), localisez une AMI Amazon Linux en haut de la liste et choisissez Select (Sélectionner).
4. Dans Étape 2 : Sélectionnez un type d'Instance (Étape 2 : Choisir un type d'instance), choisissez Next: Configure Instance Details (Suivant : Configurer les détails de l'instance).
5. Dans Étape 3: Configure Instance Details (Étape 3 : Configurer les détails de l'instance), fournissez les informations suivantes :
 - Pour Réseau, choisissez l'entrée pour le même VPC que celui dans se trouve le système de fichiers EFS que vous Montez.
 - Pour Sous-réseau, choisissez un sous-réseau par défaut dans n'importe quelle Zone de disponibilité.
 - Pour Système de fichiers, choisissez le système de fichiers EFS que vous souhaitez Monter. Le chemin indiqué à côté de l'ID du système de fichiers est le point de montage que l' EC2 instance utilisera, que vous pouvez modifier.
 - Sous Détails avancés, les données utilisateur sont générées automatiquement et comprennent les commandes nécessaires pour Monter les systèmes de fichiers EFS que vous avez spécifiés sous Systèmes de fichiers.
6. Choisissez Next: Add Storage (Suivant : Ajouter le stockage).
7. Choisissez Next: Add Tags (Suivant : Ajouter des balises).

8. Nommez votre instance et choisissez Next: Configure Security Group (Suivant : Configurer le groupe de sécurité).
9. Dans Step 6 : Configure Security Group (Étape 6 : Configurer le groupe de sécurité), définissez Assign a security group (Attribuer un groupe de sécurité) sur Select an existing security group (Sélectionner un groupe de sécurité existant). Choisissez le groupe de sécurité par défaut pour vous assurer que celui-ci peut accéder à votre système de fichiers EFS.

Vous ne pouvez pas accéder à votre EC2 instance via Secure Shell (SSH) à l'aide de ce groupe de sécurité. Pour l'accès par SSH, vous pouvez ultérieurement Modifier la sécurité par défaut et ajouter une règle pour autoriser SSH ou un nouveau groupe de sécurité qui autorise SSH. Vous pouvez utiliser les paramètres suivants :

- Type : SSH
 - Protocole : TCP
 - Port Range (Plage de ports) : 22
 - Source : N'importe où 0.0.0.0/0
10. Choisissez Review and Launch.
 11. Choisissez Lancer.
 12. Activez la case à cocher pour la paire de clés que vous avez créée, puis choisissez Launch Instances (Lancer des instances).

Votre EC2 instance est désormais configurée pour monter le système de fichiers EFS au lancement et chaque fois qu'il est redémarré.

Activation du montage automatique sur les instances EC2 Linux existantes

Le fichier `/etc/fstab` contient des informations sur les systèmes de fichiers. La commande `mount -a`, qui s'exécute au démarrage de l'instance, Monte tous les systèmes de fichiers répertoriés dans `/etc/fstab`. Dans cette procédure, vous allez le mettre à jour manuellement `/etc/fstab` sur une instance Amazon EC2 Linux afin que l'instance utilise l'assistant de montage EFS pour remonter automatiquement un système de fichiers EFS au redémarrage de l'instance.

Note

Les systèmes de fichiers EFS ne prennent pas en charge le montage automatique à l'`/etc/fstab` aide de l'assistant de montage EFS sur les instances EC2 Mac exécutant macOS

Big Sur ou Monterey. Au lieu de cela, vous pouvez utiliser [NFS /etc/fstab](#) pour monter automatiquement votre système de fichiers sur des instances EC2 Mac exécutant macOS Big Sur et Monterey.

Cette méthode utilise l'assistant de Montage EFS pour Monter le système de fichiers. L'assistant de Montage fait partie de l'ensemble d'outils `amazon-efs-utils`.

Les `amazon-efs-utils` outils peuvent être installés sur Amazon Linux et Amazon Linux 2 Amazon Machine Images (AMIs). Pour plus d'informations sur `amazon-efs-utils`, consultez [Installation du client Amazon EFS](#). Si vous utilisez une autre distribution Linux, telle que Red Hat Enterprise Linux (RHEL), générez et installez manuellement `amazon-efs-utils`. Pour de plus amples informations, veuillez consulter [Pour installer le client Amazon EFS sur d'autres distributions Linux](#).

Prérequis

Les conditions suivantes doivent être remplies pour que vous puissiez mettre en œuvre cette procédure avec succès :

- Vous avez déjà créé le système de fichiers EFS que vous souhaitez remonter automatiquement. Pour de plus amples informations, veuillez consulter [Création rapide à l'aide de la console](#).
- Vous avez déjà créé l'instance EC2 Linux que vous souhaitez configurer pour remonter automatiquement un système de fichiers EFS.
- L'assistant de montage EFS est installé sur l'instance EC2 Linux. Pour de plus amples informations, veuillez consulter [Installation du client Amazon EFS](#).

Mettez à jour le fichier `/etc/fstab`

Procédez comme suit pour mettre à jour le fichier `/etc/fstab` sur une instance EC2 Linux afin que celle-ci utilise l'assistant de montage EFS pour remonter automatiquement un système de fichiers EFS au redémarrage de l'instance.

Pour mettre à jour le fichier `/etc/fstab` sur votre instance EC2

1. Connectez-vous à votre EC2 instance. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Ouvrez le fichier `/etc/fstab` dans un éditeur.

3. Pour un Montage automatique à l'aide d'une autorisation IAM ou d'un point d'accès EFS :

- Pour effectuer un montage automatique avec l'autorisation IAM sur une EC2 instance dotée d'un profil d'instance, ajoutez la ligne suivante au `/etc/fstab` fichier.

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

- Pour procéder automatiquement à un Montage avec autorisation sur une instance Linux à l'aide d'un fichier d'informations d'identification, ajoutez la ligne suivante au fichier `/etc/fstab`.

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

- Pour procéder automatiquement au Montage d'un système de fichiers à l'aide d'un point d'accès EFS, ajoutez la ligne suivante au fichier `/etc/fstab`.

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

Warning

Utilisez l'option `_netdev`, utilisée pour identifier les systèmes de fichiers réseau lors du Montage automatique de votre système de fichiers. Si elle `_netdev` est absente, il est possible que votre EC2 instance cesse de répondre. Cela s'explique par le fait que les systèmes de fichiers réseau doivent être initialisés après le démarrage de la mise en réseau de l'instance de calcul. Pour de plus amples informations, veuillez consulter [Le montage automatique échoue et l'instance ne répond pas](#).

Pour plus d'informations, consultez [Montage avec autorisation IAM](#) et [Montage avec points d'accès EFS](#).

4. Enregistrez les Modifications dans le fichier.

Note

Dans certains cas, il se peut que votre EC2 instance doive démarrer quel que soit l'état de votre système de fichiers EFS monté. Dans ce cas, ajoutez l'option `nofail` à l'entrée de votre système de fichiers dans votre fichier `/etc/fstab`.

La ligne de code que vous avez ajoutée dans le fichier `/etc/fstab` effectue les opérations suivantes.

Champ	Description
<i>file-system-id</i> :/	L'ID de votre système de fichiers EFS. Vous pouvez obtenir cet ID depuis la console ou par programmation à partir de la CLI ou d'un AWS SDK.
<i>efs-mount-point</i>	Point de montage du système de fichiers EFS sur votre EC2 instance.
<code>efs</code>	Type de système de fichiers. Lorsque vous utilisez l'assistant de Montage, ce type est toujours <code>efs</code> .
<code>mount options</code>	Options de Montage pour le système de fichiers. Il s'agit d'une liste séparée par des virgules des options suivantes : <code>_netdev</code> – Cette option indique au système d'exploitation que le système de fichiers réside sur un périphérique qui nécessite l'accès au réseau. Cette option empêche l'instance de Monter le système de fichiers jusqu'à ce que le réseau a été activé sur le client. <code>noresvport</code> – Indique au client NFS d'utiliser un nouveau port source TCP (Transmission Control Protocol) lorsqu'une connexion réseau est rétablie. Cette utilisation permet de s'assurer que le système de fichiers EFS a une disponibilité ininterrompue après un événement de récupération du réseau. <code>tls</code> – Cette option active le chiffrement des données en transit. <code>iam</code>— Utilisez cette option pour effectuer un montage avec l'autorisation IAM sur une EC2 instance dotée d'un profil d'instance. L'utilisation de l'option de Montage <code>iam</code> nécessite également l'utilisation de

Champ	Description
	l'option <code>tls</code>. Pour de plus amples informations, veuillez consulter Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers. • <code>awsprofile= <i>namedprofile</i></code> – Utilisez cette option avec les options <code>iam</code> et <code>tls</code> pour procéder à un Montage avec autorisation IAM sur une instance Linux à l'aide d'un fichier d'informations d'identification. Pour plus d'informations sur les points d'accès EFS, consultez Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers. • <code>accesspoint= <i>access-point-id</i></code> – Utilisez cette option avec l'option <code>tls</code> pour procéder au Montage à l'aide d'un point d'accès EFS. Pour plus d'informations sur les points d'accès EFS, consultez Utilisation des points d'accès.
0	Une valeur différente de zéro indique que le système de fichiers doit être sauvegardé par dump. Pour EFS, cette valeur doit être 0.
0	Ordre dans lequel <code>fsck</code> vérifie les systèmes de fichiers au démarrage. Pour les systèmes de fichiers EFS, cette valeur doit être 0 pour indiquer que <code>fsck</code> ne doit pas s'exécuter au démarrage.

Activation du montage automatique sur des instances EC2 Linux ou Mac à l'aide de NFS

Utilisation de NFS sans l'assistant de montage EFS pour mettre à jour EC2 `/etc/fstab` le fichier Amazon, pour les instances EC2 Linux et Mac.

Pour mettre à jour le **`/etc/fstab`** fichier sur votre EC2 instance

1. Connectez-vous à votre EC2 instance. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Ouvrez le fichier `/etc/fstab` dans un éditeur.
3. Pour Monter automatiquement un système de fichiers à l'aide de NFS au lieu de l'aide au Montage EFS, ajoutez la ligne suivante au fichier `/etc/fstab`.
 - `file_system_id` Remplacez-le par l'ID du système de fichiers que vous montez.

- Remplacez *aws-region* par Région AWS celui dans lequel se trouve le système de fichiers, tel que `us-east-1`.
- Remplacez *mount_point* par le point de Montage du système de fichiers.

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

La ligne de code que vous avez ajoutée dans le fichier `/etc/fstab` effectue les opérations suivantes.

Champ	Description
<i>file-system-id</i> :/	L'ID de votre système de fichiers EFS. Vous pouvez obtenir cet ID depuis la console ou par programmation à partir de la CLI ou d'un AWS SDK.
<i>efs-mount-point</i>	Point de montage du système de fichiers EFS sur votre EC2 instance.
nfs4	Spécifie le type de système de fichiers.
mount options	Liste séparée par des virgules d'options de Montage pour le système de fichiers : • <code>nfsvers=4.1</code> — spécifie l'utilisation de NFS v4.1. • <code>rsiz=1048576</code> — Pour améliorer les performances, définit le nombre maximal d'octets de données que le client NFS peut recevoir pour chaque demande READ du réseau lors de la lecture de données à partir d'un fichier sur un système de fichiers EFS. 1048576 est la plus grande taille possible. • <code>wsiz=1048576</code> — Pour améliorer les performances, définit le nombre maximal d'octets de données que le client NFS peut envoyer pour chaque demande WRITE du réseau lors de l'écriture de données dans un fichier d'un système de fichiers EFS. 1048576 est la plus grande taille possible.

Champ	Description
	• <code>hard</code> – Définit le comportement de récupération du client NFS après qu'une demande NFS a expiré, de sorte que les demandes NFS sont relancées indéfiniment jusqu'à ce que le serveur réponde. Nous vous recommandons d'utiliser l'option de Montage physique (<code>hard</code>) pour garantir l'intégrité des données. Si vous utilisez un Montage <code>soft</code>, définissez le paramètre <code>timeo</code> sur au Moins 150 décisecon des (15 secondes). Vous minimiserez ainsi le risque de corruption des données inhérent aux Montages logiciels. • <code>timeo=600</code> – Définit la valeur de délai d'expiration que le client NFS utilise pour attendre une réponse avant de relancer une demande sur 600 décisecon des (60 secondes). Si vous devez Modifier le paramètre de délai (<code>timeo</code>), nous vous recommandons d'utiliser une valeur d'au Moins 150, ce qui équivaut à 15 secondes. Vous éviterez ainsi une baisse de performances. • <code>retrans=2</code> – Définit sur 2 le nombre de fois que le client NFS essaie une demande avant de tenter une action de récupération. • <code>noresvport</code> – Indique au client NFS d'utiliser un nouveau port source TCP (Transmission Control Protocol) lorsqu'une connexion réseau est rétablie. Cette utilisation permet de s'assurer que le système de fichiers EFS a une disponibilité ininterrompue après un événement de récupération du réseau. • <code>_netdev</code> – L'option empêche le client d'essayer de Monter le système de fichiers EFS tant que le réseau n'a pas été activé.
0	Spécifie la valeur <code>dump</code> ; 0 indique à l'utilitaire <code>dump</code> de ne pas sauvegarder le système de fichiers.
0	Indique à l'utilitaire <code>fsck</code> de ne pas s'exécuter au démarrage.

Démontage des systèmes de fichiers

Avant de supprimer un système de fichiers, nous vous recommandons de le démonter de chaque EC2 instance Amazon à laquelle il est connecté. Vous pouvez démonter un système de fichiers sur votre EC2 instance Amazon en exécutant la `umount` commande sur l'instance elle-même. Vous

ne pouvez pas démonter un système de fichiers EFS par le biais du AWS CLI AWS Management Console, du ou de l' AWS SDKs. Pour démonter un système de fichiers EFS connecté à une EC2 instance exécutant Linux, utilisez la `umount` commande suivante :

```
umount /mnt/efs
```

Il est conseillé de ne pas indiquer d'autres options `umount`. Evitez de définir d'autres options `umount` différentes des valeurs par défaut.

Vous pouvez vérifier que votre système de fichiers EFS a été démonté en exécutant la `df` commande. Cette commande affiche les statistiques d'utilisation du disque pour les systèmes de fichiers actuellement montés sur votre instance Amazon EC2 basée sur Linux. Si le système de fichiers EFS que vous souhaitez démonter n'est pas répertorié dans la sortie de `df` commande, cela signifie que le système de fichiers est démonté.

Exemple — Identifiez l'état de montage d'un système de fichiers EFS et démontez-le

```
$ 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% /
```

Tutoriel : créer un système de fichiers EFS et le monter sur une EC2 instance à l'aide du AWS CLI

Créez un système de fichiers EFS chiffré, montez-le sur une EC2 instance de votre VPC et testez la configuration à l'aide du AWS CLI

 Note

Dans le [Premiers pas](#) didacticiel, vous allez utiliser la console pour créer des ressources Amazon EC2 et EFS. Dans ce didacticiel, vous allez utiliser le AWS CLI pour faire de même, principalement pour vous familiariser avec l'API Amazon EFS.

Dans ce didacticiel, vous allez créer les AWS ressources suivantes dans votre compte :

- EC2 Ressources Amazon :
 - Deux groupes de sécurité (pour votre EC2 instance et le système de fichiers EFS).

Vous ajoutez des règles à ces groupes de sécurité afin d'autoriser un accès entrant/sortant approprié. Cela vous permet de vous EC2instance connecter au système de fichiers via la cible de montage en utilisant un port TCP NFSv4 .1 standard.

- Une EC2 instance de votre VPC.
- Ressources Amazon EFS :
 - Un système de fichiers.
 - Une cible de montage pour votre système de fichiers.

Pour monter votre système de fichiers sur une EC2 instance, vous devez créer une cible de montage dans votre VPC. Vous pouvez créer une cible de montage dans chacune des zones de disponibilité de votre VPC. Pour de plus amples informations, veuillez consulter [Comment fonctionne Amazon EFS](#).

Ensuite, vous testez le système de fichiers sur votre EC2 instance. L'étape de nettoyage à la fin du didacticiel fournit des informations vous permettant de supprimer ces ressources.

Le didacticiel crée toutes ces ressources dans la région de l'ouest des États-Unis (Oregon) (us-west-2). Peu importe ce que Région AWS vous utilisez, assurez-vous de l'utiliser régulièrement. Toutes vos ressources (votre VPC, vos ressources et vos EC2 ressources EFS) doivent se trouver dans les mêmes emplacements. Région AWS

Rubriques

- [Prérequis](#)
- [Configuration du AWS CLI](#)

- [Étape 1 : Création de EC2 ressources](#)
- [Étape 2 : Création de ressources EFS](#)
- [Étape 3 : monter le système de fichiers sur l' EC2 instance et tester](#)
- [Étape 4 : nettoyer](#)

Prérequis

- Vous pouvez utiliser vos informations d'identification root pour vous connecter Compte AWS à la console et essayer l'exercice de mise en route. Toutefois, AWS Identity and Access Management (IAM) vous recommande de ne pas utiliser les informations d'identification root de votre Compte AWS. Au lieu de cela, créez un administrateur dans votre compte et utilisez ces informations d'identification pour gérer les ressources de votre compte. Au lieu de cela, créez un administrateur dans votre compte et utilisez ces informations d'identification pour gérer les ressources de votre compte. Pour plus d'informations, voir [Attribuer un Compte AWS accès à un utilisateur d'IAM Identity Center](#) dans le guide de l'AWS IAM Identity Center utilisateur.
- Vous pouvez utiliser un VPC par défaut ou un VPC personnalisé que vous avez créé dans votre compte. Pour cette procédure, la configuration du VPC par défaut fonctionne. Toutefois, si vous utilisez un VPC personnalisé, vérifiez les éléments suivants :
 - Les noms d'hôte DNS sont activés. Pour plus d'informations, consultez [Attributs DNS pour votre VPC](#) dans le Guide de l'utilisateur d'Amazon VPC.
 - La passerelle Internet est attachée à votre VPC. Pour plus d'informations, consultez [Connexion à l'Internet à l'aide d'une passerelle Internet](#) dans le Guide de l'utilisateur Amazon VPC.
 - Les sous-réseaux VPC sont configurés pour demander des adresses IP publiques pour les instances lancées dans les sous-réseaux VPC. Pour plus d'informations, consultez la section [Adressage IP pour vos sous-réseaux VPCs et sous-réseaux](#) dans le guide de l'utilisateur Amazon VPC.
 - La table de routage VPC comprend une règle pour l'envoi de tout le trafic Internet entrant vers la passerelle Internet.
- Vous devez configurer AWS CLI et ajouter le profil adminuser.

Configuration du AWS CLI

Suivez les instructions ci-dessous pour configurer le profil utilisateur AWS CLI et.

Pour configurer le AWS CLI

1. Téléchargez et configurez l'interface AWS CLI. Pour obtenir des instructions, voir [Commencer avec le AWS CLI](#) dans le guide de AWS Command Line Interface l'utilisateur.
2. Définissez des profils.

Vous stockez les informations d'identification de l'utilisateur dans le AWS CLI config fichier. Les exemples de commandes CLI présentés dans ce didacticiel spécifient le profil adminuser. Créez le profil adminuser dans le fichier config. Vous pouvez également définir le profil utilisateur administrateur comme profil par défaut dans le fichier config comme illustré.

```
[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
```

Le profil précédent définit également la valeur par défaut Région AWS. Si vous ne spécifiez pas de région dans la commande CLI, c'est la région us-west-2 qui est prise en compte.

3. Vérifiez la configuration en saisissant la commande suivante à l'invite de commande. Ces deux commandes ne fournissent pas directement d'informations d'identification, par conséquent ce sont les informations du profil par défaut qui sont utilisées.
- Essayez les commandes d'aide

Vous pouvez également spécifier explicitement le profil utilisateur en ajoutant le paramètre `--profile`.

```
aws help
```

```
aws help \
--profile adminuser
```

Étape 1 : Création de EC2 ressources

Dans cette étape, vous effectuez les opérations suivantes :

- Créez deux groupes de sécurité.
- Ajoutez des règles pour les groupes de sécurité afin d'autoriser un accès supplémentaire.
- Lancez une EC2 instance. Vous allez créer et monter un système de fichiers EFS sur cette instance à l'étape suivante.

Étape 1.1 : Créer deux groupes de sécurité

Dans cette section, vous allez créer des groupes de sécurité dans votre VPC pour votre EC2 instance et votre cible de montage EFS. Plus loin dans le didacticiel, vous attribuerez ces groupes de sécurité à une EC2 instance et à une cible de montage EFS. Pour plus d'informations sur les groupes de sécurité, consultez la section [Groupes EC2 de sécurité Amazon pour les instances Linux](#).

Pour créer des groupes de sécurité

1. Créez deux groupes de sécurité à l'aide de la commande d'interface de ligne de commande `create-security-group` :
 - a. Créez un groupe de sécurité (`efs-walkthrough1-ec2-sg`) pour votre EC2 instance et fournissez votre identifiant 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
```

Notez l'ID du groupe de sécurité. Voici un exemple de réponse.

```
{  
  "GroupId": "sg-aexample"  
}
```

Pour trouver l'ID VPC, utilisez la commande ci-dessous.

```
$ aws ec2 describe-vpcs
```

- b. Créez un groupe de sécurité (`efs-walkthrough1-mt-sg`) pour votre cible de montage EFS. Vous devez fournir votre ID 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
```

Notez l'ID du groupe de sécurité. Voici un exemple de réponse.

```
{  
  "GroupId": "sg-aexample"  
}
```

2. Vérifiez les groupes de sécurité.

```
aws ec2 describe-security-groups \  
--group-ids list of security group IDs separated by space \  
--profile adminuser \  
--region us-west-2
```

Les deux doivent avoir une seule règle sortante qui autorise la sortie du trafic.

Dans la section suivante, vous autorisez un accès supplémentaire qui permet les opérations suivantes :

- Vous permet de vous connecter à votre EC2 instance.
- Activez le trafic entre une EC2 instance et une cible de montage EFS (à laquelle vous associez ces groupes de sécurité plus loin dans ce didacticiel).

Étape 1.2 : Ajouter des règles aux groupes de sécurité afin d'autoriser un accès entrant/sortant

Dans cette étape, vous ajoutez des règles aux groupes de sécurité pour autoriser un accès entrant/sortant.

Ajout de règles

1. Autorisez les connexions Secure Shell (SSH) entrantes au groupe de sécurité de votre EC2 instance (efs-walkthrough1-ec2-sg) afin de pouvoir vous connecter à votre EC2 instance via SSH depuis n'importe quel hôte.

```
$ 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
```

Vérifiez que le groupe de sécurité comporte la règle entrante et sortante que vous avez ajoutée.

```
aws ec2 describe-security-groups \
--region us-west-2 \
--profile adminuser \
--group-id security-group-id
```

2. Autorisez l'accès entrant au groupe de sécurité pour la cible de montage EFS (efs-walkthrough1-mt-sg).

À l'invite de commande, exécutez la AWS CLI `authorize-security-group-ingress` commande suivante à l'aide du profil `adminuser` pour ajouter la règle entrante.

```
$ 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. Vérifiez que les deux groupes de sécurité autorisent maintenant l'accès entrant.

```
aws ec2 describe-security-groups \
--group-names efs-walkthrough1-ec2-sg efs-walkthrough1-mt-sg \
--profile adminuser \
--region us-west-2
```

Étape 1.3 : Lancer une EC2 instance

Au cours de cette étape, vous lancez une EC2 instance.

Pour lancer une EC2 instance

1. Rassemblez les informations suivantes que vous devez fournir lors du lancement d'une EC2 instance :
 - Key pair name. Pour obtenir des instructions sur la création d'une paire de clés, consultez la section [Créer une paire de clés pour votre EC2 instance Amazon](#) dans le guide de EC2 l'utilisateur Amazon.
 - ID de l'Amazon Machine Image (AMI) que vous souhaitez lancer.

La AWS CLI commande que vous utilisez pour lancer une EC2 instance nécessite l'ID de l'Amazon Machine Image (AMI) que vous souhaitez déployer en tant que paramètre. L'exercice utilise l'AMI HVM Amazon Linux.

Note

Vous pouvez utiliser la plupart des applications Linux AMIs à usage général. Si vous utilisez une autre AMI Linux, assurez-vous que vous utilisez le gestionnaire de package de votre distribution pour installer le client NFS sur l'instance. En outre, vous pouvez avoir besoin d'ajouter des packages logiciels dès que vous en avez besoin.

Pour l'AMI Amazon Linux HVM, vous pouvez trouver la dernière version IDs sur [Amazon Linux AMI](#). Vous choisissez la valeur de l'ID dans le IDs tableau des AMI Amazon Linux comme suit :

- Choisissez la région US West Oregon. Cette procédure suppose que vous créez toutes les ressources dans la région USA Ouest (Oregon) Région (us-west-2).

- Choisissez le type EBS-backed HVM 64-bit (car dans la commande CLI vous indiquez le type d'instance `t2.micro`, qui ne prend pas en charge le stockage d'instance).
- ID du groupe de sécurité que vous avez créé pour une EC2 instance.
- Région AWS. Cette procédure utilise la région `us-west-2`.
- ID de sous-réseau de votre VPC dans lequel vous voulez lancer l'instance. Vous pouvez obtenir la liste des sous-réseaux à l'aide de la commande `describe-subnets`.

```
$ aws ec2 describe-subnets \  
--region us-west-2 \  
--filters "Name=vpc-id,Values=vpc-id" \  
--profile adminuser
```

Après avoir choisi l'ID de sous-réseau, notez les valeurs suivantes à partir du résultat `describe-subnets` :

- ID de sous-réseau – Vous avez besoin de cette valeur lorsque vous créez une cible de montage. Dans cet exercice, vous allez créer une cible de montage dans le même sous-réseau que celui dans lequel vous lancez une EC2 instance.
 - Zone de disponibilité du sous-réseau : vous avez besoin de cette valeur pour créer le nom DNS de votre cible de montage, que vous utiliserez pour monter un système de fichiers sur l'EC2 instance.
2. Exécutez la AWS CLI `run-instances` commande suivante pour lancer une EC2 instance.

```
$ 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. Notez l'ID d'instance renvoyé par la commande `run-instances`.
4. L'EC2 instance que vous avez créée doit avoir un nom DNS public que vous utilisez pour vous connecter à l'EC2 instance et y monter le système de fichiers. Le nom DNS public a le format suivant :


```
ec2-xx-xx-xx-xxx.compute-1.amazonaws.com
```

Exécutez la commande d'interface de ligne de commande suivante et notez le nom DNS public.

```
aws ec2 describe-instances \  
--instance-ids EC2 instance ID \  
--region us-west-2 \  
--profile adminuser
```

Si vous ne trouvez pas le nom DNS public, vérifiez la configuration du VPC dans lequel vous avez lancé l' EC2 instance. Pour de plus amples informations, veuillez consulter [Prérequis](#).

5. (Facultatif) Attribuez un nom à l' EC2 instance que vous avez créée. Pour ce faire, ajoutez une balise avec le nom de clé et la valeur définie sur le nom que vous souhaitez attribuer à l'instance. Pour ce faire, exécutez la AWS CLI `create-tags` commande suivante.

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

Étape 2 : Création de ressources EFS

Dans cette étape, vous effectuez les opérations suivantes :

- Créez un système de fichiers EFS chiffré.
- Activez la gestion du cycle de vie.
- Créez une cible de montage dans la zone de disponibilité dans laquelle vous avez lancé votre instance EFS.

Étape 2.1 : Création d'un système de fichiers EFS

Au cours de cette étape, vous allez créer un système de fichiers EFS. Notez le `FileSystemId` à utiliser plus tard lorsque vous créez des cibles de montage pour le système de fichiers à l'étape suivante.

Pour créer un système de fichiers

- Créez un système de fichiers avec la balise Name en option.
 - a. À l'invite de commande, exécutez la `create-file-system` commande AWS CLI suivante.

```
$ aws efs create-file-system \
--encrypted \
--creation-token FileSystemForWalkthrough1 \
--tags Key=Name,Value=SomeExampleNameValue \
--region us-west-2 \
--profile adminuser
```

Vous recevez la réponse suivante.

```
{
  "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. Notez la valeur `FileSystemId`. Vous avez besoin de cette valeur lorsque vous créez une cible de montage pour ce système de fichiers dans [Étape 2.3 : Créer une cible de montage](#).

Étape 2.2 : Activer la gestion du cycle de vie

Au cours de cette étape, vous activez la gestion du cycle de vie de votre système de fichiers afin d'utiliser la classe de stockage EFS Infrequent Access (IA). Pour en savoir plus, consultez [Gestion du cycle de vie du stockage](#) et [Classes de stockage EFS](#).

Pour activer la gestion du cycle de vie

- À l'invite de commande, exécutez la AWS CLI `put-lifecycle-configuration` commande suivante.

```
$ aws efs put-lifecycle-configuration \  
--file-system-id fs-c657c8bf \  
--lifecycle-policies TransitionToIA=AFTER_30_DAYS \  
--region us-west-2 \  
--profile adminuser
```

Vous recevez la réponse suivante.

```
{  
  "LifecyclePolicies": [  
    {  
      "TransitionToIA": "AFTER_30_DAYS"  
    }  
  ]  
}
```

Étape 2.3 : Créer une cible de montage

Au cours de cette étape, vous créez une cible de montage pour votre système de fichiers dans la zone de disponibilité où vous avez lancé votre EC2 instance.

1. Assurez-vous de disposer des informations suivantes :
 - ID du système de fichiers (par exemple, `fs-example`) pour lequel vous créez la cible de montage.
 - ID de sous-réseau VPC dans lequel vous avez lancé l' EC2 instance. [Étape 1 : Création de EC2 ressources](#)

Pour ce didacticiel, vous créez la cible de montage dans le même sous-réseau dans lequel vous avez lancé l' EC2 instance. Vous avez donc besoin de l'ID du sous-réseau (par exemple, `subnet-example`).

- ID du groupe de sécurité que vous avez créé pour la cible de montage à l'étape précédente.
2. À l'invite de commande, exécutez la AWS CLI `create-mount-target` commande suivante.

```
$ 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
```

Vous recevez la réponse suivante.

```
{  
  "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. Vous pouvez également utiliser la commande `describe-mount-targets` pour obtenir les descriptions des cibles de montage que vous avez créées sur un système de fichiers.

```
$ aws efs describe-mount-targets \  
--file-system-id file-system-id \  
--region us-west-2 \  
--profile adminuser
```

Étape 3 : monter le système de fichiers sur l' EC2 instance et tester

Dans cette étape, vous effectuez les opérations suivantes :

- Rassemblez les informations requises.

- Installez le client NFS sur votre EC2 instance.
- Montez le système de fichiers sur votre EC2 instance et testez-le.

Rubriques

- [Étape 3.1 : Collecter des informations](#)
- [Étape 3.2 : Installation du client NFS sur votre instance EC2](#)
- [Étape 3.3 : Montez le système de fichiers sur votre EC2 instance et testez](#)

Étape 3.1 : Collecter des informations

Assurez-vous de disposer des informations suivantes avant de suivre les étapes de cette section:

- Nom DNS public de votre EC2 instance au format suivant :

```
ec2-xx-xxx-xxx-xx.aws-region.compute.amazonaws.com
```

- Nom DNS de votre système de fichiers. Vous pouvez construire ce nom DNS à l'aide du format générique suivant :

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

L'EC2 instance sur laquelle vous montez le système de fichiers à l'aide de la cible de montage peut convertir le nom DNS du système de fichiers en adresse IP de la cible de montage.

Note

Amazon EFS n'exige pas que votre EC2 instance possède une adresse IP ou un nom DNS public. Les exigences susmentionnées concernent uniquement cet exemple de procédure. Elles permettent de s'assurer que vous pouvez établir la connexion à l'instance depuis un emplacement extérieur au VPC via SSH.

Étape 3.2 : Installation du client NFS sur votre instance EC2

Vous pouvez vous connecter à votre EC2 instance depuis Windows ou depuis un ordinateur exécutant Linux, macOS X ou toute autre variante d'Unix.

Pour installer un client NFS

1. Connectez-vous à votre EC2 instance. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Exécutez les commandes suivantes sur l' EC2 instance à l'aide de la session SSH :
 - a. (Facultatif) Obtenez les mises à jour et redémarrez.

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

Après le redémarrage, reconnectez-vous à votre EC2 instance.

- b. Installez le client NFS.

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

Note

Si vous choisissez l'AMI Amazon Linux 2016.03.0 lors du lancement de EC2 votre instance, vous n'avez pas besoin de l'`nfs-utils` installer car elle est déjà incluse dans l'AMI par défaut.

Étape 3.3 : Montez le système de fichiers sur votre EC2 instance et testez

Vous devez maintenant monter le système de fichiers sur votre EC2 instance.

1. Créez un répertoire (« efs-mount-point »).

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

2. Montez le système de fichiers EFS.

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

L'EC2 instance peut convertir le nom DNS de la cible de montage en adresse IP. Vous pouvez éventuellement spécifier l'adresse IP de la cible de montage directement.

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

3. Maintenant que le système de fichiers EFS est monté sur votre EC2 instance, vous pouvez créer des fichiers.

- a. Changez de répertoire.

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

- b. Affichez le contenu du répertoire.

```
$ ls -al
```

Il doit être vide.

```
drwxr-xr-x 2 root      root      4096 Dec 29 22:33 .  
drwx----- 4 ec2-user ec2-user 4096 Dec 29 22:54 ..
```

- c. Le répertoire racine d'un système de fichiers, une fois créé, appartient à l'utilisateur racine et ce dernier peut y écrire. Il n'est donc pas nécessaire de modifier les autorisations pour ajouter des fichiers.

```
$ sudo chmod go+rw .
```

À présent, si vous essayez la commande `ls -al`, vous constatez que les autorisations ont changé.

```
drwxrwxrwx 2 root      root      4096 Dec 29 22:33 .  
drwx----- 4 ec2-user ec2-user 4096 Dec 29 22:54 ..
```

- d. Créez un fichier texte .

```
$ touch test-file.txt
```

- e. Affichez le contenu du répertoire.

```
$ ls -l
```

Vous avez maintenant créé et monté avec succès un système de fichiers EFS sur votre EC2 instance dans votre VPC.

Le système de fichiers que vous avez monté n'est pas persistant d'un redémarrage à l'autre. Pour remonter automatiquement le répertoire, vous pouvez utiliser le fichier `fstab`. Si vous utilisez un groupe Auto Scaling pour lancer EC2 des instances, vous pouvez également définir des scripts dans une configuration de lancement.

Étape 4 : nettoyer

Si vous n'avez plus besoin des ressources que vous avez créées, vous devez les supprimer. Vous pouvez faire cela à l'aide de l'interface de ligne de commande.

- Supprimez les EC2 ressources (l' EC2 instance et les deux groupes de sécurité). Amazon EFS supprime l'interface réseau lorsque vous supprimez la cible de montage.
- Supprimez les ressources EFS (système de fichiers, cible de montage).

Pour supprimer les AWS ressources créées lors de cette procédure pas à pas

1. Mettez fin à l' EC2 instance que vous avez créée pour ce didacticiel.

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

Vous pouvez également supprimer EC2 des ressources à l'aide de la console. Pour plus d'informations, consultez [Mise hors service d'une instance](#).

2. Supprimez la cible de montage.

Vous devez supprimer les cibles de montage créées pour le système de fichiers avant de supprimer ce dernier. Vous pouvez obtenir une liste des cibles de montage à l'aide de la commande d'interface de ligne de commande `describe-mount-targets`.


```
$ aws efs describe-mount-targets \  
--file-system-id file-system-ID \  
--profile adminuser \  
--region aws-region
```

Supprimez ensuite la cible de montage à l'aide de la commande d'interface de ligne de commande `delete-mount-target`.

```
$ aws efs delete-mount-target \  
--mount-target-id ID-of-mount-target-to-delete \  
--profile adminuser \  
--region aws-region
```

3. (Facultatif) Supprimez les deux groupes de sécurité que vous avez créés. Vous ne payez pas pour la création des groupes de sécurité.

Vous devez d'abord supprimer le groupe de sécurité de la cible de montage, avant de supprimer le groupe de sécurité de l' EC2 instance. Le groupe de sécurité de la cible de montage possède une règle qui fait référence au groupe EC2 de sécurité. Par conséquent, vous ne pouvez pas d'abord supprimer le groupe de sécurité de l' EC2 instance.

Pour obtenir des instructions, consultez [Supprimer votre groupe de sécurité](#) dans le guide de EC2 l'utilisateur Amazon.

4. Supprimez le système de fichiers à l'aide de la commande d'interface de ligne de commande `delete-file-system`. Vous pouvez obtenir une liste de vos systèmes de fichiers à l'aide de la commande d'interface de ligne de commande `describe-file-systems`. Vous pouvez obtenir l'ID de système de fichiers à partir de la réponse.

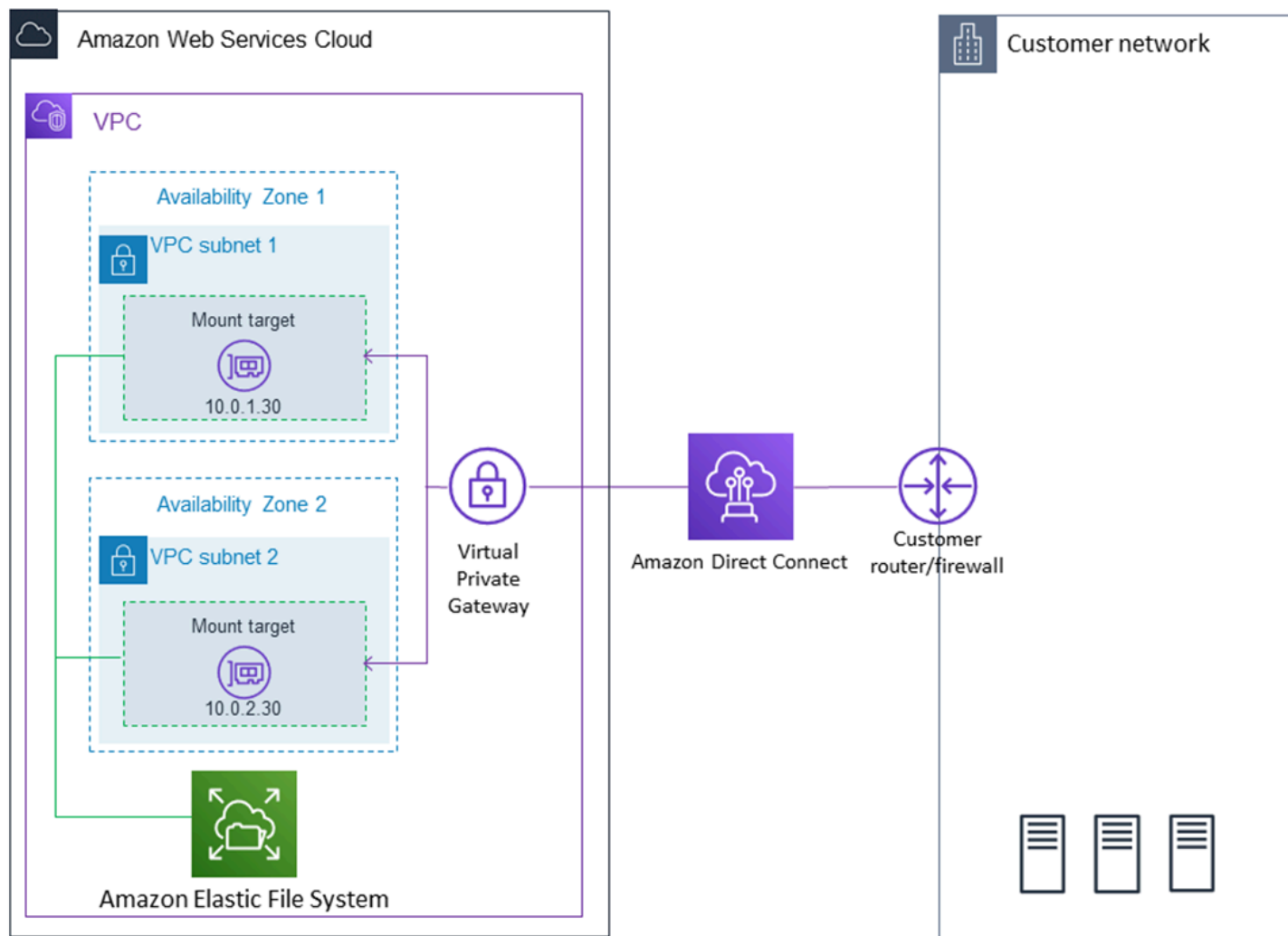
```
aws efs describe-file-systems \  
--profile adminuser \  
--region aws-region
```

Supprimez le système de fichiers en fournissant l'ID du système de fichiers.

```
$ aws efs delete-file-system \  
--file-system-id ID-of-file-system-to-delete \  
--region aws-region \  
--profile adminuser
```

Tutoriel : Montage avec des clients Linux locaux

Vous pouvez monter vos systèmes de fichiers Amazon EFS sur les serveurs de votre centre de données sur site lorsque vous êtes connecté à votre Amazon VPC ou à AWS Direct Connect un VPN. Le graphique suivant montre un schéma de haut niveau illustrant les éléments Services AWS requis pour le montage de systèmes de fichiers Amazon EFS sur site.



Note

L'utilisation d'Amazon EFS avec des clients basés sur Microsoft Windows n'est pas prise en charge.

Rubriques

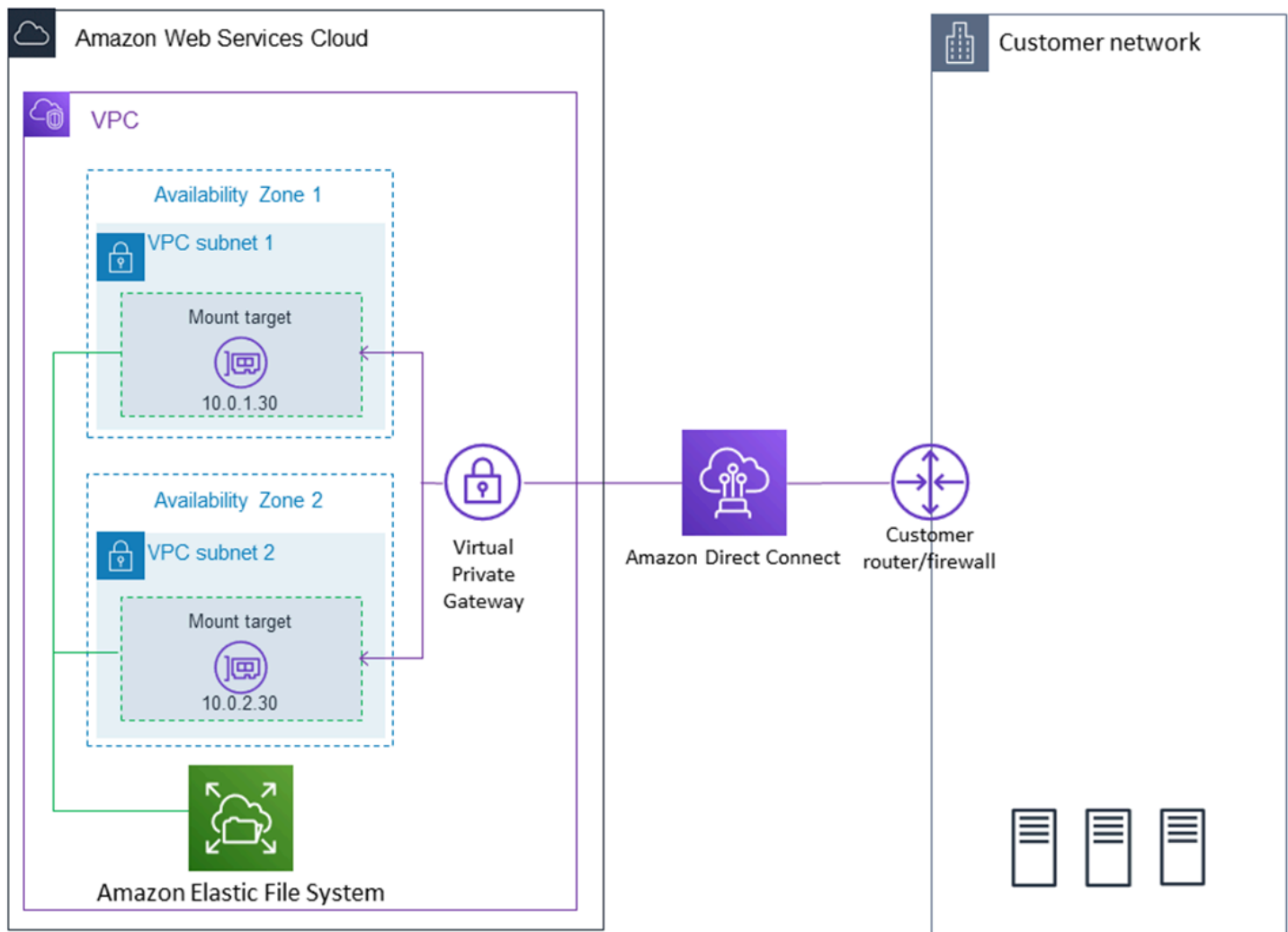
- [Prérequis](#)
- [Étape 1 : Création de vos ressources EFS](#)
- [Étape 2 : Installation du client NFS](#)
- [Étape 3 : Monter le système de fichiers Amazon EFS sur votre client sur site](#)
- [Étape 4 : Nettoyer les ressources et protéger votre compte AWS](#)
- [Facultatif : Chiffrement des données en transit](#)

Prérequis

Assurez-vous que vous disposez déjà d'une connexion VPN AWS Direct Connect ou d'une connexion VPN. Pour plus d'informations sur AWS Direct Connect, consultez le [Guide de l'utilisateur AWS Direct Connect](#). Pour plus d'informations sur la configuration d'une connexion VPN, consultez [Connecter votre VPC à des réseaux distants AWS Virtual Private Network à l'aide](#) du guide de l'utilisateur Amazon VPC.

Après avoir établi une connexion AWS Direct Connect ou un VPN, créez un système de fichiers EFS et une cible de montage dans votre Amazon VPC. Ensuite, vous téléchargez et installez les amazon-efs-utils outils. Testez ensuite le système de fichiers à partir de votre client sur site. Enfin, l'étape de nettoyage à la fin de la procédure fournit des informations concernant la suppression de ces ressources.

Le guide crée toutes ces ressources dans la région USA Ouest (Oregon) (us-west-2). Peu importe ce que Région AWS vous utilisez, assurez-vous de l'utiliser régulièrement. Toutes vos ressources (votre VPC, votre cible de montage et votre système de fichiers Amazon EFS) doivent être Région AWS identiques, comme indiqué dans le schéma suivant.



Note

Dans certains cas, votre application locale peut avoir besoin de savoir si le système de fichiers EFS est disponible. Dans ces cas-là, votre application doit être en mesure de pointer vers une adresse IP de point de montage différente si le premier point de montage n'est pas disponible temporairement. Dans ce scénario, nous vous recommandons d'avoir deux clients locaux connectés à votre système de fichiers via différentes zones de disponibilité (AZs) pour une meilleure disponibilité.

Vous pouvez utiliser les informations d'identification root de votre ordinateur Compte AWS pour vous connecter à la console et essayer cet exercice. Toutefois, les meilleures pratiques AWS Identity and Access Management (IAM) recommandent de ne pas utiliser les informations d'identification root de votre Compte AWS. Au lieu de cela, créez un administrateur dans votre compte et utilisez ces

informations d'identification pour gérer les ressources de votre compte. Pour plus d'informations, consultez la section [Accès par authentification unique Comptes AWS dans le](#) Guide de l'AWS IAM Identity Center utilisateur.

Vous pouvez utiliser un VPC par défaut ou un VPC personnalisé que vous avez créé dans votre compte. Pour cette procédure, la configuration du VPC par défaut fonctionne. Toutefois, si vous utilisez un VPC personnalisé, vérifiez les éléments suivants :

- La passerelle Internet est attachée à votre VPC. Pour plus d'informations, consultez [Activer l'accès à Internet pour un VPC à l'aide d'une passerelle Internet](#) dans le guide de l'utilisateur Amazon VPC.
- La table de routage VPC comprend une règle pour l'envoi de tout le trafic Internet entrant vers la passerelle Internet.

Étape 1 : Création de vos ressources EFS

Au cours de cette étape, vous allez créer votre système de fichiers EFS et monter les cibles.

Pour créer votre système de fichiers EFS

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Sélectionnez Créer un système de fichiers.
3. Choisissez votre VPC par défaut dans la liste VPC.
4. Cochez les cases correspondant à toutes les zones de disponibilité. Veillez à ce qu'elles comportent toutes les sous-réseaux par défaut, les adresses IP automatiques et les groupes de sécurité par défaut choisis. Il s'agit de vos cibles de montage. Pour de plus amples informations, veuillez consulter [Gérer des cibles de Montage](#).
5. Choisissez Étape suivante.
6. Nommez votre système de fichiers, conservez la sélection usage général comme mode de performance par défaut et choisissez Étape suivante.
7. Sélectionnez Créer un système de fichiers.
8. Choisissez votre système de fichiers dans la liste et prenez note de la valeur de Security group (Groupe de sécurité). Vous avez besoin de cette valeur pour l'étape suivante.

Le système de fichiers que vous venez de créer possède des cibles de montage. Chaque cible de montage dispose d'un groupe de sécurité associé. Ce groupe de sécurité fait office de pare-feu virtuel contrôlant le trafic réseau. Si vous n'avez pas indiqué de groupe de sécurité lors de la création d'une

cible de montage, Amazon EFS lui associe le groupe de sécurité par défaut du VPC. Si vous avez suivi scrupuleusement les étapes précédentes, vos cibles de montage utilisent le groupe de sécurité par défaut.

Vous allez maintenant ajouter une règle au groupe de sécurité de la cible de montage pour autoriser le trafic entrant vers le port NFS (2049). Vous pouvez utiliser le AWS Management Console pour ajouter la règle aux groupes de sécurité de votre cible de montage dans votre VPC.

Pour autoriser le trafic entrant vers le port NFS

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sous RÉSEAU ET SÉCURITÉ, choisissez Groupes de sécurité.
3. Choisissez le groupe de sécurité associé à votre système de fichiers. Vous avez pris note de cette valeur à la fin de l'[Étape 1 : Création de vos ressources EFS](#).
4. Dans le volet à onglets qui s'affiche sous la liste des groupes de sécurité, cliquez sur l'onglet Entrant.
5. Choisissez Modifier.
6. Choisissez Ajouter une règle, puis choisissez une règle du type suivant :
 - Type – NFS
 - Source – Anywhere (N'importe où)

Nous vous recommandons d'utiliser uniquement la source N'importe où pour les tests. Vous pouvez décider de créer un ensemble de sources personnalisées défini à l'adresse IP du client sur site, ou d'utiliser la console à partir du client lui-même, puis de choisir Mon IP.

 Note

Vous n'avez pas besoin d'ajouter une règle sortante, car la règle sortante par défaut autorise tout le trafic en sortie. Si ce n'est pas le cas, vous devez ajouter une règle sortante pour ouvrir une connexion TCP sur le port NFS, en identifiant le groupe de sécurité de la cible de montage en tant que destination.

Étape 2 : Installation du client NFS

Dans cette étape, vous installez le client NFS.

Pour installer le client NFS sur votre serveur sur site

Note

Si vous avez besoin de chiffrer les données en transit, utilisez l'assistant de montage Amazon EFS, `amazon-efs-utils`, au lieu du client NFS. Pour plus d'informations sur l'installation `amazon-efs-utils`, consultez la section [Facultatif : chiffrement des données en transit](#).

1. Accédez au terminal pour votre client sur site.
2. Installez NFS.

Si vous utilisez Red Hat Linux, installez NFS avec la commande suivante.

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

Si vous utilisez Ubuntu, installez NFS avec la commande suivante.

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

Étape 3 : Monter le système de fichiers Amazon EFS sur votre client sur site

Pour créer un annuaire de montage

1. Créez un répertoire pour le montage point à l'aide de la commande suivante.

Exemple

```
mkdir ~/efs
```

2. Choisissez votre adresse IP préférée de la cible de montage dans la zone de disponibilité. Vous pouvez mesurer la latence de vos clients Linux sur site. Pour ce faire, utilisez un outil basé sur

un terminal, par exemple par ping rapport à l'adresse IP de vos EC2 instances situées dans différentes zones de disponibilité, afin de trouver celle qui présente la latence la plus faible.

- Exécutez la commande de montage pour monter le système de fichiers via l'adresse IP de la cible de montage.

```
$ sudo mount -t nfs -o  
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport mount-  
target-IP:/ ~/efs
```

Maintenant que vous avez monté votre système de fichiers Amazon EFS, vous pouvez le tester avec la procédure suivante.

Pour tester la connexion du système de fichiers Amazon EFS

1. Remplacez les répertoires par le nouveau répertoire que vous avez créé à l'aide de la commande suivante.

```
$ cd ~/efs
```

2. Créez un sous-répertoire et remplacez le propriétaire de ce sous-répertoire par l'utilisateur de votre EC2 instance. Ensuite, accédez à ce nouveau répertoire à l'aide des commandes suivantes.

```
$ sudo mkdir getting-started  
$ sudo chown ec2-user getting-started  
$ cd getting-started
```

3. Créez un fichier texte contenant la commande suivante.

```
$ touch test-file.txt
```

4. Affichez le contenu du répertoire à l'aide de la commande suivante.

```
$ ls -al
```

Le fichier suivant est alors créé.


```
-rw-rw-r-- 1 username username 0 Nov 15 15:32 test-file.txt
```

Warning

Utilisez l'option `_netdev`, utilisée pour identifier les systèmes de fichiers réseau lors du Montage automatique de votre système de fichiers. Si elle `_netdev` est absente, il est possible que votre EC2 instance cesse de répondre. Cela s'explique par le fait que les systèmes de fichiers réseau doivent être initialisés après le démarrage de la mise en réseau de l'instance de calcul. Pour de plus amples informations, veuillez consulter [Le montage automatique échoue et l'instance ne répond pas](#).

Étape 4 : Nettoyer les ressources et protéger votre compte AWS

Une fois que vous avez suivi cette procédure, ou si vous ne voulez pas aller plus avant, vous devez suivre les étapes suivantes pour nettoyer vos ressources et protéger votre compte AWS .

Pour nettoyer les ressources et protéger votre Compte AWS

1. Démontez le système de fichiers Amazon EFS à l'aide de la commande suivante.

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

2. Ouvrez la console Amazon EFS sur la console [Amazon EFS](#).
3. Choisissez le système de fichiers Amazon EFS que vous souhaitez supprimer dans la liste des systèmes de fichiers.
4. Dans Actions, choisissez Supprimer le système de fichiers.
5. Dans la boîte de dialogue Supprimer définitivement le système de fichiers, saisissez l'ID du système de fichiers Amazon EFS que vous voulez supprimer, puis sélectionnez Supprimer le système de fichiers.
6. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
7. Dans le panneau de navigation, choisissez Groupes de sécurité.
8. Sélectionnez le nom du groupe de sécurité auquel vous avez ajouté la règle de cette procédure.

 Warning

Ne supprimez pas le groupe de sécurité par défaut pour votre VPC.

9. Pour Actions, choisissez Modifier les règles entrantes.
10. Choisissez le X à la fin de la règle entrante que vous ajoutée, puis choisissez Enregistrer.

Facultatif : Chiffrement des données en transit

Pour chiffrer les données en transit, utilisez l'assistant de montage Amazon EFS au lieu du client NFS. `amazon-efs-utils`

Le package `amazon-efs-utils` est une collection d'outils Amazon EFS. La `amazon-efs-utils` collection est fournie avec un assistant de montage et des outils qui facilitent le chiffrement des données en transit pour Amazon EFS. Pour plus d'informations sur ce package, consultez [Installation du client Amazon EFS](#). Ce package est disponible en téléchargement gratuit sur le site GitHub, que vous pouvez obtenir en clonant le dépôt du package.

Pour cloner à `amazon-efs-utils` partir de GitHub

1. Accédez au terminal pour votre client sur site.
2. Depuis le terminal, clonez l' `amazon-efs-utils` depuis le répertoire de votre choix GitHub à l'aide de la commande suivante.

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

Maintenant que vous avez le package, vous pouvez l'installer. Cette installation est gérée différemment selon la distribution Linux de votre client sur site. Les distributions suivantes sont prises en charge :

- Amazon Linux 2
- Amazon Linux
- Red Hat Enterprise Linux (et dérivés telles que CentOS) version 7 et versions ultérieures
- Ubuntu 16.04 LTS et les versions plus récentes

Pour compiler et installer amazon-efs-utils en tant que package RPM

1. Ouvrez un terminal sur votre client et accédez au répertoire contenant le amazon-efs-utils package cloné. GitHub
2. Créez le package avec la commande suivante :

```
make rpm
```

Note

Si vous ne l'avez pas déjà fait, installez le package rpm-builder à l'aide de la commande suivante.

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

3. Installez le package à l'aide de la commande suivante :

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

Pour compiler et installer amazon-efs-utils sous forme de package deb

1. Ouvrez un terminal sur votre client et accédez au répertoire contenant le amazon-efs-utils package cloné. GitHub
2. Créez le package avec la commande suivante :

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

3. Installez le package à l'aide de la commande suivante :

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

Une fois le package installé, configurez-le amazon-efs-utils pour une utilisation dans votre Région AWS with AWS Direct Connect ou VPN.

Pour configurer amazon-efs-utils pour une utilisation dans votre Région AWS

1. Dans l'éditeur de texte de votre choix, ouvrez le fichier `/etc/amazon/efs/efs-utils.conf` pour le modifier.
2. Recherchez la ligne `dns_name_format = {fs_id}.efs.{region}.amazonaws.com`.
3. Remplacez `{region}` par l'ID de votre région AWS , par exemple `us-west-2`.

Pour monter le système de fichiers EFS sur votre client sur site, vous devez d'abord ouvrir un terminal sur votre client Linux sur site. Pour monter le système, vous avez besoin de l'ID du système de fichiers, de l'adresse IP de cible de montage pour l'une de vos cibles de montage et de Région AWS du système de fichiers. Si vous avez créé plusieurs cibles de montage pour votre système de fichiers, vous pouvez choisir l'une d'elles.

Lorsque vous avez ces informations, vous pouvez monter votre système de fichiers en trois étapes :

Pour créer un annuaire de montage

1. Créez un répertoire pour le montage point à l'aide de la commande suivante.

Exemple

```
mkdir ~/efs
```

2. Choisissez votre adresse IP préférée de la cible de montage dans la zone de disponibilité. Vous pouvez mesurer la latence de vos clients Linux sur site. Pour ce faire, utilisez un outil basé sur un terminal, par exemple par ping rapport à l'adresse IP de vos EC2 instances situées dans différentes zones de disponibilité, afin de trouver celle qui présente la latence la plus faible.

Pour mettre à jour `/etc/hosts`

- Ajoutez une entrée à votre fichier `/etc/hosts` local avec l'ID du système de fichiers et l'adresse IP de la cible de montage, au format suivant.

```
mount-target-IP-Address file-system-ID.efs.region.amazonaws.com
```

Exemple

```
192.0.2.0 fs-12345678.efs.us-west-2.amazonaws.com
```

Pour créer un annuaire de montage

1. Créez un répertoire pour le montage point à l'aide de la commande suivante.

Exemple

```
mkdir ~/efs
```

2. Exécutez la commande mount pour monter le système de fichiers.

Exemple

```
sudo mount -t efs fs-12345678 ~/efs
```

Si vous souhaitez utiliser le chiffrement des données en transit, votre commande de montage doit se présenter comme suit :

Exemple

```
sudo mount -t efs -o tls fs-12345678 ~/efs
```

Tutoriel : monter un système de fichiers à partir d'un autre VPC

Dans ce didacticiel, vous allez configurer une EC2 instance pour monter un système de fichiers EFS situé dans un autre cloud privé virtuel (VPC). Pour ce faire, utilisez l'assistant de montage EFS. L'assistant de montage fait partie de l'ensemble d'outils `amazon-efs-utils`. Pour plus d'informations sur `amazon-efs-utils`, consultez [Installation du client Amazon EFS](#).

Le VPC du client et le VPC de votre système de fichiers EFS doivent être connectés à l'aide d'une connexion d'appairage de VPC ou d'une passerelle de transit de VPC. Lorsque vous utilisez une connexion d'appairage VPC ou une passerelle de transit pour vous connecter VPCs, les EC2 instances d'un VPC peuvent accéder aux systèmes de fichiers EFS d'un autre VPC, même si elles appartiennent à des comptes différents. VPCs

Note

L'utilisation d'Amazon EFS avec des clients basés sur Microsoft Windows n'est pas prise en charge.

Rubriques

- [Prérequis](#)
- [Étape 1 : Déterminer l'ID de la zone de disponibilité de la cible de montage](#)
- [Étape 2 : Déterminer l'adresse IP cible du montage](#)
- [Étape 3 : ajouter une entrée d'hôte pour la cible de montage](#)
- [Étape 4 : monter votre système de fichiers à l'aide de l'assistant de montage EFS](#)
- [Étape 5 : Nettoyez les ressources et protégez votre Compte AWS](#)

Prérequis

Pour terminer ce didacticiel, vous devez disposer des éléments suivants :

- L'ensemble d'outils amazon-efs-utils est installé sur l'EC2 instance avant d'utiliser cette procédure. Pour obtenir des instructions sur l'installation de l'ensemble d'outils amazon-efs-utils, veuillez consulter [Installation du client Amazon EFS](#).
- L'un des éléments suivants :
 - Une connexion d'appairage VPC entre le VPC où réside le système de fichiers EFS et le VPC où réside l'instance. EC2 Une connexion d'appairage VPC est une connexion réseau entre deux VPCs. Ce type de connexion vous permet d'acheminer le trafic entre eux à l'aide d'adresses privées du protocole Internet version 4 (IPv4) ou du protocole Internet version 6 (IPv6). Vous pouvez utiliser le peering VPC pour vous connecter au VPCs sein d'un même Région AWS système ou entre les deux. Régions AWS Pour de plus amples informations, consultez [Création et acceptation d'une connexion d'appairage de VPC](#) dans le Guide de peering Amazon VPC.
 - Passerelle de transit reliant le VPC où réside le système de fichiers EFS et le VPC où réside l'instance. EC2 Une passerelle de transit est un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations, consultez [Getting Started with using Amazon VPC Transit Gateways](#) dans le guide Amazon VPC Transit Gateways.

Étape 1 : Déterminer l'ID de la zone de disponibilité de la cible de montage

Pour garantir la haute disponibilité de votre système de fichiers, nous vous recommandons de toujours utiliser une adresse IP cible de EC2 montage située dans la même zone de disponibilité que votre client NFS. Si vous montez un système de fichiers EFS qui se trouve dans un autre compte, assurez-vous que le client NFS et la cible de montage EFS possèdent le même ID de Zone de

disponibilité. Cette exigence s'applique en raison des noms de zone de disponibilité qui peuvent différer selon les comptes.

Pour déterminer l'ID de zone de disponibilité de l' EC2 instance

1. Connectez-vous à votre EC2 instance. Pour plus d'informations, consultez [Connect to your EC2 instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Déterminez l'ID de zone de disponibilité dans lequel se trouve l' EC2 instance à l'aide de la commande `describe-availability-zones` CLI comme suit.

```
[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 de zone de disponibilité est renvoyé dans l'`ZoneId` d'établissement, `use2-az2`.

Étape 2 : Déterminer l'adresse IP cible du montage

Maintenant que vous connaissez l'ID de zone de disponibilité de l' EC2 instance, vous pouvez récupérer l'adresse IP de la cible de montage qui se trouve dans le même ID de zone de disponibilité.

Pour déterminer l'adresse IP de la cible de montage qui possède le même ID de zone de disponibilité

- Récupérez l'adresse IP de la cible de montage de votre système de fichiers dans l'ID de zone de disponibilité `use2-az2` à l'aide de la commande d'interface de ligne de commande `describe-mount-targets`, comme suit.

```
$ 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 cible de montage de l'ID de zone de disponibilité use2-az2 possède l'adresse IP 10.0.2.153.

Étape 3 : ajouter une entrée d'hôte pour la cible de montage

Vous pouvez désormais créer une entrée dans le `/etc/hosts` fichier de l' EC2 instance qui mappe l'adresse IP cible du montage au nom d'hôte de votre système de fichiers EFS.

Pour ajouter une entrée hôte pour la cible de montage

1. Ajoutez une ligne pour l'adresse IP cible du montage dans le `/etc/hosts` fichier de l' EC2 instance. L'entrée utilise le format `mount-target-IP-Address file-system-ID.efs.region.amazonaws.com`. Utilisez la commande suivante pour ajouter la ligne dans le fichier.


```
echo "10.0.2.153 fs-01234567.efs.us-east-2.amazonaws.com" | sudo tee -a /etc/hosts
```

2. Assurez-vous que les groupes de sécurité VPC de l' EC2 instance et de la cible de montage disposent de règles autorisant l'accès au système de fichiers EFS, selon les besoins. Pour de plus amples informations, veuillez consulter [Utilisation de groupes de sécurité VPC](#).

Étape 4 : monter votre système de fichiers à l'aide de l'assistant de montage EFS

Pour monter votre système de fichiers EFS, vous devez d'abord créer un répertoire de montage sur l' EC2 instance. Ensuite, à l'aide de l'assistant de montage EFS, vous pouvez monter le système de fichiers avec une autorisation AWS Identity and Access Management (IAM) ou un point d'accès EFS. Pour plus d'informations, consultez [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#) et [Utilisation des points d'accès](#).

Pour créer un annuaire de montage

- Créez un répertoire dans lequel monter le système de fichiers à l'aide de la commande suivante.

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

Pour monter le système de fichiers avec une autorisation IAM

- Utilisez la commande suivante pour monter le système de fichiers avec une autorisation IAM.

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

Pour monter le système de fichiers à l'aide d'un point d'accès EFS

- Utilisez la commande suivante pour monter le système de fichiers à l'aide d'un point d'accès EFS.

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

Maintenant que vous avez monté votre système de fichiers EFS, vous pouvez le tester à l'aide de la procédure suivante.

Pour tester la connexion au système de fichiers EFS

1. Remplacez les répertoires par le nouveau répertoire que vous avez créé à l'aide de la commande suivante.

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

2. Créez un sous-répertoire et remplacez le propriétaire de ce sous-répertoire par l'utilisateur de votre EC2 instance. Ensuite, accédez à ce nouveau répertoire à l'aide des commandes suivantes :

```
$ sudo mkdir getting-started
$ sudo chown ec2-user getting-started
$ cd getting-started
```

3. Créez un fichier texte contenant la commande suivante.

```
$ touch test-file.txt
```

4. Affichez le contenu du répertoire à l'aide de la commande suivante.

```
$ ls -al
```

Le fichier suivant est alors créé.

```
-rw-rw-r-- 1 username username 0 Nov 15 15:32 test-file.txt
```

Vous pouvez également monter votre système de fichiers automatiquement en ajoutant une entrée au fichier `/etc/fstab`. Pour de plus amples informations, veuillez consulter [Activation du montage automatique sur les instances EC2 Linux existantes](#).

Warning

Utilisez l'option `_netdev`, utilisée pour identifier les systèmes de fichiers réseau lors du montage automatique de votre système de fichiers. Si elle `_netdev` est absente, il est possible que votre EC2 instance cesse de répondre. Cela s'explique par le fait que les

systèmes de fichiers réseau doivent être initialisés après le démarrage de la mise en réseau de l'instance de calcul. Pour de plus amples informations, veuillez consulter [Le montage automatique échoue et l'instance ne répond pas](#).

Étape 5 : Nettoyez les ressources et protégez votre Compte AWS

Après avoir terminé ce didacticiel, effectuez les étapes suivantes pour nettoyer vos ressources et protéger vos Compte AWS.

Pour nettoyer les ressources et protéger votre Compte AWS

1. Démontez le système de fichiers EFS à l'aide de la commande suivante.

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

2. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
3. Choisissez le système de fichiers &EFS; que vous souhaitez supprimer dans la liste des systèmes de fichiers.
4. Dans Actions, choisissez Supprimer le système de fichiers.
5. Dans la boîte de dialogue Supprimer définitivement le système de fichiers, saisissez l'ID du système de fichiers EFS que vous voulez supprimer, puis sélectionnez Supprimer le système de fichiers.
6. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
7. Dans le panneau de navigation, choisissez Groupes de sécurité.
8. Sélectionnez le nom du groupe de sécurité auquel vous avez ajouté la règle pour ce didacticiel.

Warning

Ne supprimez pas le groupe de sécurité par défaut pour votre VPC.

9. Pour Actions, choisissez Modifier les règles entrantes.
10. Choisissez le X à la fin de la règle entrante que vous ajoutée, puis choisissez Enregistrer.

Résolution des problèmes de montage

Vous trouverez ci-dessous des informations sur la résolution des problèmes de montage du système de fichiers EFS.

Le montage du système de fichiers sur l'instance Windows échoue

Le montage d'un système de fichiers sur une EC2 instance Amazon sous Microsoft Windows échoue.

Action à exécuter

N'utilisez pas Amazon EFS avec des EC2 instances Windows, qui ne sont pas prises en charge.

Accès refusé par le serveur

Un montage de système de fichiers échoue avec le message suivant :

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

Ce problème peut se produire si votre client NFS n'a pas l'autorisation de monter le système de fichiers.

Action à exécuter

Si vous essayez de monter le système de fichiers à l'aide d'IAM, assurez-vous d'utiliser l'option `-o iam` or `-o tls` dans votre commande de montage. Cela indique à l'assistant de montage EFS de transmettre vos informations d'identification à la cible de montage EFS. Si vous n'avez toujours pas accès, vérifiez votre stratégie de système de fichiers et votre stratégie d'identité pour vous assurer qu'aucune clause DENY ne s'applique à votre connexion et qu'au moins une clause ALLOW s'applique à la connexion. Pour plus d'informations, consultez [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#) et [Création de politiques de système de fichiers](#).

Le montage automatique échoue et l'instance ne répond pas

Ce problème peut survenir si le système de fichiers a été monté automatiquement sur une instance et si l'option `_netdev` n'a pas été déclarée. Si elle `_netdev` est absente, il est possible que votre EC2 instance cesse de répondre. Cela s'explique par le fait que les systèmes de fichiers réseau doivent être initialisés après le démarrage de la mise en réseau de l'instance de calcul.

Action à exécuter

Si ce problème se produit, contactez AWS le Support.

Le montage de plusieurs systèmes de fichiers Amazon EFS dans /etc/fstab échoue

Pour les instances qui utilisent le système d'initialisation systemd avec plusieurs entrées Amazon EFS dans /etc/fstab, il peut arriver que tout ou partie de ces entrées ne soient pas montées. Dans ce cas, la sortie dmesg affiche une ou plusieurs lignes similaires à ce qui suit :

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

Action à exécuter

Dans ce cas, nous vous recommandons de créer un nouveau fichier de service système dans /etc/systemd/system/mount-nfs-sequentially.service. Le code à inclure dans le fichier varie selon que vous montez les systèmes de fichiers manuellement ou que vous utilisez l'assistant de montage Amazon EFS.

- Si vous montez manuellement les systèmes de fichiers, la ExecStart commande doit pointer sur Network File System (NFS4). Inclure le code suivant dans le fichier :

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

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

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

- Si vous utilisez l'assistant de montage Amazon EFS, la ExecStart commande doit pointer vers EFS au lieu d' NFS4 utiliser le protocole TLS (Transport Layer Security). Inclure le code suivant dans le fichier :

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

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

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

Après avoir créé le fichier, exécutez les deux commandes suivantes :

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

Redémarrez ensuite votre EC2 instance Amazon. Les systèmes de fichiers sont montés à la demande, généralement en une seconde.

La commande de montage échoue avec le message d'erreur « type de fs erroné »

La commande de montage échoue avec le message d'erreur suivant.

```
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.
```

Action à exécuter

Si vous recevez ce message, installez le package `nfs-utils` (ou `nfs-common` sur Ubuntu). Pour de plus amples informations, veuillez consulter [Installation du client NFS](#).

La commande de montage échoue avec le message d'erreur « option de montage incorrecte »

La commande de montage échoue avec le message d'erreur suivant.

```
mount.nfs: an incorrect mount option was specified
```

Action à exécuter

Ce message d'erreur signifie probablement que votre distribution Linux ne prend pas en charge les versions 4.0 et 4.1 (NFSv4) du système de fichiers réseau. Pour vérifier si c'est le cas, vous pouvez exécuter la commande suivante :

```
$ grep CONFIG_NFS_V4_1 /boot/config*
```

Si la commande précédente est renvoyée `# CONFIG_NFS_V4_1 is not set`, la version NFSv4 .1 n'est pas prise en charge sur votre distribution Linux. Pour obtenir la liste des Amazon Machine Images (AMIs) pour Amazon Elastic Compute Cloud (Amazon EC2) compatibles avec la NFSv4 version 1.1, consultez [NFS Support](#).

Le montage avec point d'accès échoue

La commande de montage échoue lors du montage avec un point d'accès, avec le message d'erreur suivant :

```
mount.nfs4: mounting access_point failed, reason given by server: No such file or directory
```

Action à exécuter

Ce message d'erreur indique que le chemin EFS spécifié n'existe pas. Assurez-vous de fournir la propriété et les autorisations pour le répertoire racine du point d'accès. EFS ne créera pas le répertoire racine sans cette information. Pour de plus amples informations, veuillez consulter [Utilisation des points d'accès](#).

Si vous ne spécifiez aucune propriété ni aucune autorisation pour le répertoire racine, et si le répertoire racine n'existe pas déjà, EFS ne créera pas le répertoire racine. Dans ce cas, toute tentative de montage du système de fichiers à l'aide du point d'accès échoue.

Le montage du système de fichiers échoue immédiatement après la création du système de fichiers

La propagation complète des enregistrements DNS (Domain Name Service) dans Région AWS peut prendre jusqu'à 90 secondes après la création d'une cible de montage.

Action à exécuter

Si vous créez et montez des systèmes de fichiers par programmation, par exemple à l'aide d'un AWS CloudFormation modèle, nous vous recommandons d'implémenter une condition d'attente.

Le montage du système de fichiers se bloque, puis échoue avec une erreur de dépassement de délai d'attente

La commande de montage du système de fichiers se bloque pendant une minute ou deux, puis échoue avec une erreur de dépassement de délai d'attente au bout d'une ou deux minutes. Le code suivant en présente un exemple.

```
$ sudo mount -t nfs -o
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-ip:/ mnt

[2+ minute wait here]
mount.nfs: Connection timed out
$
```

Action à exécuter

Cette erreur peut se produire car l' EC2 instance Amazon ou les groupes de sécurité cibles du montage ne sont pas correctement configurés. Assurez-vous que le groupe de sécurité cible de montage dispose d'une règle entrante qui autorise l'accès NFS depuis le groupe de EC2 sécurité. Pour de plus amples informations, veuillez consulter [Utilisation de groupes de sécurité VPC](#).

Vérifiez que l'adresse IP de la cible montage que vous avez spécifiée est valide. Si vous spécifiez une adresse IP erronée et que rien à cette adresse IP ne rejette le montage, vous pouvez rencontrer ce problème.

Le montage d'un système de fichiers avec NFS à l'aide d'un nom DNS échoue

Les tentatives de montage d'un système de fichiers à l'aide d'un client NFS (sans le client amazon-efs-utils) en utilisant le nom DNS du système de fichiers échouent, comme illustré dans l'exemple suivant :

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



```
mount.nfs: Failed to resolve server file-system-id.efs.aws-region.amazonaws.com:
  Name or service not known.

$
```

Action à exécuter

Vérifiez la configuration de votre VPC. Si vous utilisez un VPC personnalisé, assurez-vous que les paramètres DNS sont activés. Pour plus d'informations, consultez [DNS attributes for your VPC](#) (Attributs DNS pour votre VPC) dans le Guide de l'utilisateur d'Amazon VPC. De plus, les noms DNS du système de fichiers et de la cible de montage ne peuvent pas être résolus depuis l'extérieur du VPC où ils existent.

Avant de monter un système de fichiers en utilisant son nom DNS dans la mount commande, vous devez effectuer les opérations suivantes :

- Assurez-vous qu'il existe une cible de montage Amazon EFS dans la même zone de disponibilité que l' EC2 instance Amazon.
- Assurez-vous qu'il existe une cible de montage dans le même VPC que l'instance Amazon EC2 . Sinon, vous ne pouvez pas utiliser la résolution de noms DNS pour les cibles de montage EFS qui se trouvent dans un autre VPC. Pour de plus amples informations, veuillez consulter [Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC](#).
- Connectez votre EC2 instance Amazon au sein d'un Amazon VPC configuré pour utiliser le serveur DNS fourni par Amazon. Pour plus d'informations, consultez [Jeux d'options DHCP](#) dans le Guide de l'utilisateur Amazon VPC.
- Assurez-vous que les noms d'hôte DNS sont activés sur le VPC Amazon de l' EC2 instance Amazon connectée. Pour plus d'informations, consultez [Attributs DNS pour votre VPC](#) dans le Guide de l'utilisateur d'Amazon VPC.

Échec du montage d'un système de fichiers avec « nfs ne répond pas »

Le montage d'un système de fichiers échoue sur un événement de reconnexion à un port source TCP (Transmission Control Protocol) avec "nfs: server_name still not responding".

Action à exécuter

Utilisez l'option de montage `noresvport` pour vous assurer que le client NFS utilise un nouveau port source TCP (Transmission Control Protocol) lorsqu'une connexion réseau est rétablie. Cette

utilisation permet de garantir une disponibilité ininterrompue après un événement de récupération du réseau.

L'état de cycle de vie de la cible de montage est bloqué

L'état de cycle de vie de la cible de montage est bloqué à l'état creating (création) ou deleting (suppression).

Action à exécuter

Recommencez l'appel `CreateMountTarget` ou `DeleteMountTarget`.

L'état du cycle de vie cible du montage indique une erreur

L'état du cycle de vie de la cible de montage s'affiche comme une Erreur.

Action à exécuter

Amazon EFS ne peut pas créer les enregistrements système de nom de domaine (DNS) nécessaires pour les nouvelles cibles de montage du système de fichiers si le cloud privé virtuel (VPC) comporte des zones hébergées en conflit. Amazon EFS ne peut pas créer de nouveaux enregistrements dans une zone hébergée appartenant au client. Si vous devez gérer une zone hébergée avec une plage DNS `efs.<region>.amazonaws.com` conflictuelle, créez-la dans un VPC distinct. Pour plus d'informations sur les considérations DNS pour un VPC, consultez la section [Attributs DNS pour votre VPC](#).

Pour résoudre ce problème, supprimez l'hôte `efs.<region>.amazonaws.com` en conflit dans le VPC et créez à nouveau la cible de montage. Pour plus d'informations sur la suppression de la cible de montage, consultez [Gérer des cibles de Montage](#).

Le montage ne répond pas

Un montage Amazon EFS ne semble pas répondre. Par exemple, des commandes telles que `ls` se bloquent.

Action à exécuter

Cette erreur peut se produire si une autre application écrit de grandes quantités de données sur le système de fichiers. L'accès aux fichiers qui sont écrits peut être bloqué jusqu'à ce que l'opération

soit terminée. En général, les commandes ou les applications qui essaient d'accéder aux fichiers en cours d'écriture peuvent sembler bloquées. Par exemple, la commande `ls` peut se bloquer lorsqu'elle essaie d'accéder au fichier qui est en cours d'écriture. Ceci s'explique par le fait que certaines distributions Linux utilisent l'alias de commande `ls` afin d'extraire les attributs, en plus de la liste du contenu du répertoire.

Pour résoudre ce problème, vérifiez si une autre application est en train d'écrire dans des fichiers sur le montage Amazon EFS, et si elle est à l'état `Uninterruptible sleep (D)` comme dans l'exemple suivant :

```
$ 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
```

Après avoir vérifié que c'est le cas, vous pouvez résoudre le problème en attendant que l'autre opération d'écriture se termine, ou en essayant une solution de contournement. Dans l'exemple `ls`, vous pouvez utiliser la commande `/bin/ls` directement, au lieu d'un alias. Cela permet à la commande de continuer sans suspendre le fichier dans lequel sont écrites les données. En général, si l'application qui écrit les données peut forcer un vidage périodique des données, peut-être en utilisant `fsync(2)`, cette opération peut contribuer à améliorer la réactivité de votre système de fichiers pour d'autres applications. Cependant, cette amélioration peut se faire aux dépens des performances lorsque l'application écrit des données.

Le client monté est déconnecté

Un client monté sur un système de fichiers Amazon EFS peut parfois être déconnecté pour diverses raisons. Les clients NFS sont conçus pour se reconnecter automatiquement en cas d'interruption afin de minimiser l'impact des déconnexions de routine sur les performances et la disponibilité des applications. Dans la plupart des cas, les clients se reconnectent de manière transparente en quelques secondes.

Cependant, les logiciels clients NFS inclus dans les anciennes versions du noyau Linux (versions v5.4 et antérieures) ont un comportement qui fait que les clients NFS tentent de se reconnecter sur le même port source TCP en cas de déconnexion. Ce comportement n'est pas conforme à la RFC TCP et peut empêcher ces clients de rétablir rapidement les connexions à leur serveur NFS (dans ce cas, un système de fichiers EFS).

Pour résoudre ce problème, nous vous recommandons vivement d'utiliser l'assistant de montage Amazon EFS pour monter vos systèmes de fichiers EFS. L'assistant de montage EFS utilise

des paramètres de montage optimisés pour les systèmes de fichiers Amazon EFS. Pour plus d'informations sur le client EFS et l'aide au montage, consultez [Installation du client Amazon EFS](#).

Si vous ne pouvez pas utiliser l'assistant de montage EFS, nous vous recommandons vivement d'utiliser l'option de montage NFS `noresvport`, qui indique aux clients NFS de rétablir les connexions en utilisant de nouveaux ports source TCP pour éviter ce problème. Pour de plus amples informations, veuillez consulter [Paramètres de montage NFS recommandés](#).

Les opérations sur un système de fichiers nouvellement monté renvoient l'erreur « mauvaise gestion de fichier »

Les opérations effectuées sur un système de fichiers nouvellement monté renvoient une erreur `bad file handle`.

Cette erreur peut se produire si une EC2 instance Amazon a été connectée à un système de fichiers et à une cible de montage avec une adresse IP spécifiée, puis que le système de fichiers et la cible de montage ont été supprimés. Si vous créez un nouveau système de fichiers et une nouvelle cible de montage pour vous connecter à cette EC2 instance Amazon avec la même adresse IP cible de montage, ce problème peut survenir.

Action à exécuter

Vous pouvez résoudre cette erreur en démontant le système de fichiers, puis en le remontant sur l'instance Amazon. EC2 Pour plus d'informations sur le démontage de votre système de fichiers Amazon EFS, consultez [Démontage des systèmes de fichiers](#).

Le démontage d'un système de fichiers échoue

Si votre système de fichiers est occupé, vous ne pouvez pas le démonter.

Action à exécuter

Vous pouvez résoudre ce problème en procédant de l'une des manières suivantes :

- Utilisez `lazy unmount`, `umount -l` qui détache le système de fichiers de la hiérarchie du système de fichiers lors de son exécution, puis nettoie toutes les références au système de fichiers dès qu'il n'est plus occupé.
- Patientez jusqu'à ce que toutes les opérations de lecture et d'écriture soient terminées, puis essayez de relancer la commande `umount`.

- Forcez un démontage à l'aide de la commande `umount -f`.

 Warning

Le fait de forcer un démontage interrompt toutes les opérations de lecture ou d'écriture de données qui sont en cours pour le système de fichiers. Consultez la [page de manuel de démontage](#) pour plus d'informations et de conseils sur l'utilisation de cette option.

Transfert de données vers et depuis Amazon EFS

Vous pouvez utiliser AWS DataSync et AWS Transfer Family transférer des données depuis et vers vos systèmes de fichiers Amazon EFS. AWS DataSync est un service de transfert de données en ligne qui permet de copier des données entre le système de fichiers NFS (Network File System), les serveurs de fichiers SMB (Server Message Block), le stockage d'objets autogéré et également entre les services. AWS Pour plus d'informations sur l'utilisation DataSync avec Amazon EFS, consultez [Utilisation AWS DataSync pour transférer des données](#).

AWS Transfer Family est un AWS service entièrement géré que vous pouvez utiliser pour transférer des fichiers vers et depuis les systèmes de fichiers Amazon EFS via le protocole SFTP (Secure File Transfer Protocol), le protocole FTP (File Transfer Protocol) et le protocole FTP via le protocole FTPS (Secure Sockets Layer). Grâce à Transfer Family, vous pouvez permettre à vos partenaires commerciaux d'accéder aux fichiers stockés dans vos systèmes de fichiers Amazon EFS pour des cas d'utilisation tels que la distribution de données, la chaîne logistique, la gestion de contenu et les applications de service Web. Pour de plus amples informations sur l'utilisation de Transfer Family avec Amazon EFS, veuillez consulter [Utilisation AWS Transfer Family pour transférer des données](#).

Rubriques

- [Utilisation AWS DataSync pour transférer des données](#)
- [Utilisation AWS Transfer Family pour transférer des données](#)

Utilisation AWS DataSync pour transférer des données

AWS DataSync est un service de transfert de données en ligne qui simplifie, automatise et accélère le déplacement et la réplication des données entre les systèmes de stockage sur site, ainsi qu'entre les AWS services de stockage. DataSync peut copier des données entre le système de fichiers NFS (Network File System), les serveurs de fichiers SMB (Server Message Block), le stockage d'objets autogéré, les compartiments Amazon AWS Snowball Edge S3, les systèmes de fichiers EFS FSx et les systèmes de fichiers Windows File Server.

Vous pouvez également l'utiliser DataSync pour transférer des fichiers entre deux systèmes de fichiers EFS, y compris des systèmes de fichiers appartenant à des Région AWS s différents et des systèmes de fichiers appartenant à des Compte AWS s différents. DataSync Pour copier des données entre des systèmes de fichiers EFS, vous pouvez effectuer des migrations de données

ponctuelles, une ingestion périodique des données pour les charges de travail distribuées et automatiser la réplication pour la protection et la restauration des données.

Pour plus d'informations, veuillez consulter [Commencer à utiliser Amazon EFS](#) et le [Guide de l'utilisateur AWS DataSync](#).

Utilisation AWS Transfer Family pour transférer des données

AWS Transfer Family est un AWS service entièrement géré que vous pouvez utiliser pour transférer des fichiers vers et depuis les systèmes de fichiers Amazon EFS via les protocoles suivants :

- Protocole de transfert de fichiers Secure Shell (SSH) (SFTP) (AWS Transfer for SFTP)
- Protocole de transfert de fichiers sécurisé (FTPS) (AWS Transfer for FTPS)
- Protocole de transfert de fichiers (FTP) (AWS Transfer for FTP)

Grâce à Transfer Family, vous pouvez permettre à des tiers tels que vos fournisseurs, partenaires ou clients d'accéder en toute sécurité à vos fichiers via les protocoles pris en charge à grande échelle dans le monde entier, sans avoir à gérer d'infrastructure. De plus, vous pouvez désormais accéder facilement à vos systèmes de fichiers EFS à partir d'environnements Windows, macOS et Linux à l'aide de clients SFTP, FTPS et FTP. Cela permet d'étendre l'accessibilité de vos données au-delà des clients et des points d'accès NFS, pour les utilisateurs de plusieurs environnements.

L'utilisation de Transfer Family pour transférer des données dans les systèmes de fichiers Amazon EFS est prise en compte de la même manière que l'utilisation des autres clients. Pour plus d'informations, consultez [Modes de débit](#) et [Quotas Amazon EFS](#).

Pour en savoir plus AWS Transfer Family, consultez le [guide de AWS Transfer Family l'utilisateur](#).

Note

L'utilisation de Transfer Family avec Amazon EFS est désactivée par défaut pour Compte AWS les systèmes de fichiers Amazon EFS dotés de politiques autorisant l'accès public créées avant le 6 janvier 2021. Pour activer l'utilisation de Transfer Family afin d'accéder à votre système de fichiers, contactez Support.

Rubriques

- [Conditions préalables à l'utilisation AWS Transfer Family avec Amazon EFS](#)

- [Configuration de votre système de fichiers EFS pour AWS Transfer Family](#)

Conditions préalables à l'utilisation AWS Transfer Family avec Amazon EFS

Pour utiliser Transfer Family et accéder aux fichiers de votre système de fichiers Amazon EFS, votre configuration doit répondre aux conditions suivantes :

- Le serveur Transfer Family et votre système de fichiers Amazon EFS se trouvent dans le même emplacement Région AWS.
- Les politiques IAM sont configurées pour permettre l'accès au rôle IAM utilisé par Transfer Family. Pour plus d'informations, consultez [Créer un rôle IAM et une politique IAM](#) dans le AWS Transfer Family Guide de l'utilisateur.
- (Facultatif) Si le serveur Transfer Family appartient à un autre compte, activez l'accès intercompte.
 - Assurez-vous que la politique de votre système de fichiers n'autorise pas l'accès public. Pour de plus amples informations, veuillez consulter [Blocage de l'accès public aux systèmes de fichiers EFS](#).
 - Modifiez la politique du système de fichiers pour activer l'accès intercompte. Pour de plus amples informations, veuillez consulter [Configuration de l'accès intercompte pour Transfer Family](#).

Configuration de votre système de fichiers EFS pour AWS Transfer Family

La configuration d'un système de fichiers Amazon EFS pour qu'il fonctionne avec Transfer Family nécessite les étapes suivantes :

- Étape 1. Obtenez la liste des POSIX IDs alloués aux utilisateurs de Transfer Family.
- Étape 2. Assurez-vous que les répertoires de votre système de fichiers sont accessibles aux utilisateurs de Transfer Family en utilisant le POSIX IDs alloué aux utilisateurs de Transfer Family.
- Étape 3. Configurez IAM pour permettre l'accès au rôle IAM utilisé par la Transfer Family.

Configuration des autorisations de fichiers et de répertoires pour les utilisateurs de Transfer Family

Assurez-vous que les utilisateurs de Transfer Family ont accès aux fichiers et aux répertoires nécessaires sur votre système de fichiers EFS. Attribuez des autorisations d'accès au répertoire à l'aide de la liste des POSIX IDs allouées aux utilisateurs de Transfer Family. Dans cet exemple,

un utilisateur crée un répertoire nommé `transferFam` sous le point de montage Amazon EFS. La création d'un répertoire est facultative. Cela dépend de votre cas d'utilisation. Si nécessaire, vous pouvez choisir son nom et son emplacement dans le système de fichiers EFS.

Pour attribuer des autorisations de fichiers et de répertoires aux utilisateurs POSIX pour Transfer Family

1. Connectez-vous à votre EC2 instance Amazon. Amazon EFS prend uniquement en charge le montage par des instances basées sur Linux EC2 .
2. Montez votre système de fichiers EFS s'il n'est pas déjà monté sur l' EC2 instance. Pour de plus amples informations, veuillez consulter [Montage des systèmes de fichiers EFS](#).
3. L'exemple suivant crée le répertoire dans le système de fichiers EFS et remplace son groupe par l'ID de groupe POSIX pour les utilisateurs de Transfer Family, qui est 1101 dans cet exemple.
 - a. Créez le répertoire `efs/transferFam` à l'aide des commandes suivantes. En pratique, vous pouvez utiliser un nom et un emplacement sur le système de fichiers de votre choix.

```
[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. Utilisez la commande suivante pour remplacer le groupe par le GID POSIX attribué aux utilisateurs de Transfer Family. `efs/transferFam`

```
[ec2-user@ip-192-0-2-0 ~]$ sudo chown :1101 efs/transferFam/
```

- c. Confirmez la modification.

```
[ec2-user@ip-192-0-2-0 ~]$ ls -l efs
total 0
drwxr-xr-x 2 root 1101 6 Jan  6 15:58 transferFam
```

Configurez IAM pour permettre l'accès au rôle IAM utilisé par la Transfer Family.

Dans Transfer Family, vous créez une politique IAM basée sur les ressources et un rôle IAM qui définissent l'accès des utilisateurs au système de fichiers EFS. Pour plus d'informations, consultez [Créer un rôle IAM et une politique IAM](#) dans le AWS Transfer Family Guide de l'utilisateur. Vous devez accorder à ce rôle IAM Transfer Family l'accès à votre système de fichiers EFS à l'aide d'une politique d'identité IAM ou d'une politique de système de fichiers.

Voici un exemple de politique de système de fichiers qui accorde les accès ClientMount (lecture) et ClientWrite au rôle EFS-role-for-transfer IAM.

```
{
  "Version": "2012-10-17",
  "Id": "efs-policy-wizard-8698b356-4212-4d30-901e-ad2030b57762",
  "Statement": [
    {
      "Sid": "Grant-transfer-role-access",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/EFS-role-for-transfer"
      },
      "Action": [
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientMount"
      ]
    }
  ]
}
```

Pour plus d'informations sur la création d'un système de fichiers, consultez [Création de politiques de système de fichiers](#). Pour plus d'informations sur l'utilisation de stratégies IAM basées sur l'identité pour gérer l'accès aux ressources EFS, consultez [Politiques basées sur l'identité pour Amazon EFS](#).

Configuration de l'accès intercompte pour Transfer Family

Si le serveur Transfer Family utilisé pour accéder à votre système de fichiers appartient à un autre serveur Compte AWS, vous devez autoriser ce compte à accéder à votre système de fichiers. De plus, la politique de votre système de fichiers doit être non publique. Pour plus d'informations sur le blocage de l'accès public à votre système de fichiers, consultez [Blocage de l'accès public aux systèmes de fichiers EFS](#).

Vous pouvez accorder un Compte AWS accès différent à votre système de fichiers dans la politique du système de fichiers. Dans la console Amazon EFS, utilisez la section Accorder des autorisations supplémentaires de l'éditeur de politique du système de fichiers pour spécifier le niveau Compte AWS et le niveau d'accès au système de fichiers que vous accordez. Pour plus d'informations sur la création ou la modification d'une stratégie de système de fichiers, consultez [Création de politiques de système de fichiers](#).

Vous pouvez spécifier le compte à l'aide de l'ID de compte ou de l'Amazon Resource Name (ARN). Pour plus d'informations ARNs, consultez la section [IAM ARNs](#) dans le guide de l'utilisateur d'IAM.

L'exemple suivant est une politique de système de fichiers non public qui accorde un accès intercompte au système de fichiers. Il comporte les deux instructions suivantes :

1. La première instruction, `NFS-client-read-write-via-fsmt`, accorde des privilèges de lecture, d'écriture et de racine aux clients NFS accédant au système de fichiers à l'aide d'une cible de montage du système de fichiers.
2. La deuxième instruction accorde uniquement des privilèges de lecture et d'écriture au Compte AWS 111122223333, qui est le compte propriétaire du serveur Transfer Family qui doit accéder à ce système de fichiers EFS dans votre compte. `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 politique de système de fichiers suivante ajoute une déclaration accordant l'accès au rôle IAM utilisé par 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"
    ]
  }
]
```

Gestion des systèmes de fichiers EFS

Les tâches de gestion du système de fichiers incluent la gestion de l'accessibilité au réseau d'un système de fichiers avec des cibles de montage, la modification de son mode de débit, la mise à jour de ses politiques de cycle de vie et la gestion de son chiffrement.

Vous pouvez effectuer ces tâches de gestion du système de fichiers à l'aide du AWS Management Console AWS Command Line Interface (AWS CLI) ou de l'API par programmation, comme indiqué dans les sections suivantes.

Rubriques

- [Comprendre l'état du système de fichiers](#)
- [Gérer des cibles de Montage](#)
- [Gestion du débit du système de fichiers](#)
- [Gestion du cycle de vie du stockage](#)
- [Gestion de l'accès aux systèmes de fichiers chiffrés](#)

Comprendre l'état du système de fichiers

Vous pouvez consulter l'état des systèmes de fichiers Amazon EFS à l'aide de la console Amazon EFS ou du AWS CLI. Un système de fichiers Amazon EFS peut avoir l'une des valeurs d'état décrites dans le tableau suivant.

État du système de fichiers	Description
DISPONIBLE	Le système de fichiers est en bon état, accessible et prêt à être utilisé.
CREAtION	Amazon EFS est en train de créer le nouveau système de fichiers.
SUPPRESSION	Amazon EFS supprime le système de fichiers en réponse à une demande de suppression initiée par l'utilisateur. Pour de plus amples informations, veuillez consulter Suppression de systèmes de fichiers EFS .

État du système de fichiers	Description
SUPPRIMÉ	Amazon EFS a supprimé le système de fichiers en réponse à une demande de suppression initiée par l'utilisateur. Pour de plus amples informations, veuillez consulter Suppression de systèmes de fichiers EFS .
MISE À JOUR	Le système de fichiers est en cours de mise à jour en réponse à une demande de mise à jour initiée par l'utilisateur.
ERROR	Applicable aux systèmes de fichiers Zone unique, y compris les systèmes de fichiers dans une configuration de réplication. Le système de fichiers est en panne et est irrécupérable. Pour accéder aux données du système de fichiers, restaurez une sauvegarde de ce système de fichiers sur un nouveau système de fichiers. Pour de plus amples informations, consultez Sauvegarde et réplication de données dans Amazon EFS.

Gérer des cibles de Montage

Vous montez votre système de fichiers sur Amazon EC2 ou sur une autre instance de AWS calcul dans votre cloud privé virtuel (VPC) à l'aide d'une ou de plusieurs cibles de montage que vous créez pour le système de fichiers. Vous pouvez créer la cible de montage lorsque vous créez le système de fichiers ou après avoir créé le système de fichiers.

Après avoir créé une cible de montage pour un système de fichiers, vous pouvez créer des cibles de montage supplémentaires, supprimer des cibles de montage et modifier les groupes de sécurité pour les cibles de montage. Si vous souhaitez modifier le VPC pour les cibles de montage, vous devez d'abord supprimer les cibles de montage existantes.

Note

Vous ne pouvez pas Modifier l'adresse IP d'une cible de Montage existante. Pour modifier une adresse IP, vous devez supprimer la cible de montage et en créer une nouvelle avec la nouvelle adresse.

Rubriques

- [Cibles de montage et zones de disponibilité](#)
- [Création de cibles de montage](#)
- [Supprimer des cibles de montage](#)
- [Modification du VPC cible de montage](#)
- [Modification des groupes de sécurité cibles de montage](#)

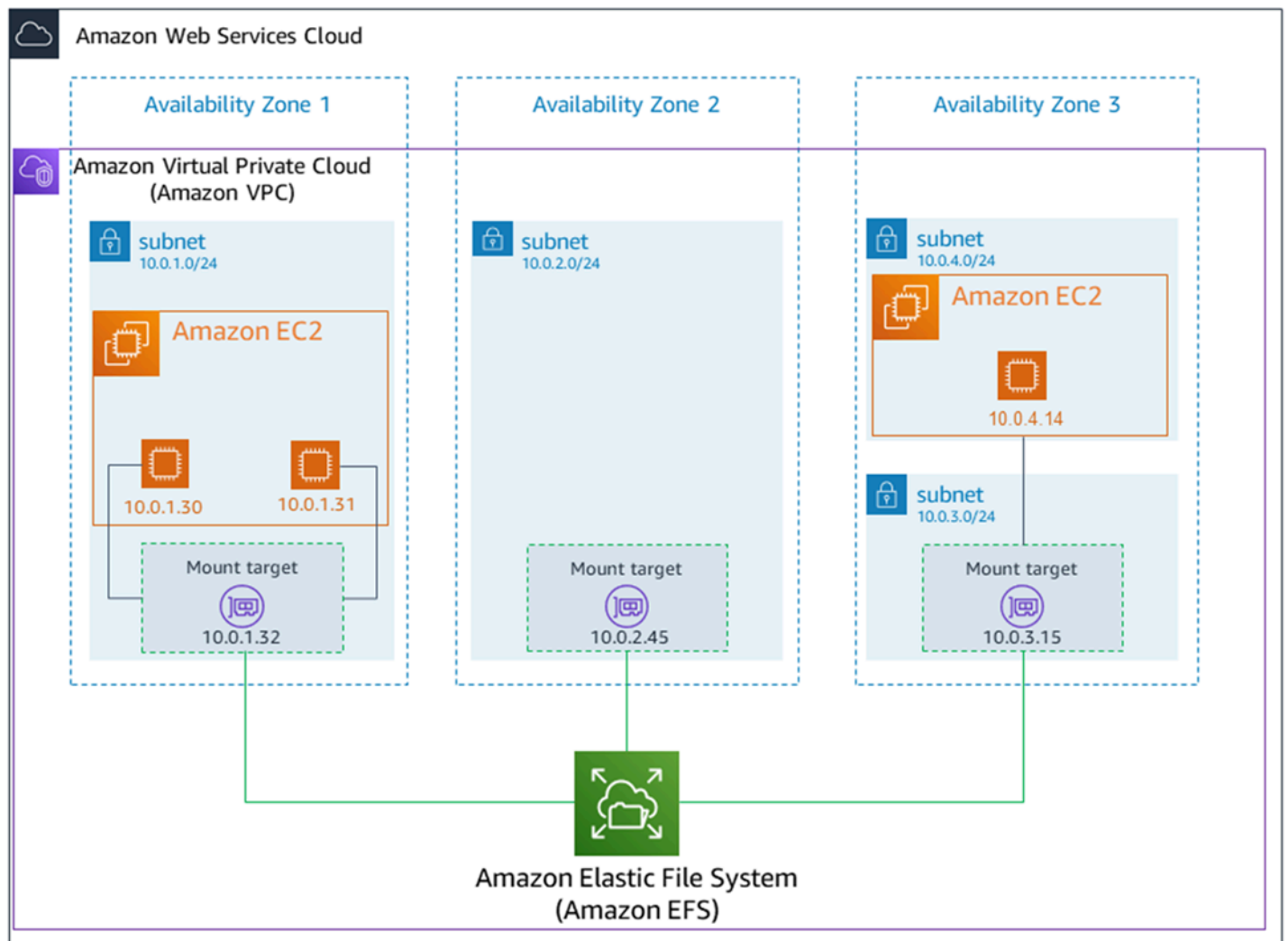
Cibles de montage et zones de disponibilité

Pour les systèmes de fichiers EFS qui utilisent des classes de stockage régionales, vous pouvez créer une cible de montage dans chaque zone de disponibilité d'une Région AWS.

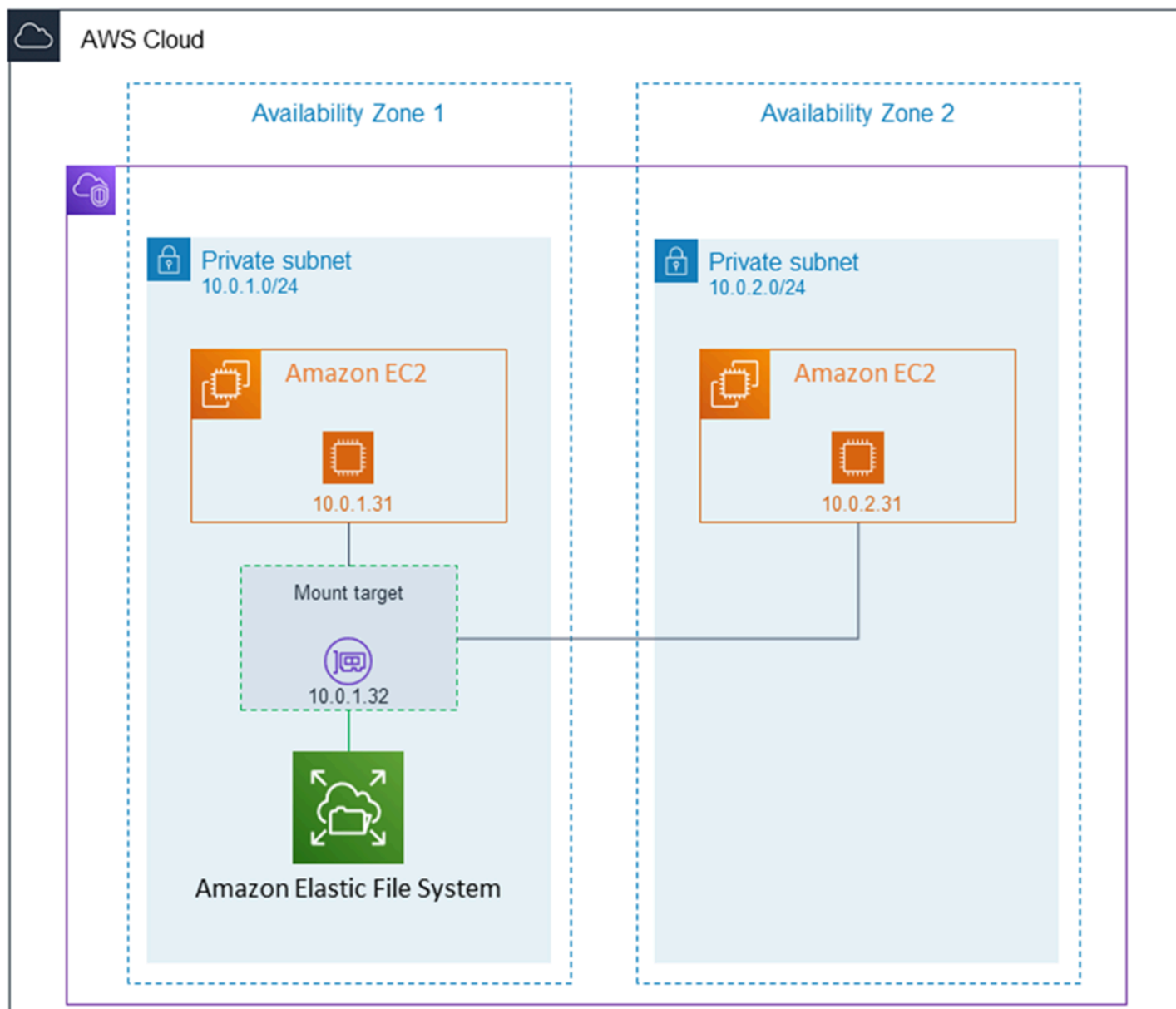
Pour les systèmes de fichiers One Zone, vous ne pouvez créer qu'une cible de montage unique dans la même zone de disponibilité que le système de fichiers. Vous pouvez ensuite monter le système de fichiers sur des instances de calcul, notamment Amazon EC2, Amazon ECS, et AWS Lambda dans votre cloud privé virtuel (VPC).

Le schéma suivant montre un système de fichiers régional avec des cibles de montage créées dans toutes les zones de disponibilité du VPC. L'illustration montre trois EC2 instances lancées dans différents sous-réseaux VPC accédant à un système de fichiers EFS. L'illustration montre également une cible de Montage dans chacune des Zones de disponibilité (quel que soit le nombre de sous-réseaux dans chaque Zone de disponibilité).

Vous pouvez créer un seul Montage cible par Zone de disponibilité. Si une Zone de disponibilité comporte plusieurs sous-réseaux, comme indiqué dans l'une des zones de l'illustration, vous créez une cible de Montage dans un seul des sous-réseaux. Tant que vous avez une cible de montage dans une zone de disponibilité, les EC2 instances lancées dans l'un de ses sous-réseaux peuvent partager la même cible de montage.



Le schéma suivant montre un système de fichiers One Zone, avec une cible de montage unique créée dans la même zone de disponibilité que le système de fichiers. L'accès au système de fichiers à l'aide de l'EC2 instance dans la zone de us-west2c disponibilité entraîne des frais d'accès aux données car elle se trouve dans une zone de disponibilité différente de celle de la cible de montage.



Le groupe de sécurité de la cible de montage fait office de pare-feu virtuel contrôlant le trafic. Par exemple, il détermine les clients qui peuvent accéder au système de fichiers. Cette section décrit les éléments suivants :

- Gestion des groupes de sécurité de cible de montage et activation du trafic.
- Montage du système de fichiers sur vos clients.
- Considérations relatives aux autorisations de niveau NFS.

Au départ, seul l'utilisateur root de l'EC2 instance Amazon dispose d' read-write-
execute autorisations sur le système de fichiers. Cette rubrique décrit les autorisation de niveau

NFS et fournit des exemples qui expliquent comment accorder des autorisations dans des scénarios courants. Pour de plus amples informations, veuillez consulter [Utilisateurs, groupes et autorisations au niveau du système de fichiers réseau \(NFS\)](#).

Création de cibles de montage

Pour accéder à un système de fichiers EFS dans un VPC, vous devez créer des cibles de montage pour le système de fichiers.

Pour un système de fichiers EFS, ce qui suit est vrai :

- Vous pouvez créer des cibles de montage pour le système de fichiers dans un VPC à la fois. Si vous souhaitez accéder au système de fichiers depuis un autre VPC, vous devez supprimer les cibles de montage du VPC actuel, puis créer de nouvelles cibles de montage dans l'autre VPC. Pour de plus amples informations, veuillez consulter [Modification du VPC cible de montage](#).
- Si le VPC comporte plusieurs sous-réseaux dans une Zone de disponibilité, vous pouvez créer une cible de Montage dans une seul de ces sous-réseaux. Toutes les EC2 instances de la zone de disponibilité peuvent partager la cible de montage unique.
- Vous devez au minimum créer une cible de montage dans chaque zone de disponibilité à partir de laquelle vous souhaitez accéder au système de fichiers.

Note

Le montage d'un système de fichiers sur une EC2 instance d'une zone de disponibilité par le biais d'une cible de montage créée dans une autre zone de disponibilité comporte des considérations financières. Pour plus d'informations, consultez la section [Tarification d'Amazon EFS](#). En outre, en utilisant systématiquement un système local de Montage cible dans la Zone de disponibilité de l'instance, vous éliminez un scénario d'échec partiel. Si la zone de la cible de Montage est défaillante, vous ne pouvez pas accéder à votre système de fichiers par le biais de cette cible de Montage.

Vous pouvez créer des cibles de montage pour un système de fichiers en utilisant le AWS Management Console AWS CLI, ou par programmation en utilisant le. AWS SDKs Dans la console, vous pouvez créer des cibles de montage lorsque vous créez le système de fichiers ou après sa

création. Pour obtenir des instructions sur la création de cibles de montage lors de la création d'un système de fichiers, consultez [Création personnalisée à l'aide de la console](#).

Utilisation de la console

Utilisez la procédure suivante pour ajouter des cibles de montage à un système de fichiers EFS existant.

Pour créer une cible de montage sur un système de fichiers EFS

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis sélectionnez le système de fichiers pour lequel vous souhaitez modifier le VPC.
3. Choisissez Réseau, puis Gérer pour afficher les cibles de montage du système de fichiers.
4. Choisissez le système de fichiers auquel vous souhaitez ajouter des cibles de montage en choisissant son nom ou son ID de système de fichiers.

Note

Pour les systèmes de fichiers One Zone, vous ne pouvez créer qu'une seule cible de montage située dans la même zone de disponibilité que le système de fichiers.

5. Pour les systèmes de fichiers qui utilisent les classes de stockage régionales EFS, choisissez Ajouter une cible de montage pour chaque cible de montage que vous souhaitez créer pour le système de fichiers.
6. Définissez les paramètres de la cible de montage :
 - a. Choisissez la zone de disponibilité et l'ID de sous-réseau pour la cible de montage.
 - b. Pour le type d'adresse IP, choisissez de IPv4 ne prendre en charge que IPv4 les adresses, IPv6 uniquement pour prendre en charge IPv6 les adresses, ou Dual-Stack pour prendre en charge IPv4 les deux IPv6 adresses.

Note

Le type d'adresse IP doit correspondre au type IP du sous-réseau. En outre, le type d'adresse IP remplace l'attribut d'adressage IP de votre sous-réseau. Par exemple, si le type d'adresse IP est IPv4 -only et que l'attribut d'IPv6 adressage est activé pour votre sous-réseau, les interfaces réseau créées dans le sous-réseau reçoivent

une IPv4 adresse provenant de la plage du sous-réseau. Pour plus d'informations, consultez [Modifier les attributs d'adressage IP de votre sous-réseau](#).

- c. Si vous connaissez l'adresse IP où vous souhaitez placer la cible de montage, saisissez-la dans le champ Adresse IP correspondant au type d'adresse IP. Si vous ne spécifiez aucune valeur, Amazon EFS sélectionne une adresse IP non utilisée dans le sous-réseau spécifié.

 Note

Vous ne pouvez pas modifier l'adresse IP d'une cible de montage une fois celle-ci créée. Pour modifier une adresse IP, vous devez supprimer la cible de montage et en créer une nouvelle avec la nouvelle adresse.

7. Choisissez au moins un groupe de sécurité à associer à la cible de montage. Vous pourrez [modifier les groupes de sécurité](#) ultérieurement.
8. Choisissez Enregistrer.

En utilisant le AWS CLI

Cette section fournit des exemples de création d'une cible de montage à l' AWS CLI aide de la `create-mount-target` commande. La commande API équivalente est [CreateMountTarget](#).

- Si vous ne spécifiez aucun type d'adresse IP pour la cible de montage, l'option IPv4 -only est utilisée.
- Si vous ne spécifiez pas d'adresse IP pour la cible de montage, Amazon EFS attribue une adresse disponible sur le sous-réseau spécifié.
- Le type d'adresse IP remplace l'attribut d'adressage IP de votre sous-réseau. Par exemple, si le type d'adresse IP est IPv4 -only et que l'attribut d' IPv6 adressage est activé pour votre sous-réseau, les interfaces réseau créées dans le sous-réseau reçoivent une IPv4 adresse provenant de la plage du sous-réseau. Pour plus d'informations, consultez [Modifier les attributs d'adressage IP de votre sous-réseau](#).

 Note

Pour les systèmes de fichiers One Zone, vous ne pouvez créer qu'une seule cible de montage située dans la même zone de disponibilité que le système de fichiers.

Exemple : créer une cible de montage à une IPv4 adresse disponible sur un sous-réseau

La commande suivante spécifie le système de fichiers, le sous-réseau et le groupe de sécurité pour la cible de montage. La cible est créée à une IPv4 adresse disponible sur le sous-réseau spécifié.

```
$ 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 \  

```

L'exemple suivant présente la commande avec des exemples de données.

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

```

Une fois la cible de montage créée, Amazon EFS renvoie la description de la cible de montage au format JSON, comme illustré dans l'exemple suivant.

```
{  
  "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"  
}
```

Exemple : créer une cible de montage à une IPv4 adresse spécifique

La commande suivante indique le système de fichiers, le sous-réseau, le groupe de sécurité et l'IPv4 adresse à utiliser pour la cible de montage. La cible est créée à l'IPv4 adresse spécifiée sur le sous-réseau spécifié.

```
$ 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 \  

```

L'exemple suivant présente la commande avec des exemples de données.

```
$ 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 \  

```

Une fois la cible de montage créée, Amazon EFS renvoie la description de la cible de montage au format JSON, comme illustré dans l'exemple suivant.

```
{  
  "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"  
}
```

Exemple : créer une cible de montage à une IPv6 adresse spécifique

La commande suivante indique le système de fichiers, le sous-réseau, le groupe de sécurité et l'IPv6 adresse à utiliser pour la cible de montage. La cible est créée à l'IPv6 adresse spécifiée sur le sous-réseau spécifié.

```
$ 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 \
```

L'exemple suivant présente la commande avec des exemples de données.

```
$ 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 \
```

Une fois la cible de montage créée, Amazon EFS renvoie la description de la cible de montage au format JSON, comme illustré dans l'exemple suivant.

```
{  
  "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"  
}
```

Exemple : créer une cible de montage à une IPv4 adresse disponible sur un sous-réseau à double pile

La commande spécifie le système de fichiers, le sous-réseau, le groupe de sécurité, le type d'adresse IP à double pile et l'IPv6 adresse de la cible de montage. La cible est créée à une IPv4 adresse disponible et à l'IPv6 adresse spécifiée sur le sous-réseau à double pile.

```
$ 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 \
```

L'exemple suivant présente la commande avec des exemples de données.

```
$ 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 \
```

Une fois la cible de montage créée, Amazon EFS renvoie la description de la cible de montage au format JSON, comme illustré dans l'exemple suivant.

```
{  
  "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"  
}
```

Supprimer des cibles de montage

Lorsque vous supprimez une cible de montage, l'opération interrompt de force tous les montages du système de fichiers, ce qui peut perturber les instances ou les applications utilisant ces montages. Pour éviter toute perturbation des applications, arrêtez-les et démontez le système de fichiers avant de supprimer la cible de Montage. Pour de plus amples informations, veuillez consulter [Démontage des systèmes de fichiers](#).

Vous pouvez supprimer les cibles de montage d'un système de fichiers en utilisant le AWS Management Console AWS CLI, ou par programmation en utilisant le AWS SDKs

Utilisation de la console

Utilisez la procédure suivante pour supprimer les cibles de montage d'un système de fichiers EFS existant.

Pour supprimer des cibles de montage sur un système de fichiers EFS

1. Démontez le système de fichiers. Pour obtenir des instructions, veuillez consulter [Démontage des systèmes de fichiers](#).
2. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
3. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis sélectionnez le système de fichiers pour lequel vous souhaitez supprimer la cible de montage.
4. Choisissez Réseau, puis Gérer pour afficher les cibles de montage du système de fichiers.
5. Pour chaque cible de montage que vous souhaitez supprimer, choisissez Supprimer.
6. Choisissez Enregistrer.

En utilisant le AWS CLI

Pour supprimer une cible de montage existante, utilisez la `delete-mount-target` AWS CLI commande (l'opération correspondante est [DeleteMountTarget](#)), comme indiqué ci-dessous.

Note

Avant de supprimer une cible de montage, démontez le système de fichiers.

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

Voici un exemple de données pour un tel cas :

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

```

Modification du VPC cible de montage

Vous pouvez utiliser un système de fichiers EFS dans un VPC basé sur le service Amazon VPC à la fois. Autrement dit, vous créez des cibles de Montage dans un VPC pour votre système de fichiers, puis vous utilisez ces cibles de Montage pour permettre l'accès au système de fichiers.

Vous pouvez monter le système de fichiers EFS à partir des cibles suivantes :

- EC2 Instances Amazon dans le même VPC
- EC2 instances d'un VPC connectées par peering VPC
- Serveurs sur site en utilisant AWS Direct Connect
- Serveurs sur site via un réseau privé AWS virtuel (VPN) à l'aide d'Amazon VPC

Une connexion d'appairage VPC est une connexion réseau entre deux personnes VPCs qui vous permet d'acheminer le trafic entre elles. La connexion peut utiliser le protocole Internet privé version 4 (IPv4) ou version 6 (IPv6). Pour plus d'informations sur le fonctionnement d'Amazon EFS avec l'appairage de VPC, consultez [Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC](#).

Pour modifier le VPC d'un système de fichiers

Voici les étapes que vous allez effectuer pour modifier le VPC pour la configuration réseau d'un système de fichiers EFS.

1. Supprimez chaque cible de montage attribuée au système de fichiers. Pour obtenir des instructions, veuillez consulter [Supprimer des cibles de montage](#).
2. Lorsque l'état des cibles de montage pour chaque cible de montage est supprimé, attribuez le nouveau VPC et créez de nouvelles cibles de montage pour le système de fichiers. Pour obtenir des instructions, veuillez consulter [Création de cibles de montage](#).

Modification des groupes de sécurité cibles de montage

Les groupes de sécurité définissent les accès entrant et sortant. Lorsque vous Modifiez les groupes de sécurité associés à une cible de Montage, assurez-vous que vous autorisez les accès entrant et sortant nécessaires. Cela permet à votre EC2 instance de communiquer avec le système de fichiers. Pour plus d'informations sur les groupes de sécurité, consultez [Utilisation de groupes de sécurité VPC](#).

Vous pouvez ajouter ou supprimer des groupes de sécurité pour la cible de montage d'un système de fichiers en utilisant le AWS Management Console AWS CLI, ou par programmation en utilisant le AWS SDKs

Utilisation de la console

Pour modifier les groupes de sécurité pour les cibles de montage

Utilisez la procédure suivante pour ajouter ou supprimer des groupes de sécurité cibles de montage pour un système de fichiers EFS existant.

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis sélectionnez le système de fichiers pour lequel vous souhaitez gérer les cibles de montage.
3. Choisissez Réseau, puis Gérer pour afficher les cibles de montage du système de fichiers.
4. Pour supprimer un groupe de sécurité d'une cible de montage, choisissez X à côté de l'ID du groupe de sécurité.
5. Pour ajouter un groupe de sécurité à une cible de montage, choisissez la sécurité dans la liste des groupes de sécurité.
6. Choisissez Enregistrer.

En utilisant le AWS CLI

Pour modifier les groupes de sécurité en vigueur pour une cible de montage, utilisez la `modify-mount-target-security-group` AWS CLI commande (l'opération correspondante est [ModifyMountTargetSecurityGroups](#)) pour remplacer les groupes de sécurité existants, comme indiqué ci-dessous.

```
$ 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
```

Voici un exemple de données pour un tel cas :

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

```
--region us-east-2
```

Gestion du débit du système de fichiers

Le débit élastique est le mode de débit par défaut de la console Amazon EFS et il est recommandé dans la plupart des cas d'utilisation. Le débit élastique permet d'augmenter ou de réduire automatiquement les performances pour répondre aux besoins de l'activité de votre charge de travail. Si, toutefois, vous connaissez les Modèles d'accès spécifiques à vos charges de travail (notamment le débit, la latence et les besoins de stockage), vous pouvez choisir de Modifier le mode de débit.

Note

Bien que le débit élastique soit conçu pour s'adapter de manière élastique à votre débit, nous vous recommandons de mettre en œuvre une gouvernance appropriée en surveillant les indicateurs avec des indicateurs CloudWatch (mesurésIOBytes) et des alertes d'utilisation dans le cadre de vos meilleures pratiques opérationnelles. Cela vous permet de maintenir une utilisation optimale des ressources et de respecter les paramètres opérationnels planifiés. Pour de plus amples informations, veuillez consulter [Surveillance des métriques avec Amazon CloudWatch](#).

Les autres modes de débit que vous pouvez choisir sont les suivants :

- Débit alloué – Vous spécifiez le niveau de débit que le système de fichiers peut gérer indépendamment de la taille du système de fichiers ou de l'augmentation du solde créditeur.
- Débit en rafales – Le débit s'adapte à la quantité de stockage de votre système de fichiers et permet de passer à des niveaux supérieurs jusqu'à 12 heures par jour.

Pour plus d'informations sur les modes de débit Amazon EFS, consultez [Modes de débit](#).

Note

Vous pouvez Modifier le mode de débit et le débit alloué une fois que le système de fichiers est disponible. Le changement de mode de débit n'entraîne pas d'interruption des applications. Toutefois, chaque fois que vous Modifiez le système de fichiers en mode Débit alloué ou que vous augmentez le débit alloué, vous devez attendre au Moins 24 heures avant de pouvoir Modifier à nouveau le mode de débit ou diminuer le Montant alloué.

Vous pouvez gérer le mode de débit du système de fichiers à l'aide de la console Amazon EFS, du AWS Command Line Interface (AWS CLI) et de l'API Amazon EFS.

Utilisation de la console

Pour gérer le débit du système de fichiers

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers pour afficher la liste des systèmes de fichiers EFS de votre compte.
3. Choisissez le système de fichiers dont vous souhaitez modifier le mode de débit.
4. Sur la page de détails du système de fichiers, dans la section Général, choisissez Modifier. La page Modifier s'affiche.
5. Modifiez le paramètre du mode Débit.
 - Pour utiliser le débit élastique ou le débit alloué, choisissez Améliorée, puis élastique ou Alloué.

Si vous choisissez Provisioned, dans Débit provisionné (MiB/s), entrez le débit à allouer pour les requêtes du système de fichiers. La valeur du Débit de lecture maximal affichée est trois fois supérieure à celle du débit saisi. Les systèmes de fichiers EFS mesurent les demandes de lecture à un tiers du taux des autres demandes. Une fois que vous avez indiqué le débit, une estimation du coût mensuel du système de fichiers s'affiche.

Note

Vous pouvez Modifier le mode de débit et le débit alloué une fois que le système de fichiers est disponible. Toutefois, chaque fois que vous modifiez le débit du système de fichiers sur Provisioned ou que vous augmentez le débit provisionné, vous devez attendre au moins 24 heures avant de pouvoir modifier à nouveau le mode de débit ou diminuer le montant provisionné.

- Pour utiliser le débit en rafale, choisissez En rafale.

Pour plus d'informations sur le choix du mode de débit adapté à vos besoins en termes de performances, consultez [Modes de débit](#).

6. Choisissez Enregistrer les Modifications pour appliquer vos Modifications.

En utilisant le AWS CLI

Utilisez la commande [update-file-system](#) CLI ou l'action [UpdateFileSystem](#) API pour modifier le mode de débit d'un système de fichiers.

Gestion du cycle de vie du stockage

Vous pouvez gérer vos systèmes de fichiers de manière à ce qu'ils disposent d'un stockage rentable tout au long de leur cycle de vie. Utilisez la gestion du cycle de vie pour transférer automatiquement les données entre les classes de stockage en fonction de la configuration du cycle de vie du système de fichiers. La configuration du cycle de vie comprend trois politiques de cycle de vie que vous définissez pour le système de fichiers.

Les politiques de cycle de vie indiquent à la gestion du cycle de vie à quel moment transférer des fichiers vers et depuis les classes de stockage EFS Infrequent Access (IA) et EFS Archive. La durée de transition est basée sur la date du dernier accès aux fichiers dans la classe de stockage Standard. Pour déterminer l'heure du dernier accès dans la classe de stockage Standard, un temporisateur interne suit la date du dernier accès à un fichier (et non les attributs du système de fichiers POSIX qui sont accessibles au public). Chaque fois qu'un fichier est consulté dans Standard, le temporisateur de gestion du cycle de vie est réinitialisé.

Les politiques de cycle de vie s'appliquent à l'ensemble du système de fichiers EFS.

Les politiques de cycle de vie de l'EFS sont les suivantes :

- Transition vers l'IA : indique à la gestion du cycle de vie à quel moment déplacer les fichiers vers le stockage à accès peu fréquent, qui est optimisé en termes de coûts pour les données auxquelles on accède seulement quelques fois par trimestre. Par défaut, les fichiers qui ne sont pas accessibles dans le stockage standard pendant 30 jours sont transférés vers IA.
- Transition vers l'archivage : indique à la gestion du cycle de vie à quel moment déplacer les fichiers vers la classe de stockage Archive, qui est optimisée en termes de coûts pour les données consultées seulement quelques fois par an ou moins. Par défaut, les fichiers qui ne sont pas accessibles dans le stockage standard pendant 30 jours sont transférés vers IA.
- Transition vers le standard : indique à la gestion du cycle de vie s'il convient de transférer les fichiers hors IA ou Archive et de les remettre dans le stockage standard lorsque les fichiers sont accessibles dans le stockage IA ou Archive. Par défaut, les fichiers ne sont pas replacés dans le stockage standard et restent dans la classe de stockage IA ou Archive lors de l'accès.

Pour les cas d'utilisation sensibles aux performances qui exigent les performances de latence les plus rapides (comme les applications qui fonctionnent avec un grand volume de petits fichiers), choisissez de transférer les fichiers vers le stockage standard Dès le premier accès.

Pour plus d'informations sur la configuration des stratégies de cycle de vie pour un système de fichiers, consultez [Configuration des politiques de cycle de vie](#).

Opérations sur le système de fichiers pour la gestion du cycle de vie

Les opérations du système de fichiers pour la gestion du cycle de vie sont Moins prioritaires que les opérations pour les charges de travail du système de fichiers EFS. Le temps nécessaire pour transférer des fichiers vers ou hors du stockage IA et Archive varie en fonction de la taille du fichier et de la charge de travail du système de fichiers. Par exemple, la transition de millions de petits fichiers peut prendre plus de temps que la transition de moins de fichiers plus volumineux ayant la même taille de stockage totale.

Les métadonnées de fichier, telles que les noms de fichiers, les informations de propriété et la structure de répertoires du système de fichiers, sont toujours stockées dans le Standard afin de garantir des performances de métadonnées constantes.

Les opérations de métadonnées pour les systèmes de fichiers dans le stockage IA ou Archive, telles que la liste du contenu d'un répertoire, ne sont pas considérées comme des accès aux fichiers. Lors de la transition du contenu d'un fichier vers les classes de stockage IA ou Archive, le fichier est stocké dans la classe de stockage Standard et est facturé à ce tarif de stockage.

Toutes les opérations d'écriture sur les fichiers des classes de stockage IA ou Archive du système de fichiers sont d'abord écrites dans des classes de stockage standard, puis peuvent être transférées vers la classe de stockage applicable après 24 heures.

Configuration des politiques de cycle de vie

Lorsque vous créez un système de fichiers EFS doté des paramètres recommandés à l'aide de AWS Management Console, le système de fichiers est automatiquement configuré avec la configuration de cycle de vie par défaut suivante :

- Transition vers IA définie sur 30 jours depuis le dernier accès.
- Transition vers Archive définie sur 90 jours depuis le dernier accès.
- Transition vers Standard définie sur Aucun.

Vous pouvez modifier les politiques de cycle de vie par défaut lors de la création d'un système de fichiers avec des paramètres personnalisés à l'aide du AWS Management Console ou lors de la création d'un système de fichiers à l'aide du AWS CLI. Vous pouvez également modifier les politiques une fois le système de fichiers créé, comme décrit dans les procédures suivantes.

Utilisation de la console

Vous pouvez utiliser le AWS Management Console pour définir les politiques de cycle de vie d'un système de fichiers existant.

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/efs/>.
2. Choisissez Systèmes de fichiers pour afficher la liste des systèmes de fichiers de votre compte.
3. Choisissez le système de fichiers sur lequel vous souhaitez Modifier les politiques de cycle de vie.
4. Sur la page de détails du système de fichiers, dans la section Général, choisissez Modifier. La page Modifier s'affiche.
5. Pour la gestion du cycle de vie, configurez les politiques de cycle de vie :
 - Réglez Transition vers IA sur l'une des options disponibles. Pour arrêter de déplacer des fichiers vers le stockage IA, choisissez Aucun.
 - Définissez Transition vers l'archivage sur l'une des options disponibles. Pour arrêter le transfert de fichiers vers le stockage d'archives, choisissez Aucun.
 - Définissez Transition vers Standard sur Accès initial pour déplacer les fichiers stockés dans IA vers le stockage standard lorsqu'ils sont utilisés pour des opérations autres que les métadonnées.

Pour arrêter de déplacer des fichiers depuis IA ou Archive vers le stockage standard lors du premier accès, sélectionnez Aucun.
6. Choisissez Enregistrer les Modifications pour enregistrer vos Modifications.

En utilisant le AWS CLI

Vous pouvez utiliser le AWS CLI pour définir ou modifier les politiques de cycle de vie d'un système de fichiers.

- Exécutez la [put-lifecycle-configuration](#) AWS CLI commande ou la commande [PutLifecycleConfiguration](#) API en spécifiant l'ID du système de fichiers pour lequel vous gérez la gestion du cycle de vie.

```
$ 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
```

Vous recevez la réponse suivante.

```
{
  "LifecyclePolicies": [
    {
      "TransitionToIA": "AFTER_60_DAYS"
    },
    {
      "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
    },
    {
      "TransitionToArchive": "AFTER_90_DAYS"
    }
  ]
}
```

Pour arrêter la gestion du cycle de vie pour un système de fichiers existant (CLI)

- Exécutez la commande `put-lifecycle-configuration` en spécifiant l'ID du système de fichiers pour lequel vous souhaitez arrêter la gestion du cycle de vie. Laissez la propriété `--lifecycle-policies` vide.

```
$ aws efs put-lifecycle-configuration \
--file-system-id File-System-ID \
--lifecycle-policies \
--region us-west-2 \
--profile adminuser
```

Vous recevez la réponse suivante.

```
{
  "LifecyclePolicies": []
}
```

Gestion de l'accès aux systèmes de fichiers chiffrés

Vous pouvez créer des systèmes de fichiers chiffrés en utilisant Amazon EFS. Amazon EFS prend en charge deux formes de chiffrement pour les systèmes de fichiers, le chiffrement en transit et le chiffrement au repos. Les opérations de gestion de clés que vous devez effectuer concernent uniquement le chiffrement au repos. Amazon EFS gère automatiquement les clés pour le chiffrement en transit.

Si vous créez un système de fichiers qui utilise le chiffrement au repos, les données et métadonnées sont chiffrées au repos. Amazon EFS utilise AWS Key Management Service (AWS KMS) pour la gestion des clés. Lorsque vous créez un système de fichiers utilisant le chiffrement au repos, vous spécifiez une AWS KMS key. La clé KMS peut être `aws/elasticfilesystem` (celle Clé gérée par AWS pour Amazon EFS) ou il peut s'agir d'une clé gérée par le client que vous gérez.

Les données des fichiers : (le contenu de vos fichiers) sont chiffrées au repos à l'aide de la clé KMS que vous avez spécifiée lors de la création de votre système de fichiers. Les métadonnées : noms de fichiers, noms de répertoires et contenu des répertoires - sont chiffrées à l'aide d'une clé gérée par Amazon EFS.

L'EFS Clé gérée par AWS de votre système de fichiers est utilisé comme clé KMS pour chiffrer les métadonnées de votre système de fichiers, par exemple les noms de fichiers, les noms de répertoires et le contenu des répertoires. Vous êtes le propriétaire de la clé gérée par le client utilisée pour chiffrer les données de fichier (contenu de vos fichiers) au repos.

Vous gérez les personnes ayant accès à vos clés KMS et au contenu de vos systèmes de fichiers chiffrés. Cet accès est contrôlé à la fois par les politiques AWS Identity and Access Management (IAM) et AWS KMS. Les politiques IAM contrôlent l'accès des utilisateurs aux actions de l'API Amazon EFS. AWS KMS les politiques relatives aux clés contrôlent l'accès d'un utilisateur à la clé KMS que vous avez spécifiée lors de la création du système de fichiers. Pour plus d'informations, consultez les ressources suivantes :

- [Utilisateurs IAM](#) dans le Guide utilisateur IAM
- [Politiques clés décrites AWS KMS](#) dans le guide du AWS Key Management Service développeur
- [Les subventions figurent AWS KMS](#) dans le guide du AWS Key Management Service développeur.

En tant qu'administrateur de clé, vous pouvez importer des clés externes. Vous pouvez également les activer, les désactiver ou les supprimer. L'état de la clé KMS que vous avez spécifiée (lors de la création du système de fichiers avec chiffrement au repos) affecte l'accès à son contenu. La clé KMS doit être en bon état pour que les utilisateurs puissent accéder au contenu d'un système de fichiers chiffré à l'aide de cette clé.

Gestion des clés KMS pour les systèmes de fichiers EFS

Vous pouvez désactiver ou supprimer vos clés KMS gérées par le client, ou révoquer l'accès d'Amazon EFS à vos clés KMS. La désactivation et la révocation de l'accès d'Amazon EFS à vos clés sont des actions réversibles. La suppression des clés KMS doit être effectuée avec beaucoup de précaution. La suppression d'une clé KMS est une action irréversible.

Si vous désactivez ou supprimez la clé KMS utilisée pour votre système de fichiers Monté, les conditions suivantes sont remplies :

- Cette clé KMS ne peut pas être utilisée comme clé pour les nouveaux systèmes de fichiers chiffrés.
- Les systèmes de fichiers chiffrés existants qui utilisent cette clé KMS cessent de fonctionner après un certain temps.

Si vous révoquez l'accès d'Amazon EFS à un octroi pour un système de fichiers Monté existant, le comportement est le même que si vous aviez désactivé ou supprimé la clé KMS associée. En d'autres termes, le système de fichiers chiffrés continue de fonctionner, mais cesse de fonctionner après un certain temps.

Vous pouvez empêcher l'accès à un système de fichiers chiffrés doté d'une clé KMS à laquelle vous avez désactivé, supprimé ou révoqué l'accès à Amazon EFS. Pour ce faire, démontez le système de fichiers et supprimez vos cibles de Montage Amazon EFS.

Vous ne pouvez pas supprimer immédiatement un AWS KMS key, mais vous pouvez planifier sa suppression dans un délai de 7 à 30 jours. Quand la suppression d'une clé KMS est planifiée, vous ne pouvez pas l'utiliser pour les opérations de chiffrement. Vous pouvez également annuler une suppression de clé KMS planifiée.

Pour savoir comment désactiver et réactiver les clés KMS gérées par le client, consultez [Activation et désactivation des clés](#) dans le Guide du développeur AWS Key Management Service . Pour savoir comment planifier la suppression des clés KMS gérées par le client, consultez la section [Suppression des clés KMS](#) dans le guide du développeur AWS Key Management Service .

Surveillance d'Amazon EFS

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon EFS et de vos AWS solutions. Nous vous recommandons de collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. Toutefois, avant de commencer la surveillance d'Amazon EFS, créez un plan de surveillance incluant les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

L'étape suivante consiste à établir une référence de performances Amazon EFS normales dans votre environnement, en mesurant la performance à divers Moments et dans diverses conditions de charge. Lorsque vous surveillez Amazon EFS, vous devez envisager de stocker les données de supervision historiques. Ces données stockées constituent une référence pour comparer avec des données de performances actuelles, identifier les Modèles de performance normaux et les anomalies de performance, et concevoir des méthodes pour résoudre les problèmes.

Par exemple, avec Amazon EFS, vous pouvez surveiller le débit du réseau, les E/S pour les opérations de lecture, d'écriture, et les opérations de métadonnées, les connexions client et le solde de crédit des transmissions en rafale pour vos systèmes de fichiers. Si les performances sortent de votre cadre de référence, vous devez peut-être Modifier la taille de votre système de fichiers ou le nombre de clients connectés afin d'optimiser le système de fichiers pour votre charge de travail.

Pour établir une référence, vous devez, au Moins, superviser les éléments suivants :

- Le débit réseau de votre système de fichiers.
- Le nombre de connexions client à un système de fichiers.
- Le nombre d'octets pour chaque opération de système de fichiers, y compris les opérations de lecture des données, d'écriture des données et les opérations de métadonnées.

Rubriques

- [Outils de surveillance](#)
- [Comment Amazon EFS indique les tailles des systèmes de fichiers et des objets](#)
- [Affichage de classe de stockage](#)
- [Surveillance des métriques avec Amazon CloudWatch](#)
- [Journalisation des appels d'API Amazon EFS avec AWS CloudTrail](#)

Outils de surveillance

AWS fournit différents outils que vous pouvez utiliser pour surveiller Amazon EFS. Vous pouvez configurer certains outils pour qu'ils effectuent la supervision automatiquement, tandis que d'autres nécessitent une intervention manuelle. Nous vous recommandons d'automatiser le plus possible les tâches de supervision.

Outils de surveillance automatique

Vous pouvez utiliser les outils de surveillance automatique pour surveiller Amazon EFS et signaler un problème éventuel :

- Amazon CloudWatch Alarms : surveillez une seule métrique sur une période que vous spécifiez et effectuez une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon Simple Notification Service (Amazon SNS) ou à une politique Amazon EC2 Auto Scaling. CloudWatch les alarmes n'appellent pas d'actions uniquement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour de plus amples informations, veuillez consulter [Surveillance des métriques avec Amazon CloudWatch](#).
- Amazon CloudWatch Logs — Surveillez, stockez et accédez à vos fichiers journaux depuis AWS CloudTrail ou d'autres sources. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon CloudWatch Logs ?](#) dans le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Events : associez les événements et acheminez-les vers une ou plusieurs fonctions ou flux cibles afin d'apporter des modifications, de recueillir des informations d'état et de prendre des mesures correctives. Pour plus d'informations, consultez la section [Qu'est-ce qu'Amazon CloudWatch Events](#) dans le guide de CloudWatch l'utilisateur Amazon.

- AWS CloudTrail Surveillance des journaux : partagez les fichiers journaux entre les comptes, surveillez les fichiers CloudTrail CloudWatch journaux en temps réel en les envoyant à Logs, écrivez des applications de traitement des journaux en Java et vérifiez que vos fichiers journaux n'ont pas changé après leur livraison par CloudTrail. Pour plus d'informations, consultez la section [Utilisation des fichiers CloudTrail journaux](#) dans le Guide de AWS CloudTrail l'utilisateur.

Outils de surveillance manuelle

Un autre aspect important de la surveillance d'Amazon EFS consiste à surveiller manuellement les éléments non couverts par les CloudWatch alarmes Amazon. Amazon EFS et d'autres AWS Management Console tableaux de bord fournissent une at-a-glance vue d'ensemble de l'état de votre AWS environnement. CloudWatch Nous vous recommandons de consulter également les fichiers journaux des systèmes de fichiers.

- À partir de la console Amazon EFS, vous pouvez trouver les éléments suivants pour vos systèmes de fichiers :
 - La taille mesurée actuelle
 - Le nombre de cibles de Montage
 - L'état de cycle de vie
- CloudWatch la page d'accueil montre :
 - Alarmes et statuts en cours
 - Graphiques des alarmes et des ressources
 - Statut d'intégrité du service

En outre, vous pouvez utiliser CloudWatch pour effectuer les opérations suivantes :

- Créer des [tableaux de bord personnalisés](#) pour surveiller les services que vous utilisez
- Données de métriques de graphiques pour résoudre les problèmes et découvrir les tendances.
- Recherchez et parcourez tous les indicateurs de vos AWS ressources.
- Créer et Modifier des alarmes pour être informé des problèmes.

Comment Amazon EFS indique les tailles des systèmes de fichiers et des objets

Les sections suivantes décrivent comment Amazon EFS indique la taille des systèmes de fichiers, la taille des objets au sein d'un système de fichiers et le débit du système de fichiers.

Mesurer les objets du système de fichiers EFS

Les objets que vous pouvez visualiser dans un système de fichiers EFS incluent des fichiers ordinaires, des répertoires, des liens symboliques et des fichiers spéciaux (FIFOs et des sockets). Chacun de ces objets est mesuré pour 2 Kio (kibi-octets) de métadonnées (pour son inode) et un ou plusieurs incréments de 4 Kio de données. La liste suivante explique la taille des données mesurées pour différents types d'objets du système de fichiers :

- Fichiers normaux – La taille des données mesurées d'un fichier normal correspond à la taille logique du fichier arrondie à l'incrément suivante de 4 Kio ; elle peut être inférieure pour les fichiers partiellement alloués.

Un fichier partiellement alloué est un fichier dans lequel les données ne sont pas écrites à tous les emplacements du fichier avant qu'il n'atteigne sa taille logique. Pour un fichier partiellement alloué, le stockage réellement utilisé peut être inférieur à la taille logique arrondie aux 4 Kio d'incrément suivants. Dans ce cas, Amazon EFS rapporte le stockage réel utilisé en tant que taille de données mesurée.

- Répertoires - La taille de données mesurée d'un répertoire est le stockage réel utilisé pour les entrées de répertoire et la structure de données qui les détient, arrondie aux 4 Kio d'incrément suivants. La taille des données mesurée n'inclut pas le stockage réellement utilisé par le fichier de données.
- Liens symboliques et fichiers spéciaux – La taille des données mesurées pour ces objets est toujours de 4 Kio.

Lorsqu'Amazon EFS indique l'espace utilisé pour un objet, via l'attribut `space_used` NFSv4 .1, il inclut la taille de données mesurée actuelle de l'objet, mais pas la taille de ses métadonnées. Vous pouvez utiliser deux utilitaires pour mesurer l'utilisation disque d'un fichier : `du` et `stat`. Voici un exemple d'utilisation de l'utilitaire `du` sur un fichier vide qui inclut l'option permettant de renvoyer le résultat en kilo-octets.

```
$ du -k file
```

4 file

L'exemple suivant montre comment utiliser l'utilitaire `stat` sur un fichier vide pour renvoyer l'utilisation du disque par le fichier.

```
$ /usr/bin/stat --format="%b*%B" file | bc
4096
```

Pour mesurer la taille d'un répertoire, utilisez l'utilitaire `stat`. Recherchez la valeur `Blocks` et multipliez-la par la taille de bloc. Voici un exemple illustrant la procédure d'utilisation de l'utilitaire `stat` sur un répertoire vide :

```
$ /usr/bin/stat --format="%b*%B" . | bc
4096
```

Taille mesurée d'un système de fichiers EFS

La taille mesurée d'un système de fichiers EFS inclut la somme des tailles de tous les objets actuels dans toutes les classes de stockage EFS. La taille des objets est calculée à partir d'un échantillon représentatif de leurs tailles au cours de l'heure mesurée, par exemple entre 8 et 9 heures du matin.

Un fichier vide contribue avec 6 kio (2 kio de métadonnées + 4 kio de données) à la taille mesurée de son système de fichiers. Lors de sa création, un système de fichiers comporte un répertoire racine vide unique et par conséquent a une taille mesurée de 6 kio.

Les tailles mesurées d'un système de fichiers particulier définissent l'utilisation pour laquelle le compte propriétaire est facturé pour ce système de fichiers pour cette heure.

Note

La taille mesurée calculée ne représente pas un instantané cohérent du système de fichiers à un Moment donné au cours de cette heure. Au lieu de cela, elle représente les tailles des objets qui existaient dans le système de fichiers à différents Moments au sein de chaque heure, ou éventuellement de l'heure la précédant. Ces tailles sont additionnées afin de déterminer la taille mesurée du système de fichiers pour l'heure. La taille mesurée d'un système de fichiers peut donc être cohérente avec les tailles mesurées des objets stockés lorsqu'il n'y a aucune écriture sur le système de fichiers.

Vous pouvez consulter la taille mesurée d'un système de fichiers EFS de différentes manières :

- À l'aide de la [describe-file-systems](#) AWS CLI commande et de l'opération [DescribeFileSystem](#) API, la réponse inclut les éléments suivants :

```
"SizeInBytes":{
    "Timestamp": 1403301078,
    "Value": 29313744866,
    "ValueInIA": 675432,
    "ValueInStandard": 29312741784
    "ValueInArchive": 327650
}
```

Où la taille mesurée de ValueInStandard est également utilisée pour déterminer votre débit d'E/S de référence et les taux de rafale pour les systèmes de fichiers utilisant le débit de rafale.

- Consultez la StorageBytes CloudWatch métrique, qui affiche la taille totale mesurée des données dans chaque classe de stockage. Pour plus d'informations sur la métrique StorageBytes, consultez [CloudWatch métriques pour Amazon EFS](#).
- Exécutez la df commande sous Linux à l'invite du terminal d'une EC2 instance.

N'utilisez pas la du commande à la racine du système de fichiers à des fins de mesure du stockage, car la réponse ne reflète pas l'ensemble des données utilisées pour mesurer votre système de fichiers.

Note

La taille mesurée de ValueInStandard est également utilisée pour déterminer votre référence de débit d'E-S et les débits de transmission en rafale. Pour de plus amples informations, veuillez consulter [Débit exceptionnel](#).

Mesurer les accès peu fréquents et les classes de stockage d'archives

Les classes de stockage EFS Infrequent Access (IA) et Archive sont mesurées par incréments de 4 KiB et sont soumises à des frais de facturation minimaux par fichier de 128 KiB. Les métadonnées des fichiers IA et Archive (2 KIB par fichier) sont toujours stockées et mesurées dans la classe de stockage Standard. Support pour les fichiers inférieurs à 128 KiB uniquement pour les politiques de

cycle de vie mises à jour le 26 novembre 2023 à 12 h 00 (heure du Pacifique) ou après cette date. L'accès aux données pour le stockage IA et Archive est mesuré par incréments de 128 KiB.

Vous pouvez utiliser la `StorageBytes` CloudWatch métrique pour afficher la taille mesurée des données dans chacune des classes de stockage. La métrique affiche également le nombre total d'octets consommés par l'arrondissement de petits fichiers au sein des classes de stockage IA et Archive. Pour plus d'informations sur l'affichage CloudWatch des métriques, consultez [Accès aux CloudWatch métriques pour Amazon EFS](#). Pour plus d'informations sur la métrique `StorageBytes`, consultez [CloudWatch métriques pour Amazon EFS](#).

Débit de mesure

Amazon EFS mesure le débit des demandes de lecture à un tiers du taux des autres opérations d'E/S du système de fichiers. Par exemple, si vous consommez 30 mégaoctets par seconde (MiBps) de débit en lecture et en écriture, la portion de lecture compte pour 10 MiBps de débit effectif, la portion d'écriture pour 30 MiBps et le débit mesuré combiné est de 40. MiBps Ce débit combiné ajusté en fonction des taux de consommation est reflété dans la `MeteredIOBytes` CloudWatch métrique.

Mesurer le débit élastique

Lorsque le mode débit élastique est activé pour un système de fichiers, vous ne payez que pour la quantité de métadonnées et de données lues ou écrites dans le système de fichiers. Les systèmes de fichiers EFS utilisant le mode de débit élastique mesurent les métadonnées et facturent les lectures sous forme d'opérations de lecture et les écritures de métadonnées sous forme d'opérations d'écriture. Les opérations de métadonnées sont mesurées par incréments de 1 KiB après les 4 premiers KiB. Les opérations de données sont mesurées par incréments de 1 KiB après les 32 premiers KiB.

Note

Bien que le débit élastique soit conçu pour s'adapter de manière élastique à votre débit, nous vous recommandons de mettre en œuvre une gouvernance appropriée en surveillant les indicateurs avec des indicateurs CloudWatch (mesurés `IOBytes`) et des alertes d'utilisation dans le cadre de vos meilleures pratiques opérationnelles. Cela vous permet de maintenir une utilisation optimale des ressources et de respecter les paramètres opérationnels planifiés. Pour de plus amples informations, veuillez consulter [Surveillance des métriques avec Amazon CloudWatch](#).

Mesurer le Débit apalloué

Pour les systèmes de fichiers qui utilisent le mode débit provisionné, vous ne payez que pour la durée pendant laquelle le débit est activé. Amazon EFS mesure les systèmes de fichiers avec le mode de débit provisionné activé une fois par heure. Pour la mesure lorsque le mode de débit provisionné est défini pour moins d'une heure, Amazon EFS calcule la moyenne temporelle à l'aide d'une précision de la milliseconde.

Affichage de classe de stockage

Vous pouvez consulter la quantité de données stockée dans chaque classe de stockage de votre système de fichiers à l'aide de la console Amazon EFS, de l' AWS CLI API EFS ou de l'API EFS.

Utilisation de la console

L'onglet Taille mesurée de la page des détails du système de fichiers affiche la taille mesurée actuelle du système de fichiers en multiples binaires d'octets (kibioctets, mebioctets, gibioctets et tebioctets). La métrique est émise toutes les 15 minutes et vous permet de visualiser la taille mesurée de votre système de fichiers au fil du temps. La taille mesurée affiche les informations suivantes concernant la taille de stockage du système de fichiers :

- La taille totale est la taille (en octets binaires) des données stockées dans le système de fichiers, y compris toutes les classes de stockage.
- La taille en standard est la taille (en octets binaires) des données stockées dans la classe de stockage standard EFS.
- La taille en IA est la taille (en octets binaires) des données stockées dans la classe de stockage EFS Infrequent Access. Les fichiers inférieurs à 128 Ko sont arrondis à 128 Ko.
- La taille dans Archive est la taille (en octets binaires) des données stockées dans la classe de stockage EFS Archive. Les fichiers inférieurs à 128 Ko sont arrondis à 128 Ko.

Vous pouvez également consulter la métrique Storage bytes dans l'onglet Surveillance de la page Détails du système de fichiers de la console Amazon EFS. Pour de plus amples informations, veuillez consulter [Accès aux CloudWatch métriques pour Amazon EFS](#).

En utilisant le AWS CLI

Vous pouvez consulter la quantité de données stockée dans chaque classe de stockage de votre système de fichiers à l'aide de l' AWS CLI API EFS. Consultez les détails de stockage de données

en appelant la commande CLI `describe-file-systems` (l'opération d'API correspondante est [DescribeFileSystems](#)).

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

Dans la réponse, `ValueInIA` affiche la dernière taille mesurée en octets dans la classe de stockage Infrequent Access du système de fichiers. `ValueInStandard` affiche la dernière taille mesurée en octets dans la classe de stockage Standard. `ValueInArchive` affiche la dernière taille mesurée en octets dans la classe de stockage Archive. La somme des trois valeurs est égale à la taille de l'ensemble du système de fichiers, qui est affiché dans `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"
    }
  ]
}
```

Pour s'informer sur les autres façons d'afficher et de mesurer l'utilisation du disque, consultez [Mesurer les objets du système de fichiers EFS](#).

Surveillance des métriques avec Amazon CloudWatch

Vous pouvez surveiller les systèmes de fichiers à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes d'Amazon EFS pour en faire des métriques lisibles en temps quasi réel. Les

statistiques sont enregistrées pour une période de 15 Mois, ce qui vous permet d'avoir une meilleure idée de la performance de votre application ou service web.

Par défaut, les données métriques Amazon EFS sont automatiquement envoyées à des CloudWatch intervalles d'une minute, sauf indication contraire pour certaines mesures individuelles. La console Amazon EFS affiche une série de graphiques basés sur les données brutes d'Amazon CloudWatch. Selon vos besoins, vous préférerez peut-être obtenir les données de vos systèmes de fichiers à partir des graphiques de la console CloudWatch plutôt qu'à partir des graphiques.

Pour plus d'informations sur Amazon CloudWatch, consultez [Qu'est-ce qu'Amazon CloudWatch ?](#) dans le guide de CloudWatch l'utilisateur Amazon.

Les CloudWatch métriques Amazon EFS sont signalées sous forme d'octets bruts. Les octets ne sont pas arrondis à la décimale ou à un multiple binaire de l'unité.

Rubriques

- [CloudWatch métriques pour Amazon EFS](#)
- [Accès aux CloudWatch métriques pour Amazon EFS](#)
- [Utilisation de CloudWatch métriques pour Amazon EFS](#)
- [Utiliser les mathématiques métriques avec CloudWatch les métriques](#)
- [Surveillance des réussites et des échecs des tentatives de montage](#)
- [Création d' CloudWatch alarmes pour surveiller Amazon EFS](#)

CloudWatch métriques pour Amazon EFS

Les métriques Amazon EFS utilisent l'espace de EFS noms. L'espace de noms AWS/EFS inclut les métriques suivantes. Toutes les métriques, à TimeSinceLastSync l'exception de, concernent une seule dimension, FileSystemId. L'ID d'un système de fichiers est disponible dans la console de gestion Amazon EFS et est au format fs-abcdef0123456789a.

TimeSinceLastSync

Indique le temps écoulé depuis la dernière synchronisation réussie avec le système de fichiers de destination dans une configuration de réplication. Toutes les Modifications apportées aux données du système de fichiers source avant la valeur TimeSinceLastSync ont été correctement répliquées. Les Modifications survenues après TimeSinceLastSync risquent de ne pas être entièrement répliquées.

Cette métrique utilise deux dimensions :

- `FileSystemId` — ID du système de fichiers source dans la configuration de réplication.
- `DestinationFileSystemId` — ID du système de fichiers de destination dans la configuration de réplication.

Unités : secondes

Statistiques valides : Minimum, Maximum, Average

PercentIOLimit

Indique comment la fermeture d'un système de fichiers consiste à atteindre la limite d'E/S du mode de performances à usage général.

Unités : pourcentage

Statistiques valides : Minimum, Maximum, Average

BurstCreditBalance

Nombre de crédits de transmission en rafales dont un système de fichiers dispose. Les crédits de transmission en rafales permettent à un système de fichiers d'atteindre des niveaux de débit supérieurs au niveau de départ d'un système de fichiers sur des périodes données.

La statistique `Minimum` correspond au plus petit solde de crédit de transmission en rafales par minute au cours de la période. La statistique `Maximum` correspond au plus grand solde de crédit de transmission en rafales par minute au cours de la période. La statistique `Average` correspond au solde Moyen de crédit de transmission en rafales au cours de la période.

Unités : octets

Statistiques valides : Minimum, Maximum, Average

PermittedThroughput

Le débit maximum qu'un système de fichiers peut gérer.

- Pour les systèmes de fichiers utilisant le débit élastique, cette valeur reflète le débit d'écriture maximal du système de fichiers.
- Pour les systèmes de fichiers utilisant le débit provisionné, si la quantité de données stockée dans la classe de stockage EFS Standard permet à votre système de fichiers de générer un

débit supérieur à celui que vous avez provisionné, cette métrique reflète le débit supérieur plutôt que le montant provisionné.

- Pour les systèmes de fichiers en débit rapide, cette valeur est fonction de la taille du système de fichiers et. `BurstCreditBalance`

La statistique `Minimum` correspond au plus petit débit autorisé par minute au cours de la période. La statistique `Maximum` correspond au plus grand débit autorisé par minute au cours de la période. La statistique `Average` correspond au débit Moyen autorisé au cours de la période.

Note

Les opérations de lecture sont mesurées à un tiers du taux des autres opérations.

Unités : octets par seconde

Statistiques valides : `Minimum`, `Maximum`, `Average`

MeteredIOBytes

Nombre d'octets mesurés pour chaque opération du système de fichiers, y compris les opérations de lecture, d'écriture de données et de métadonnées, les opérations de lecture étant réduites en fonction de la limite de débit.

Vous pouvez créer une [expression mathématique CloudWatch métrique](#) qui se compare `MeteredIOBytes` à `PermittedThroughput`. Si ces valeurs sont égales, vous consommez la totalité du débit alloué à votre système de fichiers. Dans ce cas, vous pouvez envisager de Modifier le mode de débit du système de fichiers pour obtenir un débit supérieur.

La statistique `Sum` correspond au nombre total d'octets mesurés associés à toutes les opérations du système de fichiers. La statistique `Minimum` correspond à la plus petite taille d'opération au cours de la période. La statistique `Maximum` correspond à la plus grande taille d'opération au cours de la période. La statistique `Average` correspond à la taille Moyenne d'une opération au cours de la période. La statistique `SampleCount` fournit le nombre de toutes les opérations.

Unités :

- Octets pour les statistiques `Minimum`, `Maximum`, `Average` et `Sum`.
- Nombre de `SampleCount`.

Statistiques valides : `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

Total IOBytes

Le nombre réel d'octets pour chaque opération de système de fichiers traitée par Amazon EFS, sans aucune réduction de lecture. Ce nombre peut différer du montant réel demandé dans vos demandes car il inclut les minimums. Ce nombre peut également être supérieur aux chiffres indiqués dans `PermittedThroughput`.

Les opérations de données sont mesurées à 32 KiB et les autres opérations sont mesurées à 4 KiB. Après le minimum, toutes les opérations sont mesurées par KiB.

La statistique `Sum` correspond au nombre total d'octets associés à toutes les opérations du système de fichiers. La statistique `Minimum` correspond à la plus petite taille d'opération au cours de la période. La statistique `Maximum` correspond à la plus grande taille d'opération au cours de la période. La statistique `Average` correspond à la taille Moyenne d'une opération au cours de la période. La statistique `SampleCount` fournit le nombre de toutes les opérations.

Note

Pour calculer la Moyenne des opérations par seconde au cours d'une période, divisez la statistique `SampleCount` par le nombre de secondes constituant la période. Pour calculer le débit Moyen (octets par seconde) pour une période, divisez la statistique `Sum` par le nombre de secondes constituant la période.

Unités :

- Octets pour les statistiques `Minimum`, `Maximum`, `Average` et `Sum`.
- Nombre de `SampleCount`.

Statistiques valides : `Minimum`, `Maximum`, `Average`, `Sum`, `SampleCount`

DataReadIOBytes

Nombre réel d'octets pour chaque opération de lecture du système de fichiers.

La statistique `Sum` correspond au nombre total d'octets associés aux opérations de lecture. La statistique `Minimum` correspond à la plus petite taille d'opération de lecture au cours de la période. La statistique `Maximum` correspond à la plus grande taille d'opération de lecture au cours de la période. La statistique `Average` correspond à la taille Moyenne des opérations de lecture au cours de la période. La statistique `SampleCount` fournit un nombre d'opérations de lecture.

Unités :

- Octets pour Minimum, Maximum, Average et Sum.
- Nombre de SampleCount.

Statistiques valides : Minimum, Maximum, Average, Sum, SampleCount

DataWriteIOBytes

Nombre réel d'octets pour chaque opération d'écriture du système de fichiers.

La statistique Sum correspond au nombre total d'octets associés aux opérations d'écriture. La statistique Minimum correspond à la plus petite taille d'opération d'écriture au cours de la période. La statistique Maximum correspond à la plus grande taille d'opération d'écriture au cours de la période. La statistique Average correspond à la taille Moyenne des opérations d'écriture au cours de la période. La statistique SampleCount fournit un nombre d'opérations d'écriture.

Unités :

- Les octets représentent les unités des statistiques Minimum, Maximum, Average et Sum.
- Nombre de SampleCount.

Statistiques valides : Minimum, Maximum, Average, Sum, SampleCount

MetadataIOBytes

Nombre réel d'octets pour chaque opération de métadonnées.

La statistique Sum correspond au nombre total d'octets associés aux opérations de métadonnées. La statistique Minimum correspond à la plus petite taille d'opération de métadonnées au cours de la période. La statistique Maximum correspond à la plus grande taille d'opération de métadonnées au cours de la période. La statistique Average correspond à la taille Moyenne des opérations de métadonnées au cours de la période. La statistique SampleCount fournit un nombre d'opérations de métadonnées.

Unités :

- Les octets représentent les unités des statistiques Minimum, Maximum, Average et Sum.
- Nombre de SampleCount.

Statistiques valides : Minimum, Maximum, Average, Sum, SampleCount

MetadataReadIOBytes

Nombre réel d'octets pour chaque opération de lecture de métadonnées.

La **Sum** statistique représente le nombre total d'octets associés aux opérations de lecture des métadonnées. La **Minimum** statistique représente la taille de la plus petite opération de lecture de métadonnées au cours de la période. La **Maximum** statistique représente la taille de la plus grande opération de lecture de métadonnées au cours de la période. La **Average** statistique représente la taille moyenne des opérations de lecture de métadonnées au cours de la période. La **SampleCount** statistique fournit le nombre d'opérations de lecture de métadonnées.

Unités :

- Les octets représentent les unités des statistiques **Minimum**, **Maximum**, **Average** et **Sum**.
- Nombre de **SampleCount**.

Statistiques valides : **Minimum**, **Maximum**, **Average**, **Sum**, **SampleCount**

MetadataWriteIOBytes

Nombre réel d'octets pour chaque opération d'écriture de métadonnées.

La **Sum** statistique représente le nombre total d'octets associés aux opérations d'écriture de métadonnées. La **Minimum** statistique représente la taille de la plus petite opération d'écriture de métadonnées au cours de la période. La **Maximum** statistique représente la taille de la plus grande opération d'écriture de métadonnées au cours de la période. La **Average** statistique représente la taille moyenne des opérations d'écriture de métadonnées au cours de la période. La **SampleCount** statistique fournit le nombre d'opérations d'écriture de métadonnées.

Unités :

- Les octets représentent les unités des statistiques **Minimum**, **Maximum**, **Average** et **Sum**.
- Nombre de **SampleCount**.

Statistiques valides : **Minimum**, **Maximum**, **Average**, **Sum**, **SampleCount**

ClientConnections

Le nombre de connexions client à un système de fichiers. Lorsque vous utilisez un client standard, il existe une connexion par EC2 instance Amazon montée.

Note

Pour calculer la Moyenne des **ClientConnections** sur des périodes supérieures à 1 minute, divisez la statistique **Sum** par le nombre de minutes constituant la période.

Unités : Nombre de connexions client

Statistiques valides : Sum

StorageBytes

Taille du système de fichiers en octets, y compris la quantité de données stockées dans les classes de stockage EFS. Cette métrique est émise CloudWatch toutes les 15 minutes.

La StorageBytes métrique a les dimensions suivantes :

- **Total** est la taille mesurée (en octets) des données stockées dans le système de fichiers, dans toutes les classes de stockage. Pour les classes de stockage EFS Infrequent Access (IA) et EFS Archive, les fichiers inférieurs à 128 Ko sont arrondis à 128 Ko.
- **Standard** est la taille mesurée (en octets) des données stockées dans la classe de stockage EFS Standard.
- **IA** est la taille réelle (en octets) des données stockées dans la classe de stockage EFS Infrequent Access.
- **IASizeOverhead** est la différence (en octets) entre la taille réelle des données dans la classe de stockage EFS Infrequent Access (indiquée dans la IA dimension) et la taille mesurée de la classe de stockage, après avoir arrondi les petits fichiers à 128 Ko.
- **Archive** est la taille réelle (en octets) des données stockées dans la classe de stockage EFS Archive.
- **ArchiveSizeOverhead** est la différence (en octets) entre la taille réelle des données de la classe de stockage EFS Archive (indiquée dans la Archive dimension) et la taille mesurée de la classe de stockage, après avoir arrondi les petits fichiers à 128 Ko.

Unités : octets

Statistiques valides : Minimum, Maximum, Average

Note

StorageBytes est affiché sur la page des métriques du système de fichiers de la console Amazon EFS en utilisant 1024 unités de base (kibibytes, mebibytes, gibibytes et tebibytes).

Accès aux CloudWatch métriques pour Amazon EFS

Vous pouvez consulter les métriques Amazon EFS CloudWatch de différentes manières :

- Dans la console Amazon EFS.
- Dans la CloudWatch console
- Utilisation de la CloudWatch CLI
- Utilisation de l' CloudWatch API

Pour consulter CloudWatch les métriques et les alarmes (console Amazon EFS)

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/efs/>.
2. Choisissez File Systems (Systèmes de fichiers).
3. Choisissez le système de fichiers dont vous souhaitez consulter CloudWatch les métriques.
4. Choisissez Surveillance pour afficher la page des Métriques du système de fichiers.

La page Mesures du système de fichiers affiche un ensemble de CloudWatch mesures par défaut pour le système de fichiers. Toutes les CloudWatch alarmes que vous avez configurées s'affichent également avec ces métriques. Pour les systèmes de fichiers qui utilisent le mode de performance maximale des E/S, l'ensemble de mesures par défaut inclut le solde de Crédit en rafales au lieu de la limite de pourcentage d'E/S. Vous pouvez remplacer les paramètres par défaut à l'aide de la boîte de dialogue Paramètres des mesures, accessible en ouvrant les paramètres.

Note

La métrique d'utilisation du débit (%) n'est pas une CloudWatch métrique ; elle est dérivée à l'aide de mathématiques CloudWatch métriques.

5. Vous pouvez ajuster le mode d'affichage des métriques et des alarmes à l'aide des commandes de la page des Métriques du système de fichiers, comme suit.
 - Basculez entre le mode d'affichage en mode Série chronologique ou Valeur unique.
 - Afficher ou masquer les CloudWatch alarmes configurées pour le système de fichiers.
 - Choisissez Afficher plus dans CloudWatch pour afficher les statistiques dans CloudWatch.

- Choisissez Ajouter au tableau de bord pour ouvrir votre CloudWatch tableau de bord et ajouter les statistiques affichées.
- Ajustez la fenêtre temporelle métrique affichée de 1 heure à 1 semaine.

Pour consulter CloudWatch les métriques et les alarmes (CloudWatch console)

1. Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de noms EFS.
4. (Facultatif) Pour afficher une métrique, entrez son nom dans le champ de recherche.
5. (Facultatif) Pour filtrer par dimension, sélectionnez FileSystemId.

Pour accéder aux métriques depuis le AWS CLI

- Utilisez la commande [list-metrics](#) avec l'espace de noms `--namespace "AWS/EFS"`. Pour plus d'informations, consultez la référence de la commande [AWS CLI](#).

Pour accéder aux métriques depuis l' CloudWatch API

- Appelez [GetMetricStatistics](#). Pour plus d'informations, consultez le [Amazon CloudWatch API Reference](#).

Utilisation de CloudWatch métriques pour Amazon EFS

Les métriques présentées par Amazon EFS fournissent des informations qui permettent divers types d'analyses. La liste suivante présente certaines utilisations courantes des métriques. Voici quelques suggestions pour vous aider à démarrer, qui ne forment pas une liste exhaustive.

Comment... ?	Métriques pertinentes
Comment puis-je déterminer Mon débit ?	Vous pouvez surveiller la statistique Sum quotidienne de la métrique <code>TotalIOBytes</code> pour consultez votre débit.

Comment... ?	Métriques pertinentes
Comment puis-je déterminer le volume total de données transférées ?	Vous pouvez suivre les Sum statistiques quotidiennes de MeteredIO Bytes pour voir le total de vos données transférées.
Comment puis-je suivre le nombre d' EC2 instances Amazon connectées à un système de fichiers ?	Vous pouvez surveiller la statistique Sum de la métrique ClientConnections . Pour calculer la Moyenne des ClientConnections sur des périodes supérieures à 1 minute, divisez la somme par le nombre de minutes constituant la période.
Comment puis-je consultez Mon solde de crédits de transmission par rafales ?	Vous pouvez consultez votre solde en surveillant la métrique BurstCreditBalance de votre système de fichiers. Pour plus d'informations sur la transmission par rafales et les crédits associés, consultez Débit exceptionnel .

Surveillance des performances de débit

Les CloudWatch mesures de surveillance du débit (TotalIOBytes, ReadIOBytesWriteIOBytes, etMetadataIOBytes) représentent le débit réel que vous générez sur votre système de fichiers. La métrique MeteredIOBytes représente le calcul du débit mesuré global que vous conduisez. Vous pouvez utiliser le graphique d'utilisation du débit (%) de la section Surveillance de la console Amazon EFS pour surveiller votre utilisation du débit. Si vous utilisez CloudWatch des tableaux de bord personnalisés ou un autre outil de surveillance, vous pouvez créer une [expression mathématique CloudWatch métrique](#) qui se compare MeteredIOBytes àPermittedThroughput.

PermittedThroughput mesure le débit autorisé pour le système de fichiers. Cette valeur est basée sur l'une des méthodes suivantes :

- Pour les systèmes de fichiers dotés d'un débit élastique, cette valeur reflète le débit d'écriture maximal du système de fichiers.
- Pour les systèmes de fichiers utilisant le débit provisionné, si la quantité de données stockée dans la classe de stockage EFS Standard permet à votre système de fichiers de générer un débit

supérieur à celui que vous avez provisionné, cette métrique reflète le débit supérieur plutôt que le montant provisionné.

- Pour les systèmes de fichiers utilisant le débit en rafale, cette valeur est fonction de la taille du système de fichiers et. `BurstCreditBalance` Surveillez `BurstCreditBalance` pour vous assurer que votre système de fichiers fonctionne à sa fréquence de rafale plutôt qu'à sa fréquence de base. Si le solde est constamment égal ou proche de zéro, envisagez de passer au débit élastique ou au débit provisionné pour obtenir un débit supplémentaire.

Lorsque les valeurs pour `MeteredIOBytes` et `PermittedThroughput` sont égales, votre système de fichiers consomme tout le débit disponible. Pour les systèmes de fichiers utilisant le débit provisionné, vous pouvez fournir un débit supplémentaire.

Utiliser les mathématiques métriques avec CloudWatch les métriques

À l'aide des mathématiques métriques, vous pouvez interroger plusieurs CloudWatch métriques Amazon et utiliser des expressions mathématiques pour créer de nouvelles séries chronologiques basées sur ces métriques. Vous pouvez visualiser les séries chronologiques obtenues dans la CloudWatch console et les ajouter aux tableaux de bord. Par exemple, vous pouvez utiliser les métriques Amazon EFS, afin de prendre le nombre d'opérations `DataRead` divisé par 60. Vous obtenez le nombre Moyen de lectures par seconde sur votre système de fichiers pour une durée d'une minute. Pour plus d'informations sur les mathématiques métriques, consultez la section [Utilisation d'expressions mathématiques avec CloudWatch des métriques](#) dans le guide de CloudWatch l'utilisateur Amazon.

Vous trouverez ci-dessous des expressions mathématiques appliquées aux métriques utiles pour Amazon EFS.

Rubriques

- [Mathématiques métriques : débit entrant MiBps](#)
- [Mathématiques appliquées aux métriques : débit en pourcentage](#)
- [Mathématiques appliquées aux métriques : pourcentage d'utilisation du débit autorisé](#)
- [Mathématiques appliquées aux métriques : Débit IOPS](#)
- [Mathématiques appliquées aux métriques : pourcentage d'IOPS](#)
- [Mathématiques appliquées aux métriques : taille d'E/S Moyenne en Kio](#)
- [Utilisation des mathématiques appliquées aux métrique via un Modèle AWS CloudFormation pour Amazon EFS](#)

Mathématiques métriques : débit entrant MiBps

Pour calculer le débit moyen (in MiBps) pour une période donnée, choisissez d'abord une statistique de somme (`DataReadIOBytes`, `DataWriteIOBytesMetadataIOBytes`, ou `TotalIOBytes`). Ensuite, convertissez la valeur en MiB et divisez-la par le nombre de secondes de la période.

Supposons par exemple que votre logique est la suivante : (somme de `TotalIOBytes` ÷ 1 048 576 (à convertir en MiB)) ÷ secondes dans la période

Vos informations CloudWatch métriques sont alors les suivantes.

ID	Métriques utilisables	Statistique	Période
m1	<code>DataReadIOBytes</code> <code>DataWriteIOBytes</code> <code>MetadataIOBytes</code> <code>TotalIOBytes</code>	sum	1 minute

Votre ID de mathématiques appliquées aux métriques et votre expression sont les suivantes :

ID	Expression
e1	$(m1/1048576)/PERIOD(m1)$

Mathématiques appliquées aux métriques : débit en pourcentage

Cette expression mathématique métrique calcule le pourcentage du débit global utilisé pour les différents types d'E/S, par exemple le pourcentage du débit total généré par les demandes de lecture. Pour calculer le pourcentage du débit global utilisé par l'un des types d'E/S (`DataReadIOBytes`, `DataWriteIOBytes`, or `MetadataIOBytes`) pour une période donnée, il faut d'abord multiplier la somme statistique correspondante par 100. Ensuite, divisez le résultat par la statistique de somme de `TotalIOBytes` pour la même période.

Supposons par exemple que votre logique est la suivante : (somme de `DataReadIOBytes` x 100 (à convertir en pourcentage)) ÷ somme de `TotalIOBytes`

Vos informations CloudWatch métriques sont alors les suivantes.

ID	Métriques utilisables	Statistique	Période
m1	• <code>TotalIOBytes</code>	sum	1 minute
m2	• <code>DataReadIOBytes</code>	sum	1 minute

Votre ID de mathématiques appliquées aux métriques et votre expression sont les suivantes :

ID	Expression
e1	$(m2 * 100) / m1$

Mathématiques appliquées aux métriques : pourcentage d'utilisation du débit autorisé

Pour calculer le pourcentage d'utilisation du débit autorisé (`MeteredIOBytes`) pour une période donnée, multipliez d'abord le débit entrant MiBps par 100. Divisez ensuite le résultat par la statistique moyenne `PermittedThroughput` convertie en MiB pour la même période.

Supposons que votre exemple de logique soit le suivant : (expression mathématique métrique pour le débit en MiBps x 100 (pour convertir en pourcentage)) ÷ (somme de `PermittedThroughput` ÷ 1 048 576 (pour convertir les octets en MiB))

Vos informations CloudWatch métriques sont alors les suivantes.

ID	Métriques utilisables	Statistique	Période
m1	<code>MeteredIOBytes</code>	sum	1 minute
m2	<code>PermittedThroughput</code>	average	1 minute

Votre ID de mathématiques appliquées aux métriques et votre expression sont les suivantes :

ID	Expression
e1	$(m1/1048576)/PERIOD(m1)$
e2	$m2/1048576$
e3	$((e1)*100)/(e2)$

Mathématiques appliquées aux métriques : Débit IOPS

Pour calculer le nombre Moyen d'opérations par seconde (IOPS) pour une période, divisez la statistique d'échantillonnage (DataReadIOBytes, DataWriteIOBytes, MetadataIOBytes ou TotalIOBytes) par le nombre de secondes dans la période.

Supposons par exemple que votre logique est la suivante : échantillonnage de DataWriteIOBytes ÷ secondes dans la période

Vos informations CloudWatch métriques sont alors les suivantes.

ID	Métriques utilisables	Statistique	Période
m1	- DataReadIOBytes - DataWriteIOBytes - MetadataIOBytes - TotalIOBytes	échantillonnage	1 minute

Votre ID de mathématiques appliquées aux métriques et votre expression sont les suivantes :

ID	Expression
e1	$m1/PERIOD(m1)$

Mathématiques appliquées aux métriques : pourcentage d'IOPS

Pour calculer le pourcentage d'IOPS par seconde des différents types d'E/S (DataReadIOBytes, DataWriteIOBytes ou MetadataIOBytes) pour une période, vous devez d'abord multiplier la statistique d'échantillonnage respective par 100. Ensuite, divisez le résultat par la statistique d'échantillonnage de TotalIOBytes pour la même période.

Supposons par exemple que votre logique est la suivante : (échantillonnage de MetadataIOBytes x 100 (à convertir en pourcentage)) ÷ échantillonnage de TotalIOBytes

Vos informations CloudWatch métriques sont alors les suivantes.

ID	Métriques utilisables	Statistique	Période
m1	• TotalIOBytes	échantillonnage	1 minute
m2	• DataReadIOBytes • DataWriteIOBytes • MetadataIOBytes	échantillonnage	1 minute

Votre ID de mathématiques appliquées aux métriques et votre expression sont les suivantes :

ID	Expression
e1	(m2*100)/m1

Mathématiques appliquées aux métriques : taille d'E/S Moyenne en Kio

Pour calculer la taille d'E/S Moyenne (en Kio) pour une période, divisez la statistique de somme respective de la métrique DataReadIOBytes, DataWriteIOBytes ou MetadataIOBytes par la même statistique d'échantillonnages de cette métrique.

Supposons par exemple que votre logique est la suivante : (somme de DataReadIOBytes ÷ 1 024 (à convertir en kio)) ÷ échantillonnage de DataReadIOBytes

Vos informations CloudWatch métriques sont alors les suivantes.

ID	Métriques utilisables	Statistique	Période
m1	- DataReadIOBytes - DataWriteIOBytes - MetadataIOBytes	sum	1 minute
m2	- DataReadIOBytes - DataWriteIOBytes - MetadataIOBytes	échantillonnage	1 minute

Votre ID de mathématiques appliquées aux métriques et votre expression sont les suivantes :

ID	Expression
e1	$(m1/1024)/m2$

Utilisation des mathématiques appliquées aux métrique via un Modèle AWS CloudFormation pour Amazon EFS

Vous pouvez également créer des expressions mathématiques métriques à l'aide AWS CloudFormation de modèles. L'un de ces modèles est disponible à télécharger et à personnaliser pour une utilisation à partir des [didacticiels Amazon EFS](#) disponibles sur le site GitHub. Pour plus d'informations sur l'utilisation AWS CloudFormation des modèles, consultez la section [Utilisation des AWS CloudFormation modèles](#) dans le Guide de AWS CloudFormation l'utilisateur.

Surveillance des réussites et des échecs des tentatives de montage

Vous pouvez utiliser Amazon CloudWatch Logs pour surveiller et signaler le succès ou l'échec des tentatives de montage de vos systèmes de fichiers EFS à distance sans avoir à vous connecter aux clients. Suivez la procédure suivante pour configurer votre EC2 instance afin qu'elle utilise CloudWatch les journaux afin de contrôler le succès ou l'échec des tentatives de montage de son système de fichiers.

Pour activer la notification de réussite ou d'échec des tentatives de montage dans CloudWatch les journaux

1. Effectuez l'installation `amazon-efs-utils` sur l' EC2 instance qui monte le système de fichiers. Pour plus d'informations, consultez [Installation ou mise à jour automatique du client Amazon EFS à l'aide de AWS Systems Manager](#) ou [Installation manuelle du client Amazon EFS](#).
2. Effectuez l'installation `botocore` sur l' EC2 instance qui va monter le système de fichiers. Pour de plus amples informations, veuillez consulter [Installation et mise à niveau botocore](#).
3. Activez la fonctionnalité CloudWatch Logs dans `amazon-efs-utils`. Lors de l'installation et AWS Systems Manager de la configuration `amazon-efs-utils`, la CloudWatch journalisation est automatiquement effectuée pour vous. Lorsque vous installez le package `amazon-efs-utils` manuellement, vous devez mettre à jour le fichier de configuration `/etc/amazon/efs/efs-utils.conf` manuellement en décommentant la ligne `# enabled = true` de la section `cloudwatch-log`. Utilisez l'une des commandes suivantes pour activer CloudWatch les journaux manuellement.

Pour les instances Linux :

```
sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/}' /etc/amazon/efs/efs-utils.conf
```

Pour les instances de macOS :

```
EFS_UTILS_VERSION= efs-utils-version  
sudo sed -i -e '/\[cloudwatch-log\]/{N;s/# enabled = true/enabled = true/;}' /usr/local/Cellar/amazon-efs-utils/${EFS_UTILS_VERSION}/libexec/etc/amazon/efs/efs-utils.conf
```

Pour les instances 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
```

- Vous pouvez éventuellement configurer les noms CloudWatch des groupes de journaux et définir les jours de conservation des journaux dans le `efs-utils.conf` fichier. Si vous souhaitez créer des groupes de journaux distincts CloudWatch pour chaque système de fichiers monté, ajoutez-les `{fs_id}` à la fin du `log_group_name` champ du `efs-utils.conf` fichier, comme suit :

```
[cloudwatch-log]
log_group_name = /aws/efs/Utils/{fs_id}
```

- Associez la politique `AmazonElasticFileSystemsUtils` AWS gérée au rôle IAM que vous avez attaché à l'EC2 instance ou aux AWS informations d'identification configurées sur votre instance. Vous pouvez utiliser Systems Manager à cette fin. Pour obtenir plus d'informations, consultez [Étape 1 : Configurez un profil d'instance \(IAM\) avec les autorisations requises.](#)

Voici des exemples d'entrées du journal d'état des tentatives de Montage :

```
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"
```

Pour afficher l'état du montage dans CloudWatch les journaux

- Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
- Sélectionnez Groupes de journalisation dans la barre de navigation de gauche.
- Choisissez le groupe `/aws/efs/Utilslog`. Vous verrez un flux de journal pour chaque combinaison d'EC2 instance Amazon et de système de fichiers EFS.
- Choisissez un flux de journal pour afficher des événements de journal spécifiques, notamment l'état de réussite ou d'échec de la tentative de Montage.

Création d' CloudWatch alarmes pour surveiller Amazon EFS

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une seule métrique pendant la période que vous spécifiez. Elle

réalise une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon SNS ou à une politique Auto Scaling.

Les alarmes déclenchent des actions uniquement pour les changements d'état prolongés. CloudWatch les alarmes n'appellent pas d'actions uniquement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes.

L'une des utilisations importantes des CloudWatch alarmes pour Amazon EFS consiste à appliquer le chiffrement au repos de votre système de fichiers. Vous pouvez activer le chiffrement au repos pour un système de fichiers Amazon EFS lors de sa création. Pour appliquer encryption-at-rest les politiques relatives aux données pour les systèmes de fichiers Amazon EFS, vous pouvez utiliser Amazon CloudWatch AWS CloudTrail pour détecter la création d'un système de fichiers et vérifier que le chiffrement au repos est activé.

 Note

Actuellement, vous ne pouvez pas appliquer le chiffrement en transit.

Les procédures suivantes expliquent comment créer des alarmes pour Amazon EFS.

Utilisation de la console

Pour définir des alarmes à l'aide de la CloudWatch console

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Sélectionnez Create Alarm (Créer une alerte). L'assistant Create Alarm démarre.
3. Choisissez Métriques EFS et faites défiler les métriques afin de localiser la métrique sur laquelle vous voulez placer une alarme. Pour afficher seulement les métriques Amazon EFS dans cette boîte de dialogue, recherchez l'ID de votre système de fichiers. Sélectionnez la métrique sur laquelle créer une alarme, puis sélectionnez Suivant.
4. Indiquez les valeurs Nom, Description, Lorsque pour la métrique.
5. Si vous souhaitez vous CloudWatch envoyer un e-mail lorsque l'état d'alarme est atteint, dans le champ Chaque fois que cette alarme est :, choisissez State is ALARM. Dans le champ Send notification to:, choisissez une rubrique SNS existante. Si vous sélectionnez Create topic, vous

pouvez définir le nom d'une nouvelle liste d'abonnement par e-mail et les adresses e-mail pour cette liste. La liste est enregistrée et s'affiche dans le champ des alarmes futures.

 Note

Si vous utilisez Créer la rubrique pour créer une nouvelle rubrique Amazon SNS, les adresses e-mail doivent être vérifiées avant de pouvoir recevoir des notifications. Les e-mails sont envoyés uniquement lorsque l'alarme passe à un état défini. Si ce changement d'état de l'alarme se produit avant la vérification des adresses e-mail, ces dernières ne reçoivent pas de notification.

6. A ce stade, la zone Alarm Preview (Aperçu de l'alarme) vous offre la possibilité d'obtenir un aperçu de l'alarme que vous êtes sur le point de créer. Sélectionnez Create Alarm (Créer une alerte).

En utilisant le AWS CLI

Pour régler une alarme à l'aide du AWS CLI

- Appelez [put-metric-alarm](#). Pour plus d'informations, consultez la référence de la commande [AWS CLI](#).

Utilisation de l' CloudWatch API

Pour configurer une alarme à l'aide de l' CloudWatch API

- Appelez [PutMetricAlarm](#). Pour plus d'informations, consultez le [Amazon CloudWatch API Reference](#).

Journalisation des appels d'API Amazon EFS avec AWS CloudTrail

Amazon EFS est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Amazon EFS. CloudTrail capture tous les appels d'API pour Amazon EFS sous forme d'événements, y compris les appels depuis la console Amazon EFS et les appels de code vers les opérations d'API Amazon EFS.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon EFS. Si vous ne configurez

pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Amazon EFS, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour plus d'informations, consultez la section [Qu'est-ce que c'est AWS CloudTrail ?](#) dans le guide de AWS CloudTrail l'utilisateur.

Informations Amazon EFS dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité a lieu dans Amazon EFS, elle est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Utilisation de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris des événements pour Amazon EFS, créez un suivi. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à tous les Région AWS s. Le journal enregistre les événements provenant de tous Régions AWS les AWS éléments de la partition et envoie les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les rubriques suivantes dans le AWS CloudTrail Guide de l'utilisateur :

- [Création d'un parcours pour votre AWS compte](#)
- [AWS intégrations de services avec journaux CloudTrail](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Tous les Amazon EFS [API Amazon EFS](#) sont enregistrés par CloudTrail. Par exemple, les appels aux CreateFileSystem CreateTags opérations CreateMountTarget et les opérations génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou de l'utilisateur AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'[élément CloudTrail UserIdentity](#) dans le guide de l'AWS CloudTrail utilisateur.

Présentation des entrées des fichiers journaux Amazon EFS

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre le `CreateTags` fonctionnement lors de la création d'une balise pour un système de fichiers à partir de la 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'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`DeleteTags` action à effectuer lorsqu'une balise d'un système de fichiers est supprimée de la 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": "11112223333"
}

```

Entrées de journal pour les rôles liés à un service EFS

Le rôle lié au service Amazon EFS effectue des appels d'API vers AWS des ressources. Vous verrez les entrées du CloudTrail journal relatives `username: AWSServiceRoleForAmazonElasticFileSystem` aux appels effectués par le rôle lié au service EFS. Pour plus d'informations sur les rôles liés à un service EFS, veuillez consulter [Utilisation des rôles liés à un service pour Amazon EFS](#).

L'exemple suivant montre une entrée de CloudTrail journal qui illustre une `CreateServiceLinkedRole` action lorsqu'Amazon EFS crée le rôle `AWSServiceRoleForAmazonElasticFileSystem` lié à un service.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "11112223333",
    "arn": "arn:aws:iam::11112223333:user/user1",
    "accountId": "11112223333",
    "accessKeyId": "A11112223333",
    "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":
"111122223333-10-111122223333Statement111122223333Action111122223333AssumeRole111122223333Effect%22%3A%20%22Allow%22%2C%20%22Principal%22%3A%20%7B%22Service%22%3A%20%5B%22elasticfilesystem.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'exemple suivant montre une entrée de CloudTrail journal illustrant une `CreateNetworkInterface` action effectuée par le rôle `AWSServiceRoleForAmazonElasticFileSystem` lié à un service, indiquée dans le `sessionContext`

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",

```

```

    "arn": "arn:aws:sts::0123456789ab:assumed-role/
AWSServiceRoleForAmazonElasticFileSystem/0123456789ab",
    "accountId": "0123456789ab",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::0123456789ab:role/aws-service-role/
elasticfilesystem.amazonaws.com/AWSServiceRoleForAmazonElasticFileSystem",
        "accountId": "0123456789ab",
        "userName": "AWSServiceRoleForAmazonElasticFileSystem"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-10-23T22:50:05Z"
      }
    },
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2019-10-23T22:50:05Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CreateNetworkInterface",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "elasticfilesystem.amazonaws.com",
  "userAgent": "elasticfilesystem.amazonaws.com",
  "requestParameters": {
    "subnetId": "subnet-71e2f83a",
    "description": "EFS mount target for fs-1234567 (fsmt-1234567)",
    "groupSet": {},
    "privateIpAddressesSet": {}
  },
  "responseElements": {
    "requestId": "0708e4ad-03f6-4802-b4ce-4ba987d94b8d",
    "networkInterface": {
      "networkInterfaceId": "eni-0123456789abcdef0",
      "subnetId": "subnet-12345678",
      "vpcId": "vpc-01234567",
      "availabilityZone": "us-east-1b",
      "description": "EFS mount target for fs-1234567 (fsmt-1234567)",
      "ownerId": "666051418590",
      "requesterId": "0123456789ab",
      "requesterManaged": true,
      "status": "pending",

```



```

    "macAddress": "00:bb:ee:ff:aa:cc",
    "privateIpAddress": "192.0.2.0",
    "privateDnsName": "ip-192-0-2-0.ec2.internal",
    "sourceDestCheck": true,
    "groupSet": {
      "items": [
        {
          "groupId": "sg-c16d65b6",
          "groupName": "default"
        }
      ]
    },
    "privateIpAddressesSet": {
      "item": [
        {
          "privateIpAddress": "192.0.2.0",
          "primary": true
        }
      ]
    },
    "tagSet": {}
  },
  "requestID": "11112222-3333-4444-5555-666666777777",
  "eventID": "aaaabbbb-1111-2222-3333-444444555555",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

Entrées de journal pour l'authentification EFS

Autorisation Amazon EFS pour les émissions `NewClientConnection` et `UpdateClientConnection` CloudTrail les événements des clients NFS. Un événement `NewClientConnection` est émis lorsqu'une connexion est autorisée immédiatement après une connexion initiale et immédiatement après une reconnexion. Un `UpdateClientConnection` est émis lorsqu'une connexion est réautorisée et que la liste des actions autorisées a changé. L'événement est également émis lorsque la nouvelle liste d'actions autorisées n'inclut pas `ClientMount`. Pour de plus amples informations sur l'autorisation EFS, veuillez consulter [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#).

L'exemple suivant montre une entrée de CloudTrail journal illustrant un `NewClientConnection` événement.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::0123456789ab:assumed-role/abcdef0123456789",
    "accountId": "0123456789ab",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE ",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::0123456789ab:role/us-east-2",
        "accountId": "0123456789ab",
        "userName": "username"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-12-23T17:50:16Z"
      },
      "ec2RoleDelivery": "1.0"
    }
  },
  "eventTime": "2019-12-23T18:02:12Z",
  "eventSource": "elasticfilesystem.amazonaws.com",
  "eventName": "NewClientConnection",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "elasticfilesystem",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "27859ac9-053c-4112-ae3-f3429719d460",
  "readOnly": true,
  "resources": [
    {
      "accountId": "0123456789ab",
      "type": "AWS::EFS::FileSystem",
      "ARN": "arn:aws:elasticfilesystem:us-east-2:0123456789ab:file-system/
fs-01234567"
    },
    {
      "accountId": "0123456789ab",

```

```
        "type": "AWS::EFS::AccessPoint",
        "ARN": "arn:aws:elasticfilesystem:us-east-2:0123456789ab:access-point/
fsap-0123456789abcdef0"
    },
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "0123456789ab",
    "serviceEventDetails": {
        "permissions": {
            "ClientRootAccess": true,
            "ClientMount": true,
            "ClientWrite": true
        },
        "sourceIpAddress": "10.7.3.72"
    }
}
```

Entrées du fichier journal Amazon EFS pour les systèmes de encrypted-at-rest fichiers

Amazon EFS vous offre la possibilité d'utiliser le chiffrement au repos, le chiffrement en transit ou les deux, pour vos systèmes de fichiers. Pour de plus amples informations, veuillez consulter [Chiffrement des données dans Amazon EFS](#).

Amazon EFS envoie [le contexte de chiffrement](#) lorsque vous effectuez des demandes d' AWS KMS API pour générer des clés de données et déchiffrer les données Amazon EFS. L'ID du système de fichiers est le contexte de chiffrement de tous les systèmes de fichiers qui sont chiffrés au repos. Dans le requestParameters champ d'une entrée de CloudTrail journal, le contexte de chiffrement est similaire au suivant.

```
"EncryptionContextEquals": {}
"aws:elasticfilesystem:filesystem:id" : "fs-4EXAMPLE"
```

Utilisation des rapports AWS de facturation et d'utilisation

Lorsque vous utilisez Amazon EFS, vous ne payez que pour les ressources que vous utilisez et il n'y a pas de frais minimaux ni de frais d'installation. Comme pour les autres AWS services, les prix sont indiqués sur une base mensuelle, votre utilisation est calculée au prorata de l'heure et vous êtes facturé pour votre utilisation moyenne sur un mois.

AWS fournit les rapports suivants pour Amazon EFS :

- **Rapports de facturation** : plusieurs rapports fournissant des vues détaillées de toutes les activités liées aux AWS services que vous utilisez, y compris Amazon EFS. AWS facture toujours les frais Amazon EFS au propriétaire du système de fichiers EFS. Pour en savoir plus sur les rapports de facturation, consultez [AWS Billing rapports pour Amazon EFS](#).
- **Rapports d'utilisation** : résumé de l'activité d'un service spécifique, agrégé par heure, jour ou mois. Vous voulez choisir le type d'utilisation et les opérations à inclure. Vous pouvez également choisir la manière dont les données sont regroupées. Pour de plus amples informations, veuillez consulter [AWS rapports d'utilisation pour Amazon EFS](#).

Les rubriques suivantes fournissent des informations sur la facturation et les rapports d'utilisation pour Amazon EFS.

Rubriques

- [Utilisation des balises du système de fichiers EFS pour la répartition des coûts](#)
- [AWS Billing rapports pour Amazon EFS](#)
- [AWS rapports d'utilisation pour Amazon EFS](#)
- [Comprendre les rapports de facturation et d'utilisation pour Amazon EFS](#)

Utilisation des balises du système de fichiers EFS pour la répartition des coûts

Pour suivre le coût de stockage ou d'autres critères pour des projets individuels ou des groupes de projets, étiquetez vos systèmes de fichiers EFS à l'aide de balises de répartition des coûts. Une balise de répartition des coûts est une paire clé-valeur que vous associez à un système de fichiers. Après avoir activé les balises de répartition des coûts, AWS utilise les balises pour organiser les coûts des ressources dans votre rapport de répartition des coûts.

Le rapport de répartition des coûts répertorie l' AWS utilisation de votre compte par catégorie de produit et par utilisateur du compte associé. Il contient les mêmes postes que le rapport de facturation détaillée (consultez [Comprendre les rapports de facturation et d'utilisation pour Amazon EFS](#)), ainsi que des colonnes supplémentaires pour vos clés de balises.

AWS fournit deux types de balises de répartition des coûts, les balises AWS générées et les balises définies par l'utilisateur. AWS définit, crée et applique la clé de `aws:createdBy` balise AWS générée pour vous après un `CreateFileSystem` événement Amazon EFS. Vous définissez, créez et appliquez des balises définies par l'utilisateur à vos systèmes de fichiers.

Vous devez activer ces deux types de balises séparément dans la console de gestion des coûts et de la facturation pour qu'elles apparaissent dans vos rapports de facturation. Pour plus d'informations sur les balises AWS générées, consultez la section [Organisation et suivi des coûts à l'aide des balises de répartition des AWS coûts](#) dans le Guide de l'AWS Billing utilisateur.

- Pour plus d'informations sur la création de balises définies par l'utilisateur pour les ressources EFS, consultez [Marquage des ressources EFS](#).
- Pour plus d'informations sur l'activation des balises définies par l'utilisateur dans la console Billing and Cost Management, consultez la section [Activation des balises de répartition des coûts définies par l'utilisateur](#) dans le guide de l'AWS Billing utilisateur.
- Pour plus d'informations sur l'activation des balises AWS générées dans la console Billing and Cost Management, consultez la section [Activation des balises de répartition des coûts AWS générées](#) dans le guide de l'AWS Billing utilisateur.

Balises de répartition des coûts définies par l'utilisateur

Une balise de répartition des coûts définie par l'utilisateur comprend les composants suivants :

- Clé de balise . Il s'agit du nom de la balise. Par exemple, dans la balise projet/Trinity, projet est la clé. La balise est sensible à la casse et doit contenir entre 1 et 128 caractères Unicode.
- Valeur de balise. Il s'agit d'une chaîne obligatoire. Par exemple, dans la balise projet/Trinity, Trinity est la valeur. La valeur de clé est sensible à la casse et doit contenir entre 0 et 256 caractères Unicode.

Pour plus d'informations sur les balises définies par l'utilisateur, voir [Utilisation des balises de répartition des coûts définies par l'utilisateur](#) dans le Guide de l'AWS Billing utilisateur.

AWS Billing rapports pour Amazon EFS

Votre facture mensuelle AWS sépare vos informations d'utilisation et les coûts par AWS service et par fonction. Plusieurs rapports AWS de facturation sont disponibles : le rapport mensuel, le rapport de répartition des coûts et les rapports de facturation détaillés. Pour plus d'informations, consultez [la section Comprendre votre facture](#) dans le Guide de AWS Billing l'utilisateur.

Pour des rapports plus détaillés sur votre utilisation du stockage Amazon EFS, utilisez Exportations de données AWS pour créer des exportations du AWS Cost and Usage Report (AWS CUR). Avec AWS CUR 2.0, vous publiez vos rapports AWS de facturation dans un compartiment Amazon Simple Storage Service (Amazon S3) dont vous êtes le propriétaire. Le rapport d'utilisation d'Amazon EFS répertorie les opérations par type d'utilisation et Région AWS. Pour plus d'informations, consultez le [rapport sur les coûts et l'utilisation \(CUR\) 2.0](#) dans le guide de Exportations de données AWS l'utilisateur.

Les systèmes de fichiers EFS sont facturés en fonction des catégories d'utilisation suivantes.

- Stockage (par gigaoctet [Go]) : quantité de données stockées dans vos systèmes de fichiers EFS par mois, avec des prix différents en fonction de la classe de stockage (EFS Standard, EFS Infrequent Access (IA) et EFS Archive).
- Débit (par Go ou mebioctets par seconde [MiBps]) : quantité de données transférée (opérations de lecture/écriture) ou quantité supérieure à la quantité allouée, en fonction du débit du système de fichiers, par mois.
- Accès aux données et transition (par MiBps) : quantité de données lues et transférées vers les classes de stockage EFS Infrequent Access (IA) et EFS Archive par mois.
- Stockage de sauvegarde (par Go) : quantité d'espace de stockage consommée par les sauvegardes par mois. L'augmentation de la durée de conservation des sauvegardes ou la prise de sauvegardes de volumes supplémentaires initiées par l'utilisateur augmentent la quantité de stockage de sauvegarde consommée par votre système de fichiers. Pour de plus amples informations, consultez [Sauvegarde des systèmes de fichiers EFS](#).
- Réplication (par Go) : taux d'activité de stockage et de lecture, d'écriture et de hiérarchisation en vigueur pour vos systèmes de fichiers EFS source et de destination, ainsi que tous les frais applicables pour les activités de transfert de données entre eux, par mois.

Pour obtenir des informations détaillées sur les frais Amazon EFS, consultez la section [Tarification Amazon EFS](#).

Pour en savoir plus sur la compréhension des codes et des abréviations utilisés dans les rapports de facturation et d'utilisation d'Amazon EFS, consultez [Comprendre les rapports de facturation et d'utilisation pour Amazon EFS](#).

AWS rapports d'utilisation pour Amazon EFS

Lorsque vous téléchargez un rapport d'utilisation, vous pouvez demander à cumuler les données d'utilisation sur une base horaire, quotidienne ou mensuelle. Le rapport d'utilisation d'Amazon EFS répertorie les opérations par type d'utilisation et Région AWS. Pour obtenir des rapports plus détaillés sur votre utilisation du stockage Amazon EFS, téléchargez des rapports AWS d'utilisation générés dynamiquement. Vous voulez choisir le type d'utilisation, les opérations et la période à inclure. Vous pouvez également choisir la manière dont les données sont regroupées. Pour plus d'informations sur le téléchargement de rapports d'utilisation, consultez la section [Téléchargement d'un rapport AWS d'utilisation](#) dans le Guide de l'utilisateur AWS des exportations de données.

Le rapport d'utilisation d'Amazon EFS inclut les informations suivantes :

- Service — Amazon EFS
- UsageType— L'une des valeurs suivantes :
 - Code qui identifie le type de stockage
 - Code qui identifie le type de demande
 - Code qui identifie le type de transfert de données
 - Un code qui identifie le mode de débit
 - Un code qui identifie l'utilisation de la sauvegarde

Pour une explication détaillée des types d'utilisation d'Amazon EFS, consultez [Comprendre les rapports de facturation et d'utilisation pour Amazon EFS](#).

- Ressource : nom de la ressource associée à l'utilisation répertoriée.
- StartTime— Heure de début de la journée à laquelle s'applique l'utilisation, en temps universel coordonné (UTC).
- EndTime— Heure de fin de la journée à laquelle s'applique l'utilisation, en temps universel coordonné (UTC).
- UsageValue— L'une des valeurs de volume suivantes. L'unité de mesure standard des données est le gigaoctet (Go). Toutefois, selon le service et le rapport, des téraoctets (To) peuvent apparaître à la place.
 - Nombre de requêtes au cours de la période spécifiée

- Volume de données transférées
- Volume de données stockées dans une heure donnée

Pour en savoir plus sur la compréhension des codes et des abréviations utilisés dans les rapports de facturation et d'utilisation d'Amazon EFS, consultez [Comprendre les rapports de facturation et d'utilisation pour Amazon EFS](#).

Comprendre les rapports de facturation et d'utilisation pour Amazon EFS

Les rapports de facturation et d'utilisation d'Amazon EFS utilisent des codes et des abréviations. Pour les types d'utilisation figurant dans le tableau ci-dessous, remplacez-les *region* par les abréviations de cette liste :

- APE1: Asie-Pacifique (Hong Kong)
- APN1: Asie-Pacifique (Tokyo)
- APN2: Asie-Pacifique (Séoul)
- APN3: Asie-Pacifique (Osaka)
- APS1: Asie-Pacifique (Singapour)
- APS2: Asie-Pacifique (Sydney)
- APS3: Asie-Pacifique (Mumbai)
- APS4: Asie-Pacifique (Jakarta)
- APS5: Asie-Pacifique (Hyderabad)
- APS6: Asie-Pacifique (Melbourne)
- CAN1: Canada (Centre)
- CAN2: Canada Ouest (Calgary)
- CNN1: Chine (Pékin)
- CNW1: Chine (Ningxia)
- AFS1: Afrique (Le Cap)
- EUC2: Europe (Zurich)
- EUN1: Europe (Stockholm)
- EUS2: Europe (Espagne)

- EUC1: Europe (Francfort)
- EU : Europe (Irlande)
- EUS1: Europe (Milan)
- EUW2: Europe (Londres)
- EUW3: Europe (Paris)
- ILC1: Israël (Tel Aviv)
- MEC1: Moyen-Orient (Émirats arabes unis)
- MES1: Moyen-Orient (Bahreïn)
- SAE1: Amérique du Sud (São Paulo)
- UGW1: AWS GovCloud (US-Ouest)
- UGE1: AWS GovCloud (USA Est)
- USE1 (ou sans préfixe) : USA Est (Virginie du Nord)
- USE2: Est des États-Unis (Ohio)
- USW1: USA Ouest (Californie du Nord)
- USW2: Ouest des États-Unis (Oregon)

Pour plus d'informations sur la tarification par Région AWS, consultez la section [Tarification d'Amazon EFS](#).

La première colonne du tableau suivant répertorie les types d'utilisation qui apparaissent dans les rapports d'utilisation et de facturation. L'unité de mesure standard des données est le gigaoctet (Go). Toutefois, pour le débit provisionné, ce sont les mebiotets par seconde (MiBps) qui sont utilisés à la place.

Types d'utilisation pour Amazon EFS

Type d'utilisation	CloudWatch métrique	Unités	Granularité	Description
<i>region-</i> ArchiveD ataAccess- Bytes	N/A	Go	N/A	Quantité de données transférées ou consultées dans le stockage des archives EFS.

Type d'utilisation	CloudWatch métrique	Unités	Granularité	Description
<i>region</i> -ArchiveEarlyDelete-ByteHrs	N/A	Go Mo	N/A	Utilisation du stockage au prorata pour les fichiers supprimés du stockage des archives EFS avant la fin de l'engagement minimum de 90 jours.
<i>region</i> -ArchiveEarlyDelete-SmallFiles	N/A	Go Mo	N/A	Utilisation du stockage au prorata pour les petits fichiers (inférieurs à 128 Ko) qui ont été supprimés du stockage des archives EFS avant la fin de l'engagement minimum de 90 jours.
<i>region</i> -ArchiveTimedStorage-ByteHrs	StorageElasticArchives	Go Mo	Par heure	Nombre de Go par mois pendant lesquels les données ont été stockées dans le stockage des archives EFS.
<i>region</i> -ArchiveTimedStorage-SmallFiles	StorageElasticArchivesSizeOnRead	Go Mo	Par heure	Nombre de Go par mois pendant lesquels de petits objets (inférieurs à 128 Ko) ont été stockés dans le stockage des archives EFS.
<i>region</i> -ETDataAccess-Bytes	TotalIOBytes	Go	Par heure	Quantité de données écrites ou lues pour les fichiers à l'aide du débit élastique.
<i>region</i> -IADataAccess-Bytes	N/A	Go	Par heure	Quantité de données consultées dans le stockage EFS Infrequent Access (IA).
<i>region</i> -IATimedStorage-ByteHrs	StorageElasticIA	Go Mo	Par heure	Nombre de Go par mois pendant lesquels les données ont été stockées dans le stockage EFS IA.

Type d'utilisation	CloudWatch métrique	Unités	Granularité	Description
<i>region</i> -IATimedStorage-ET-ByteHrs	StorageElasticity.IA	Go Mo	Par heure	Nombre de Go par mois pendant lesquels les données des fichiers utilisant le débit élastique ont été stockées dans le stockage EFS IA.
<i>region</i> -IATimedStorage-ET-SmallFiles	StorageElasticity.IASizeOverhead	Go Mo	Par heure	Nombre de Go par mois pendant lesquels de petits fichiers (inférieurs à 128 Ko) ont été stockés dans le stockage EFS IA, pour les fichiers utilisant le débit élastique.
<i>region</i> -IATimedStorage-SmallFiles	StorageElasticity.IASizeOverhead	Go Mo	Par heure	Nombre de Go par mois pendant lesquels les petits fichiers (inférieurs à 128 Ko) ont été stockés dans le stockage EFS IA.
<i>region</i> -IATimedStorage-Z-ByteHrs	StorageElasticity.IA	Go Mo	Par heure	Taille réelle des données stockées dans le stockage EFS IA pour les systèmes de fichiers One Zone.
<i>region</i> -IATimedStorage-Z-SmallFiles	StorageElasticity.IASizeOverhead	Go Mo	Par heure	Nombre de Go par mois pendant lesquels les petits fichiers (inférieurs à 128 Ko) ont été stockés dans le stockage EFS IA pour les systèmes de fichiers One Zone.
<i>region</i> -IncludedTP-MiBpsHrs	PermittedThroughput	MiBps-Non	Par heure	Le débit maximum qu'un système de fichiers peut gérer.
<i>region</i> -ProvisionedTP-MiBpsHrs	PermittedThroughput	MiBps-Non	Par heure	Pour les systèmes de fichiers utilisant le débit provisionné, le débit provisionné ou le débit maximal autorisé.

Type d'utilisation	CloudWatch métrique	Unités	Granularité	Description
<i>region-</i> TimedStorage-ByteHrs	StorageElastic.StorageStandard	Go Mo	Par heure	La quantité totale réelle de données stockées dans le stockage standard EFS pour les systèmes de fichiers régionaux.
<i>region-</i> TimedStorage-Z-ByteHrs	StorageElastic.StorageStandard	Go Mo	Par heure	La quantité totale réelle de données stockées dans le stockage standard EFS pour les systèmes de fichiers One Zone.

Remarques

- Le stockage des archives EFS est facturé pour une durée de stockage minimale de 90 jours, même si les données sont supprimées avant 90 jours.
- Des frais de hiérarchisation s'appliquent aux données échelonnées du stockage EFS Standard au stockage EFS Infrequent Access (IA), et du stockage EFS IA au stockage EFS Standard.
- Le stockage EFS IA et EFS Archive a une taille de fichier facturable minimale de 128 KiB. Les fichiers dont la taille est inférieure à 128 KiB peuvent être hiérarchisés selon ces classes de stockage, mais 128 KiB de stockage sont facturés au tarif de classe de stockage approprié.
- Pour les systèmes de fichiers utilisant le débit Elastic, les opérations de métadonnées sont mesurées par incréments de 1 KiB après les 4 premiers KiB et les opérations de données sont mesurées par incréments de 1 KiB après les 32 premiers KiB.
- L'utilisation du stockage est calculée en gigaoctets binaires (Go), où 1 Go correspond à 2^{30} octets. Consultez [Comment Amazon EFS indique les tailles des systèmes de fichiers et des objets](#) pour plus de détails sur la façon dont l'utilisation du stockage et du débit est mesurée pour calculer votre facture Amazon EFS.
- Le nombre de Go par mois est obtenu en prenant le nombre total d'heures en Go, en les agrégeant au cours d'un mois, puis en divisant par le nombre d'heures du mois en question.

Opérations de suivi dans vos rapports d'utilisation

Les opérations décrivent l'action entreprise sur votre système de fichiers EFS par le type d'utilisation spécifié. Les opérations sont indiquées par des codes explicites comme `Read` ou `Delete`. Pour voir quelles actions sur votre système de fichiers ont généré un type d'utilisation spécifique, utilisez ces codes. Lorsque vous générez un rapport d'utilisation, vous pouvez baser votre rapport sur toutes les opérations ou sur une opération en particulier comme `Write`.

Spécifications de performance d'Amazon EFS

Les sections suivantes fournissent une présentation des performances Amazon EFS et décrivent l'impact de la configuration de votre système de fichiers sur les principaux aspects de la performance. Nous fournissons également des conseils et des recommandations importants pour optimiser les performances de votre système de fichiers.

Rubriques

- [Récapitulatif des performances](#)
- [Classes de stockage](#)
- [Modes de performances](#)
- [Modes de débit](#)
- [Conseils sur les performances Amazon EFS](#)
- [Résolution des problèmes de performances d'Amazon EFS](#)
- [Résolution des problèmes d'AMI et de noyau](#)

Récapitulatif des performances

Les performances du système de fichiers sont généralement mesurées à l'aide des dimensions de latence, de débit et d'Input/Output opérations par seconde (IOPS). Les performances d'Amazon EFS dans ces domaines dépendent de la configuration de votre système de fichiers. Les configurations suivantes ont une incidence sur les performances d'un système de fichiers Amazon EFS :

- Type de système de fichiers – Par région ou zone unique
- Mode performance : usage général ou nombre maximal d'E/S

Important

Le mode I/O de performance maximale présente des latences par opération plus élevées que le mode de performance à usage général. Nous vous recommandons de toujours utiliser le mode de performance Usage général pour des performances plus rapides. Pour de plus amples informations, veuillez consulter [Modes de performances](#).

- Mode de débit – Elasticité, Alloué, ou Transmission en rafales

Le tableau suivant décrit les spécifications de performance des systèmes de fichiers utilisant le mode de performance General Purpose et les différentes combinaisons possibles de type de système de fichiers et de mode de débit.

Spécifications de performance pour les systèmes de fichiers utilisant le mode de performance General Purpose

Configuration du stockage et du débit		Latence		Nombre maximal d'IOPS		Débit maximal		
Type de système de fichiers	Mode de débit	Opérations de lecture	Opérations d'écriture	Opérations de lecture	Opérations d'écriture	Performance système lecture ¹	Performance système écriture ¹	Lecture/écriture par client
Régional	Elasticité	Seulement 250 microsecondes (µs)	Seulement 2,7 millisecondes (ms)	900 000 à 2 500 000 ²	500 000 ²	20 à 60 gibioctets par seconde () GiBps	1 à 5 GiBps	1 500 mégaoctets par seconde (3) MiBps
Régional	Alloué	Seulement 250 µs	Seulement 2,7 ms	55 000	25 000	3 à 10 GiBps	1—3,33 GiBps	500 MiBps
Régional	Transmission en rafales	Seulement 250 µs	Seulement 2,7 ms	35 000	7 000	3 à 5 GiBps	1 à 3 GiBps	500 MiBps
Une zone	Élastique, provisionné, éclatant	Seulement 250 µs	Seulement 1,6 ms	35 000	7 000	3 GiBps ⁴	1 GiBps ⁴	500 MiBps

1. Le débit de lecture et d'écriture maximal dépend du Région AWS. Un débit supérieur au débit maximal Région AWS d'un nécessite une augmentation du quota de débit. Toute demande de

- débit supplémentaire est examinée sur une case-by-case base individuelle par l'équipe de service Amazon EFS. L'approbation peut dépendre de votre type de charge de travail. Pour en savoir plus sur la demande d'une révision, veuillez consulter [Quotas Amazon EFS](#).
2. Par défaut, les systèmes de fichiers qui utilisent le débit élastique génèrent un maximum de 90 000 IOPS en lecture pour les données rarement consultées, 250 000 IOPS en lecture pour les données fréquemment consultées et 50 000 IOPS en écriture. Si votre charge de travail nécessite plus d'IOPS, vous pouvez demander une augmentation jusqu'à 10 fois ces chiffres. Pour de plus amples informations, veuillez consulter [Les quotas Amazon EFS que vous pouvez augmenter](#). Des recommandations supplémentaires s'appliquent pour atteindre un maximum d'IOPS. Pour de plus amples informations, veuillez consulter [the section called "Optimisation des charges de travail exigeant un débit et des IOPS élevés"](#).
 3. Le débit de lecture et d'écriture combiné maximal est de 1 500 MiBps pour les systèmes de fichiers utilisant le débit élastique et montés à l'aide de la version 2.0 ou ultérieure du client Amazon EFS (amazon-efs-utils version) ou du pilote Amazon EFS CSI (. aws-efs-csi-driver Pour tous les autres systèmes de fichiers, la limite de débit est de 500 MiBps. Pour plus d'informations sur le client Amazon EFS, consultez [Installation du client Amazon EFS](#).
 4. Les systèmes de fichiers One Zone qui utilisent le débit en rafale peuvent atteindre les mêmes débits en per-file-system lecture et en écriture que les systèmes de fichiers régionaux utilisant le débit en rafale (lecture maximale de 5 GiBps pour la lecture et 3 pour l'écriture). GiBps

Classes de stockage

Les classes de stockage Amazon EFS sont conçues pour offrir le stockage le plus efficace possible en fonction des cas d'utilisation.

- La classe de stockage EFS Standard utilise le stockage SSD pour fournir les niveaux de latence les plus faibles pour les fichiers fréquemment consultés. Cette classe de stockage fournit des latences au premier octet aussi faibles que 250 microsecondes pour les lectures et 2,7 millisecondes pour les écritures.
- Les classes de stockage EFS Infrequent Access (IA) et EFS Archive stockent les données les moins fréquemment consultées qui ne nécessitent pas les performances de latence requises par les données fréquemment consultées. Ces classes de stockage fournissent des latences sur le premier octet de plusieurs dizaines de millisecondes.

Pour plus d'informations sur les classes de stockage EFS, consultez [the section called "Classes de stockage EFS"](#).

Modes de performances

Amazon EFS propose deux modes de performance, General Purpose et Max I/O.

- Le mode General Purpose présente la latence par opération la plus faible et constitue le mode de performance par défaut pour les systèmes de fichiers. Les systèmes de fichiers One Zone utilisent toujours le mode de performance General Purpose. Nous vous recommandons de toujours utiliser le mode de performance Usage général pour des performances plus rapides.
- Le I/O mode Max est un type de performance de génération précédente conçu pour les charges de travail hautement parallélisées qui peuvent tolérer des latences plus élevées que le mode General Purpose. Le I/O mode Max n'est pas pris en charge pour les systèmes de fichiers One Zone ou les systèmes de fichiers qui utilisent le débit élastique.

Important

En raison des latences par opération plus élevées avec Max I/O, nous recommandons d'utiliser le mode de performance Usage général pour tous les systèmes de fichiers.

Pour garantir que votre charge de travail reste dans les limites d'IOPS disponibles pour les systèmes de fichiers utilisant le mode de performance General Purpose, vous pouvez surveiller la `PercentIOLimit` CloudWatch métrique. Pour de plus amples informations, veuillez consulter [CloudWatch métriques pour Amazon EFS](#).

Les applications peuvent mettre à l'échelle leurs IOPS avec élasticité jusqu'à la limite associée au mode performance. Les IOPS ne vous sont pas facturées séparément ; elles sont incluses dans la comptabilisation du débit d'un système de fichiers. Chaque demande de système de fichiers réseau (NFS) est comptabilisée comme un débit de 4 kilo-octets (Ko), ou sa taille réelle de demande et de réponse, selon la valeur la plus élevée.

Modes de débit

Le mode de débit d'un système de fichiers détermine le débit disponible pour votre système de fichiers. Amazon EFS propose trois modes de débit : élastique, alloué, et transmission en rafales.

Le débit de lecture est réduit de manière à être supérieur au débit d'écriture. Le débit maximum disponible pour chaque mode de débit dépend du Région AWS. Pour plus d'informations sur le débit maximal du système de fichiers dans les différentes régions, consultez [Quotas Amazon EFS](#).

Votre système de fichiers peut atteindre 100 % de son débit combiné de lecture et d'écriture. Par exemple, si votre système de fichiers utilise 33 % de sa limite de débit de lecture, il peut atteindre simultanément jusqu'à 67 % de sa limite de débit d'écriture. Vous pouvez surveiller l'utilisation du débit de votre système de fichiers dans le graphique d'utilisation du débit (%) sur la page détaillée du système de fichiers de la console. Pour de plus amples informations, veuillez consulter [Surveillance des performances de débit](#).

Choisir le bon mode de débit pour un système de fichiers

Le choix du mode de débit adapté à votre système de fichiers dépend des exigences de performance de votre charge de travail.

- Débit élastique (recommandé) : utilisez le débit élastique par défaut lorsque vous êtes confronté à des charges de travail élevées ou imprévisibles et à des exigences de performances difficiles à prévoir, ou lorsque votre application augmente le débit à un average-to-peak ratio de 5 % ou moins. Pour de plus amples informations, veuillez consulter [Débit élastique](#).
- Débit provisionné : utilisez le débit provisionné si vous connaissez les exigences de performance de votre charge de travail ou lorsque votre application augmente le débit à un average-to-peak ratio de 5 % ou plus. Pour de plus amples informations, veuillez consulter [Débit alloué](#).
- Débit exceptionnel : utilisez le débit maximal lorsque vous souhaitez un débit qui s'adapte à la quantité de stockage de votre système de fichiers.

Si, après avoir utilisé le débit en rafale, vous constatez que le débit de votre application est limité (par exemple, elle utilise plus de 80 % du débit autorisé ou si vous avez utilisé tous vos crédits en rafale), vous devez utiliser le débit élastique ou provisionné. Pour de plus amples informations, veuillez consulter [Débit exceptionnel](#).

Pour plus d'informations sur les métriques de demande Amazon EFS, consultez [CloudWatch métriques pour Amazon EFS](#).

Débit élastique

Pour les systèmes de fichiers qui utilisent le débit élastique, Amazon EFS augmente ou diminue automatiquement les performances de débit pour répondre aux besoins de votre activité de charge

de travail. Le débit élastique est le meilleur mode de débit pour les charges de travail élevées ou imprévisibles dont les exigences de performance sont difficiles à prévoir, ou pour les applications dont le débit est inférieur ou égal à 5 % du débit maximal en moyenne (le ratio). average-to-peak

Étant donné que les performances de débit des systèmes de fichiers dotés d'un débit élastique évoluent automatiquement, vous n'avez pas besoin de spécifier ou de provisionner la capacité de débit pour répondre aux besoins de votre application. Vous ne payez que pour la quantité de métadonnées et de données lues ou écrites, et vous n'accumulez ni ne consommez de crédits en rafale lorsque vous utilisez le débit élastique.

Note

Bien que le débit élastique soit conçu pour s'adapter de manière élastique à votre débit, nous vous recommandons de mettre en œuvre une gouvernance appropriée en surveillant les indicateurs avec des indicateurs CloudWatch (mesurésIOBytes) et des alertes d'utilisation dans le cadre de vos meilleures pratiques opérationnelles. Cela vous permet de maintenir une utilisation optimale des ressources et de respecter les paramètres opérationnels planifiés. Pour de plus amples informations, veuillez consulter [Surveillance des métriques avec Amazon CloudWatch](#).

Pour plus d'informations sur les limites de débit élastiques par région, consultez. [Les quotas Amazon EFS que vous pouvez augmenter](#)

Débit alloué

Avec le débit provisionné, vous spécifiez le niveau de débit que le système de fichiers peut atteindre indépendamment de la taille du système de fichiers ou de l'augmentation du solde créditeur. Utilisez le débit provisionné si vous connaissez les exigences de performance de votre charge de travail ou si votre application atteint un débit égal ou supérieur à 5 % du ratio. average-to-peak

Pour les systèmes de fichiers utilisant le débit provisionné, vous êtes facturé en fonction du débit activé pour le système de fichiers. Le Montant du débit facturé en un Mois est basé sur le débit fourni en sus du débit de base inclus dans votre système de fichiers à partir du stockage standard, jusqu'aux limites de débit de base en rafales en vigueur dans le Région AWS.

Si le débit de base du système de fichiers dépasse le débit provisionné, il utilise automatiquement le débit de rafale autorisé pour le système de fichiers (dans la limite des limites de débit de base de rafale en vigueur à cet égard). Région AWS

Pour plus d'informations sur les limites de débit provisionnées par région, consultez. [Les quotas Amazon EFS que vous pouvez augmenter](#)

Débit exceptionnel

Un débit maximal est recommandé pour les charges de travail qui nécessitent un débit adapté à la quantité de stockage de votre système de fichiers. Avec le débit en rafale, le débit de base est proportionnel à la taille du système de fichiers dans la classe de stockage Standard, à raison de 50 par GiB KiBps de stockage. Les crédits de rafale sont accumulés lorsque le système de fichiers consomme Moins que son débit de base et sont déduits lorsque le débit dépasse le débit de base.

Lorsque des crédits en rafale sont disponibles, un système de fichiers peut atteindre un débit de 100 MiBps par TiB dans le stockage standard (50 KiBps par GiB), jusqu'à Région AWS la limite, avec un minimum de 100. MiBps Si aucun crédit en rafale n'est disponible, un système de fichiers peut en lire jusqu'à 50 MiBps par TiB de stockage, avec un minimum de 1. MiBps

Pour plus d'informations sur le débit en rafale par région, consultez. [General resource quotas that cannot be changed](#)

Comprendre les crédits en rafales Amazon EFS

Avec le débit en rafale, chaque système de fichiers gagne des crédits en rafale au fil du temps à un taux de référence déterminé par la taille du système de fichiers stocké dans la classe de stockage EFS Standard. Le taux de référence est de 50 MiBps par tébioctet [TiB] de stockage (équivalent à 50 par KiBps GiB de stockage). Amazon EFS mesure les opérations de lecture jusqu'à un tiers du taux des opérations d'écriture, ce qui permet au système de fichiers de générer un taux de référence allant jusqu'à 150 KiBps par GiB de débit de lecture ou 50 par KiBps GiB de débit d'écriture.

Un système de fichiers peut générer du débit à son débit de référence mesuré en continu. Un système de fichiers accumule des crédits en rafale chaque fois qu'il est inactif ou que son débit est inférieur à son taux de référence mesuré. Les crédits de transmission en rafales cumulés permettent au système de fichiers d'émettre un débit supérieur à son taux de référence.

Par exemple, un système de fichiers contenant 100 GiB de données mesurées dans la classe de stockage Standard a un débit de référence de 5. MiBps Sur une période d'inactivité de 24 heures, le système de fichiers gagne 432 000 MiB de crédit ($5 \text{ MiB} \times 86\,400 \text{ secondes} = 432\,000 \text{ MiB}$), qui peuvent être utilisés MiBps pour atteindre 100 MiB pendant 72 minutes ($432\,000 \text{ MiB} \div 100 = 72 \text{ minutes}$). MiBps

Les systèmes de fichiers d'une taille supérieure à 1 TiB peuvent toujours transmettre en rafales jusqu'à 50 % du temps s'ils sont inactifs pendant les 50 % du temps.

Le tableau suivant fournit des exemples de comportement de transmission en rafales.

Taille de système de fichiers	Débit de transmission en rafales.	Débit de référence
100 GiB de données mesurées dans le stockage standard	• Passez à 300 (MiBps) en lecture seule pendant 72 minutes maximum par jour, ou • Passez à 100 en MiBps écriture seule pendant 72 minutes par jour	• Conduisez jusqu'à 15 unités en MiBps lecture seule en continu • Conduisez jusqu'à 5 disques en MiBps écriture seule en continu
100 TiB de données mesurées dans le stockage standard	• Passez à 300 MiBps en lecture seule 12 heures par jour, ou • Passez à 100 en MiBps écriture seule pendant 12 heures par jour	• Drive 150 en MiBps lecture seule en continu • Drive 50 en MiBps écriture seule en continu
10 TiB de données mesurées dans le stockage standard	• Passez à 3 GiBps en lecture seule 12 heures par jour, ou • Passez à 1 en GiBps écriture seule pendant 12 heures par jour	• Drive 1.5 en GiBps lecture seule en continu • Drive 500 en MiBps écriture seule en continu
Généralement, les systèmes de fichiers plus volumineux	• Passez à 300 MiBps en lecture seule par TiB de stockage pendant 12 heures par jour, ou • Passez à 100 en MiBps écriture seule par TiB de stockage pendant 12 heures par jour	• Lecteur 150 unités en MiBps lecture seule par TiB de stockage en continu • Lecteur de 50 unités en MiBps écriture seule par TiB de stockage en continu

Note

Amazon EFS fournit un débit mesuré de 1 MiBps pour tous les systèmes de fichiers, même si le débit de référence est inférieur.

La taille du système de fichiers utilisée pour déterminer les taux de base et de rafale est la taille mesurée `ValueInStandard` disponible via l'opération API [DescribeFileSystems](#).

Les systèmes de fichiers peuvent obtenir des crédits jusqu'à un solde maximum de 2,1 TiB pour les systèmes de fichiers d'une taille inférieure à celle 1 TiB, ou 2,1 TiB par TiB stocké pour les systèmes de fichiers d'une taille supérieure à 1 TiB. Avec cette approche, les systèmes de fichiers peuvent cumuler suffisamment de crédits pour transmettre en rafales pendant 12 heures en continu.

Restrictions relatives au débit de commutation et à la modification du montant provisionné

Vous pouvez changer le mode de débit d'un système de fichiers existant et Modifier le débit. Toutefois, après avoir basculé le mode de débit sur Débit provisionné ou modifié le montant du débit provisionné, les actions suivantes sont limitées pendant 24 heures :

- Passage du mode débit provisionné au mode débit élastique ou en mode débit en rafale.
- Diminution du débit provisionné.

Conseils sur les performances Amazon EFS

Lors de l'utilisation d'Amazon EFS, gardez à l'esprit les conseils de performance suivants :

I/O Taille moyenne

La nature distribuée d'Amazon EFS permet de hauts niveaux de disponibilité, de durabilité et de capacité de mise à l'échelle. Cette architecture distribuée entraîne de faibles coûts en matière de latence pour chaque opération réalisée sur les fichiers. En raison de cette latence par opération, le débit global augmente généralement à mesure que la I/O taille moyenne augmente, car les frais généraux sont amortis sur une plus grande quantité de données.

Optimisation des charges de travail exigeant un débit et des IOPS élevés

Pour les charges de travail nécessitant un débit et des IOPS élevés, utilisez des systèmes de fichiers régionaux configurés avec le mode de performance General Purpose et le débit élastique.

 Note

Pour atteindre le maximum d'IOPS en lecture pour les données fréquemment consultées, le système de fichiers doit utiliser le débit élastique.

Pour atteindre les niveaux de performance les plus élevés, vous devez tirer parti de la parallélisation en configurant votre application ou votre charge de travail comme suit.

1. Répartissez la charge de travail de manière uniforme sur tous les clients et annuaires, avec au Moins le même nombre de répertoires que le nombre de clients utilisés.
2. Minimisez les conflits en alignant les threads individuels sur des jeu de données ou des fichiers distincts.
3. Répartissez la charge de travail sur 10 clients NFS ou plus, avec au moins 64 threads par client dans une seule cible de montage.

Connexions simultanées

Vous pouvez monter des systèmes de fichiers Amazon EFS sur des milliers d'instances de calcul Amazon EC2 et d'autres instances de AWS calcul simultanément. Vous pouvez obtenir des niveaux de débit plus élevés sur votre système de fichiers dans les instances regroupées.

Modèle de demande

Si vous activez les écritures asynchrones sur votre système de fichiers, les opérations d'écriture en attente sont mises en mémoire tampon sur l' EC2 instance Amazon avant d'être écrites dans Amazon EFS de manière asynchrone. Les écritures asynchrones ont généralement des latences Moindres. Lors de l'exécution d'écritures asynchrones, le noyau utilise de la mémoire supplémentaire pour la mise en cache.

Un système de fichiers qui a activé des écritures synchrones, ou qui ouvre les fichiers à l'aide d'une option qui ignore le cache (par exemple, `O_DIRECT`), émettra des requêtes synchrones vers Amazon EFS. Chaque opération fera un aller retour entre le client et Amazon EFS.

 Note

Le modèle de demande que vous avez choisi comporte des compromis en termes de cohérence (si vous utilisez EC2 plusieurs instances Amazon) et de rapidité. L'utilisation

d'écritures synchrones améliore la cohérence des données en effectuant chaque transaction de demande d'écriture avant de traiter la demande suivante. L'utilisation d'écritures asynchrones permet d'augmenter le débit en mettant en mémoire tampon les opérations d'écriture en attente.

Paramètres de Montage du client NFS

Vérifiez que vous utilisez les options de Montage recommandées, comme indiqué dans [Montage des systèmes de fichiers EFS](#) et [Considérations relatives au montage pour Linux](#).

Lorsque vous montez vos systèmes de fichiers sur EC2 des instances Amazon, Amazon EFS prend en charge les protocoles Network File System versions 4.0 et 4.1 (NFSv4). NFSv4.1 fournit de meilleures performances pour les opérations de lecture parallèle de petits fichiers (supérieures à 10 000 fichiers par seconde) par rapport à NFSv4 .0 (moins de 1 000 fichiers par seconde). Pour les instances Amazon EC2 macOS exécutant macOS Big Sur, seule la version NFSv4 2.0 est prise en charge.

N'utilisez pas les options de Montage suivantes :

- `noac,actimeo=0,acregmax=0,acdirmax=0` — Ces options désactivent le cache d'attributs, ce qui a un impact très important sur les performances.
- `lookupcache=pos, lookupcache=none` – Ces options désactivent le cache de consultation des noms de fichiers, qui a un impact très important sur les performances.
- `fsc`— Cette option active la mise en cache des fichiers locaux, mais ne Modifie pas la cohérence du cache NFS et ne réduit pas les latences.

Note

Lorsque vous Montez votre système de fichiers, pensez à augmenter la taille des tampons de lecture et d'écriture de votre client NFS à 1 Mo.

Optimisation des performances des petits fichiers

Vous pouvez améliorer les performances des petits fichiers en minimisant les réouvertures de fichiers, en augmentant le parallélisme et en regroupant les fichiers de référence dans la mesure du possible.

- Minimisez le nombre d'allers-retours vers le serveur.

Ne fermez pas inutilement des fichiers si vous en aurez besoin ultérieurement dans un flux de travail. Le fait de garder les descripteurs de fichiers ouverts permet d'accéder directement à la copie locale dans le cache. Les opérations d'ouverture, de fermeture et de métadonnées de fichiers ne peuvent généralement pas être effectuées de manière asynchrone ou via un pipeline.

Lors de la lecture ou de la rédaction de petits fichiers, les deux allers-retours supplémentaires sont importants.

Chaque aller-retour (ouverture de fichier, fermeture de fichier) peut prendre autant de temps que la lecture ou l'écriture de mégaoctets de données en masse. Il est plus efficace d'ouvrir un fichier d'entrée ou de sortie une seule fois, au début de votre tâche de calcul, et de le maintenir ouvert pendant toute la durée de la tâche.

- Utilisez le parallélisme pour réduire l'impact des temps d'aller-retour.
- Regroupez les fichiers de référence dans un fichier `.zip`. Certaines applications utilisent un grand nombre de petits fichiers de référence, pour la plupart en lecture seule. Le fait de les regrouper dans un fichier `.zip` permet de lire de nombreux fichiers en un seul aller-retour (ouverture/fermeture).

Le format `.zip` permet un accès aléatoire à des fichiers individuels.

Optimisation des performances de disque

Lors de l'exécution d'une liste (`ls`) sur de très grands répertoires (plus de 100 000 fichiers) Modifiés simultanément, les clients NFS Linux peuvent se bloquer et ne pas renvoyer de réponse. Ce problème est résolu dans le noyau 5.11, qui a été porté sur les noyaux Amazon Linux 2 4.14, 5.4 et 5.10.

Nous vous recommandons de limiter le nombre de répertoires de votre système de fichiers à Moins de 10 000, si possible. Chaque fois que possible, utilisez les sous-répertoires imbriqués.

Lorsque vous listez un répertoire, évitez d'obtenir des attributs de fichier s'ils ne sont pas obligatoires, car ils ne sont pas stockés dans le répertoire lui-même.

Optimisation de la taille NFS `read_ahead_kb`

L'attribut `read_ahead_kb` NFS définit le nombre de kilo-octets que le noyau Linux doit lire à l'avance ou à récupérer au cours d'une opération de lecture séquentielle.

Pour les versions du noyau Linux antérieures à la version 5.4.*, la `read_ahead_kb` valeur est définie en multipliant `NFS_MAX_READAHEAD` par la valeur pour `rsize` (la taille de la mémoire tampon de lecture configurée par le client définie dans les options de Montage). Lorsque vous utilisez les [options de Montage recommandées](#), cette formule définit `read_ahead_kb` sur 15 Mo.

Note

Avec les versions 5.4.* du noyau Linux, le client NFS Linux utilise une valeur `read_ahead_kb` par défaut de 128 Ko. Nous recommandons d'augmenter cette valeur jusqu'à 15 Mo.

L'assistant de Montage Amazon EFS disponible dans les versions 1.33.2 `amazon-efs-utils` et ultérieures Modifie automatiquement la valeur `read_ahead_kb` pour qu'elle soit égale à `15 * rsize`, soit 15 Mo, après le Montage du système de fichiers.

Pour les noyaux Linux 5.4 ou versions ultérieures, si vous n'utilisez pas l'assistant de Montage pour Monter vos systèmes de fichiers, pensez à régler manuellement `read_ahead_kb` à 15 Mo pour améliorer les performances. Après avoir Monté le système de fichiers, vous pouvez réinitialiser la valeur `read_ahead_kb` à l'aide de la commande suivante. Avant d'utiliser cette commande, remplacez les valeurs suivantes :

- Remplacez *read-ahead-value-kb* par la taille souhaitée en kilo-octets.
- Remplacez *efs-mount-point* par le point de Montage du système de fichiers.

```
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"
```

L'exemple qui suit définit une taille `read_ahead_kb` de 1 Mo.

```
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"
```

Résolution des problèmes de performances d'Amazon EFS

Si vous rencontrez des problèmes avec Amazon EFS et que vous avez du mal à les résoudre, vérifiez que vous utilisez un noyau Linux récent. Si vous utilisez une distribution Linux d'entreprise, nous vous recommandons de procéder comme suit :

- Amazon Linux 2 avec le noyau 4.3 ou plus récent
- Amazon Linux 2015.09 ou version ultérieure
- RHEL 7.3 ou version ultérieure
- Toutes les versions Ubuntu 16.04
- Ubuntu 14.04 avec noyau 3.13.0-83 ou version ultérieure
- SLES 12 Sp2 ou version ultérieure

Si vous utilisez une autre distribution ou un noyau personnalisé, nous recommandons la version 4.3 ou version ultérieure.

Note

RHEL 6.9 peut être sous-optimal pour certaines charges de travail en raison des [Performances médiocres à l'ouverture de plusieurs fichiers en parallèle](#).

Rubriques

- [Impossible de créer un système de fichiers EFS](#)
- [Accès refusé aux fichiers autorisés sur le système de fichiers NFS](#)
- [Erreurs lors de l'accès à la console Amazon EFS](#)
- [L' EC2 instance Amazon se bloque](#)
- [Une application qui écrit de grandes quantités de données se bloque](#)

- [Performances médiocres à l'ouverture de plusieurs fichiers en parallèle](#)
- [Paramètres NFS personnalisés entraînant des délais d'écriture](#)
- [La création de sauvegardes avec Oracle Recovery Manager est lente](#)

Impossible de créer un système de fichiers EFS

Une demande de création d'un système de fichiers EFS échoue avec le message suivant :

```
User: arn:aws:iam::111122223333:user/username is not authorized to
perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

Action à exécuter

Vérifiez votre politique AWS Identity and Access Management (IAM) pour confirmer que vous êtes autorisé à créer des systèmes de fichiers EFS avec les conditions de ressources spécifiées. Pour de plus amples informations, veuillez consulter [Gestion des identités et des accès pour Amazon EFS](#).

Accès refusé aux fichiers autorisés sur le système de fichiers NFS

Lorsqu'un utilisateur auquel plus de 16 groupes d'accès IDs (GIDs) ont été affectés tente d'effectuer une opération sur un système de fichiers NFS, l'accès aux fichiers autorisés du système de fichiers peut lui être refusé. [Ce problème se produit parce que le protocole NFS prend en charge un maximum de 16 GIDs par utilisateur, et que tout ajout GIDs est tronqué à partir de la demande du client NFS, comme défini dans la RFC 5531.](#)

Action à exécuter

Restructurez vos mappages d'utilisateurs et de groupes NFS afin qu'un maximum de 16 groupes d'accès soient attribués à chaque utilisateur (). GIDs

Erreurs lors de l'accès à la console Amazon EFS

Cette section décrit les erreurs que les utilisateurs peuvent rencontrer lors de l'accès à la console de gestion Amazon EFS.

Erreur lors de l'authentification des informations d'identification pour
ec2:DescribeVPCs

Le message d'erreur suivant s'affiche lors de l'accès à la console Amazon EFS :

AuthFailure: An error occurred authenticating your credentials for ec2:DescribeVPCs.

Cette erreur indique que vos informations de connexion ne se sont pas authentifiées avec succès auprès du EC2 service Amazon. La console Amazon EFS appelle le EC2 service Amazon en votre nom lors de la création de systèmes de fichiers EFS dans le VPC de votre choix.

Action à exécuter

Assurez-vous que l'heure à laquelle le client accède à la console Amazon EFS est correctement définie.

L' EC2 instance Amazon se bloque

Une EC2 instance Amazon peut se bloquer parce que vous avez supprimé une cible de montage du système de fichiers sans avoir préalablement démonté le système de fichiers.

Action à exécuter

Avant de supprimer la cible de montage d'un système de fichiers, démontez le système de fichiers. Pour plus d'informations sur le démontage de votre système de fichiers Amazon EFS, consultez [Démontage des systèmes de fichiers](#).

Une application qui écrit de grandes quantités de données se bloque

Une application qui écrit une grande quantité de données dans Amazon EFS se bloque et provoque le redémarrage de l'instance.

Action à exécuter

Si une application est trop longue à écrire toutes les données dans Amazon EFS, Linux peut redémarrer, car il semble que le processus ne répond plus. Deux paramètres de configuration du noyau définissent ce comportement, `kernel.hung_task_panic` et `kernel.hung_task_timeout_secs`.

Dans l'exemple suivant, l'état du processus suspendu est indiqué par la commande `ps` avec `D` avant le redémarrage de l'instance, ce qui indique que le processus est en attente en E/S.

```
$ ps aux | grep large_io.py
root 33253 0.5 0.0 126652 5020 pts/3 D+ 18:22 0:00 python large_io.py
/efs/large_file
```

Pour éviter un redémarrage, augmentez le délai d'attente ou désactivez le mode paniques du noyau lorsqu'une tâche suspendue est détectée. La commande suivante désactive le mode panique du noyau de la tâche suspendue sur la plupart des distributions Linux.

```
$ sudo sysctl -w kernel.hung_task_panic=0
```

Performances médiocres à l'ouverture de plusieurs fichiers en parallèle

Les applications qui ouvrent plusieurs fichiers en parallèle ne rencontrent pas l'amélioration attendue des performances en matière de parallélisation E/S.

Action à exécuter

Ce problème se produit sur les clients Network File System version 4 (NFSv4) et sur les clients RHEL 6 utilisant la version NFSv4 .1, car ces clients NFS sérialisent les opérations NFS OPEN et CLOSE. Utilisez la version 4.1 du protocole NFS et l'une des [distributions Linux](#) suggérées qui ne rencontrent pas ce problème.

Si vous ne pouvez pas utiliser la NFSv4 version .1, sachez que le client Linux NFSv4 .0 sérialise les demandes d'ouverture et de fermeture par ID utilisateur et par groupe. Cette sérialisation se produit même si plusieurs processus ou plusieurs threads émettent des requêtes en même temps. Le client n'envoie qu'une seule opération d'ouverture ou de fermeture à un serveur NFS à la fois, lorsque toutes les opérations IDs correspondent. Pour contourner ces problèmes, vous pouvez effectuer l'une des actions suivantes :

- Vous pouvez exécuter chaque processus à partir d'un ID utilisateur différent sur la même EC2 instance Amazon.
- Vous pouvez laisser l'utilisateur IDs le même pour toutes les demandes ouvertes et modifier l'ensemble de groupes à la IDs place.
- Vous pouvez exécuter chaque processus à partir d'une EC2 instance Amazon distincte.

Paramètres NFS personnalisés entraînant des délais d'écriture

Vous disposez de paramètres client NFS personnalisés, et il faut jusqu'à trois secondes à une EC2 instance Amazon pour qu'une opération d'écriture soit effectuée sur un système de fichiers à partir d'une autre EC2 instance Amazon.

Action à exécuter

Si vous rencontrez ce problème, vous pouvez le résoudre de l'une des façons suivantes :

- Si la mise en cache des attributs est activée sur le client NFS de l' EC2 instance Amazon qui lit les données, démontez votre système de fichiers. Ensuite, remontez-le avec l'option `noac` pour désactiver la mise en cache des attributs. La mise en cache des attributs dans la NFSv4 version .1 est activée par défaut.

 Note

Désactiver la mise en cache côté client peut éventuellement réduire les performances de votre application.

- Vous pouvez également effacer votre cache d'attribut à la demande en utilisant un langage de programmation compatible avec les procédures NFS. Pour ce faire, vous pouvez envoyer une requête de procédure `ACCESS` immédiatement avant une demande de lecture.

Par exemple, en utilisant le langage de programmation Python, vous pouvez construire l'appel suivant :

```
# 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 création de sauvegardes avec Oracle Recovery Manager est lente

La création de sauvegardes avec Oracle Recovery Manager peut être lente si Oracle Recovery Manager reste en pause pendant 120 secondes avant de démarrer une tâche de sauvegarde.

Action à exécuter

Si vous rencontrez ce problème, désactivez Oracle Direct NFS, comme décrit dans [Enabling and Disabling Direct NFS Client Control of NFS](#) dans le centre d'aide Oracle.

 Note

Amazon EFS ne prend pas en charge Oracle Direct NFS.

Résolution des problèmes d'AMI et de noyau

Vous trouverez ci-dessous des informations sur la résolution des problèmes liés à certaines versions d'Amazon Machine Image (AMI) ou du noyau lors de l'utilisation d'Amazon EFS à partir d'une EC2 instance Amazon.

Rubriques

- [Impossible d'exécuter la commande chown](#)
- [Le système de fichiers continue à effectuer des opérations plusieurs fois en raison d'un bogue client](#)
- [Client bloqué](#)
- [L'affichage de la liste de fichiers d'un répertoire volumineux prend beaucoup de temps.](#)

Impossible d'exécuter la commande chown

Vous ne pouvez pas modifier le propriétaire d'un fichier/répertoire à l'aide de la commande chown Linux.

Versions de noyau avec ce bogue

2.6.32

Action à exécuter

Vous pouvez résoudre cette erreur en procédant comme suit :

- Si vous exécutez chown pour l'étape d'installation unique nécessaire pour modifier la propriété du répertoire racine EFS, vous pouvez exécuter la commande chown depuis une instance exécutant une version plus récente du noyau. Par exemple, vous pouvez utiliser la nouvelle version d'Amazon Linux.
- Si chown fait partie de votre flux de travail de production, vous devez mettre à jour la version du noyau pour utiliser chown.

Le système de fichiers continue à effectuer des opérations plusieurs fois en raison d'un bogue client

Un système de fichiers est bloqué alors qu'il est en train d'effectuer des opérations répétées en raison d'un bogue client.

Action à exécuter

Mettez à jour le logiciel client vers la dernière version.

Client bloqué

Un client est bloqué.

Versions de noyau avec ce bogue

- CentOS-7 avec le noyau Linux 3.10.0-229.20.1.el7.x86_64
- Ubuntu 15.10 avec le noyau Linux 4.2.0-18-generic

Action à exécuter

Effectuez l'une des actions suivantes :

- Effectuez la mise à niveau vers une nouvelle version du noyau. Pour CentOS-7, la version de noyau Linux 3.10.0-327 ou ultérieure contient le correctif.
- Revenez à une ancienne version de noyau.

L'affichage de la liste de fichiers d'un répertoire volumineux prend beaucoup de temps.

Cela peut se produire si le répertoire change pendant que votre client NFS parcourt le répertoire pour terminer l'opération de liste. Chaque fois que le client NFS remarque que le contenu du répertoire a changé au cours de cette itération, il redémarre l'itération depuis le début. En conséquence, l'exécution de la commande `ls` peut prendre beaucoup de temps pour un répertoire volumineux avec des fichiers modifiés fréquemment.

Versions de noyau avec ce bogue

Versions de noyau CentOS et RHEL inférieures à 2.6.32-696.el6

Action à exécuter

Pour résoudre ce problème, effectuez une mise à niveau vers une version plus récente du noyau.

Sauvegarde et réplication de données dans Amazon EFS

Pour protéger vos données, Amazon EFS sauvegarde automatiquement vos systèmes de fichiers EFS. Pour renforcer la résilience et la protection des données, vous pouvez répliquer votre système de fichiers EFS dans une Région AWS. La sauvegarde et la réplication de vos systèmes de fichiers EFS vous permettent de fournir des opérations ou des services continus en cas de problème avec les données du système de fichiers EFS. Par exemple, en cas de corruption ou de perte de données.

Rubriques

- [Sauvegarde des systèmes de fichiers EFS](#)
- [Réplication de systèmes de fichiers EFS](#)

Sauvegarde des systèmes de fichiers EFS

Amazon EFS est intégré de manière native à AWS Backup un service entièrement géré basé sur des politiques que vous pouvez utiliser pour créer et gérer des politiques de sauvegarde afin de protéger vos données dans Amazon EFS. Les systèmes de fichiers que vous créez à l'aide de la console Amazon EFS sont automatiquement sauvegardés AWS Backup par défaut. Lorsque vous utilisez la CLI ou l'API pour créer un système de fichiers, les sauvegardes automatiques sont activées par défaut uniquement pour les systèmes de fichiers One Zone.

Avec AWS Backup Amazon EFS, vous pouvez effectuer les actions suivantes :

- Gérez la planification et la conservation automatiques des sauvegardes en configurant des plans de sauvegarde. Vous spécifiez la fréquence des sauvegardes, le moment de sauvegarde, la durée de conservation des sauvegardes et une politique de cycle de vie pour les sauvegardes.
- Restaurez les sauvegardes des données Amazon EFS. Vous pouvez restaurer les données du système de fichiers sur un nouveau système de fichiers ou sur un système de fichiers existant. Vous pouvez également choisir d'effectuer une restauration complète ou une restauration au niveau de l'élément.

Pour plus d'informations sur l'utilisation AWS Backup, voir [Getting started with AWS Backup](#) dans le Guide du AWS Backup développeur.

Rubriques

- [Comment AWS Backup fonctionne avec Amazon EFS](#)

- [Autorisations IAM requises](#)
- [Performances de sauvegarde](#)
- [Gestion des sauvegardes automatiques des systèmes de fichiers EFS](#)

Comment AWS Backup fonctionne avec Amazon EFS

Les systèmes de fichiers que vous créez à l'aide de la console Amazon EFS sont automatiquement sauvegardés AWS Backup par défaut. Lorsque vous utilisez la CLI ou l'API pour créer un système de fichiers, les sauvegardes automatiques sont activées par défaut uniquement pour les systèmes de fichiers One Zone. Vous pouvez activer les sauvegardes automatiques après avoir créé votre système de fichiers EFS à l'aide de l'API AWS CLI or. Le plan de sauvegarde EFS par défaut utilise les paramètres AWS Backup recommandés pour les sauvegardes automatiques, à savoir des sauvegardes quotidiennes avec une période de conservation de 35 jours. Les sauvegardes créées à l'aide du plan de sauvegarde EFS par défaut sont stockées dans un coffre de sauvegarde EFS par défaut, également créé par Amazon EFS en votre nom. Le plan de sauvegarde par défaut et le coffre-fort de sauvegarde ne peuvent pas être supprimés.

Toutes les données d'un système de fichiers EFS sont sauvegardées, quelle que soit leur classe de stockage. Aucun frais d'accès aux données ne vous est facturé lorsque vous sauvegardez un système de fichiers EFS pour lequel la gestion du cycle de vie est activée et qui possède des données dans la classe de stockage Infrequent Access (IA) ou d'archive. Lorsque vous restaurez un point de récupération, tous les fichiers sont restaurés dans la classe de stockage standard.

Sauvegardes incrémentielles

AWS Backup effectue des sauvegardes incrémentielles des systèmes de fichiers EFS. Pendant la sauvegarde initiale, une copie de l'ensemble du système de fichiers est effectuée. Pendant les sauvegardes suivantes de ce système de fichiers, seuls les fichiers et les répertoires qui ont été modifiés, ajoutés ou supprimés sont copiés. À chaque sauvegarde incrémentielle, AWS Backup conserve les données de référence nécessaires pour permettre une restauration complète. Cette approche réduit le temps nécessaire pour terminer la sauvegarde, ainsi que les coûts de stockage en ne dupliquant pas les données.

Cohérence de sauvegarde

Amazon EFS est conçu pour être hautement disponible. Vous pouvez accéder à vos systèmes de fichiers EFS et les modifier pendant que votre sauvegarde est en cours dans AWS Backup. Toutefois, des incohérences, telles que des données dupliquées, asymétriques ou exclues, peuvent se produire

si vous apportez des modifications à votre système de fichiers pendant que la sauvegarde est en cours. Ces modifications incluent des opérations d'écriture, de renommage, de déplacement ou de suppression. Pour garantir des sauvegardes cohérentes, nous vous recommandons de suspendre les application ou processus qui modifient le système de fichiers pour la durée du processus de sauvegarde. Vous pouvez également planifier la sauvegarde pour qu'elle ait lieu pendant les périodes où le système de fichiers n'est pas modifié.

Fenêtres de fin de sauvegarde

Vous pouvez éventuellement spécifier une fenêtre de fin pour une sauvegarde. Cette fenêtre définit la période de temps au cours de laquelle une sauvegarde doit se terminer. Si vous spécifiez une fenêtre de fin, assurez-vous de prendre en compte les performances attendues ainsi que la taille et la composition de votre système de fichiers. Cela vous permet de vous assurer que votre sauvegarde peut se terminer pendant la fenêtre.

Les sauvegardes qui ne sont pas terminées au cours de la fenêtre spécifiée sont signalées avec un statut incomplet. Lors de la prochaine sauvegarde planifiée, elle AWS Backup reprend là où elle s'est arrêtée. Vous pouvez consulter l'état de toutes vos sauvegardes sur la console AWS Backup de gestion.

Sauvegardes à la demande

Avec AWS Backup, vous pouvez enregistrer une seule ressource dans un coffre-fort de sauvegarde à la demande. Contrairement aux sauvegardes planifiées, vous n'avez pas besoin de créer un plan de sauvegarde pour lancer une sauvegarde à la demande. Vous pouvez toujours attribuer un cycle de vie à votre sauvegarde, ce qui déplace automatiquement le point de récupération vers le niveau de stockage à froid et note quand le supprimer.

En outre, les données sont AWS Backup automatiquement transférées vers le stockage à froid uniquement pour les données qui n'existent plus dans la sauvegarde à chaud la plus récente. Par exemple, votre système de fichiers contient 100 fichiers lorsque vous créez une sauvegarde et vous supprimez deux fichiers le lendemain de la création de la sauvegarde ($100 \text{ fichiers} - 2 \text{ fichiers} = 98 \text{ fichiers}$ le deuxième jour). Lorsque vous transférez les données vers le stockage à froid, seuls les deux fichiers supprimés sont transférés vers le stockage à froid et les 98 fichiers restants sont facturés comme stockage à chaud.

Sauvegardes simultanées

AWS Backup limite les sauvegardes à une sauvegarde simultanée par ressource. Par conséquent, les sauvegardes planifiées ou à la demande pourraient échouer si une tâche de sauvegarde est déjà

en cours. Pour plus d'informations sur AWS Backup les limites, consultez la section sur [AWS Backup les quotas](#) dans le guide du AWS Backup développeur.

Suppressions de sauvegarde

La politique d'accès au coffre-fort de sauvegarde EFS par défaut est définie pour refuser la suppression de points de restauration. Pour supprimer les sauvegardes existantes de vos systèmes de fichiers EFS, vous devez modifier la politique d'accès au coffre-fort. Si vous tentez de supprimer un point de récupération EFS sans modifier la politique d'accès au coffre-fort, le message d'erreur suivant s'affiche :

```
"Access Denied: Insufficient privileges to perform this action. Please consult with the account administrator for necessary permissions."
```

Pour modifier la politique d'accès au coffre-fort de sauvegarde par défaut, vous devez disposer des autorisations pour modifier les politiques. Pour plus d'informations, consultez [Autoriser toutes les actions IAM \(accès administrateur\)](#) dans le Guide de l'utilisateur IAM.

Autorisations IAM requises

AWS Backup crée un rôle lié à un service en votre nom dans votre compte. Ce rôle a les autorisations requises pour réaliser des sauvegardes Amazon EFS.

Vous pouvez utiliser les actions `elasticfilesystem:backup` et `elasticfilesystem:restore` pour autoriser ou refuser à une entité IAM (comme un utilisateur, un groupe ou un rôle) la capacité de créer ou de restaurer des sauvegardes d'un système de fichiers EFS. Vous pouvez utiliser ces actions dans le cadre d'une stratégie de système de fichiers ou dans une stratégie IAM basée sur l'identité. Pour plus d'informations, consultez [Gestion des identités et des accès pour Amazon EFS](#) et [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#).

Performances de sauvegarde

En général, vous pouvez vous attendre aux taux de sauvegarde et de restauration suivants avec AWS Backup. Les taux peuvent être inférieurs pour certaines charges de travail, telles que celles contenant un fichier ou un répertoire volumineux.

- Taux de sauvegarde de 2 000 fichiers par seconde ou de 400 mégaoctets par seconde (MBps), la valeur la plus lente étant retenue.

- Taux de restauration de 1 500 fichiers par seconde ou 200 MBps, selon le taux le plus lent.

La durée maximale d'une opération de sauvegarde AWS Backup est de 30 jours.

L'utilisation AWS Backup ne consomme pas les crédits de rafale accumulés et n'est pas prise en compte dans les limites de fonctionnement des fichiers en mode performance à usage général. Pour de plus amples informations, veuillez consulter [Quotas pour les systèmes de fichiers Amazon EFS](#).

Gestion des sauvegardes automatiques des systèmes de fichiers EFS

Lorsque vous créez un système de fichiers avec la console Amazon EFS, les sauvegardes automatiques sont activées par défaut. Vous pouvez activer les sauvegardes automatiques après avoir créé votre système de fichiers à l'aide de l'API AWS CLI or.

Vous pouvez modifier les paramètres du plan de sauvegarde par défaut à l'aide de la AWS Backup console. Pour plus d'informations, consultez [la section Gestion des plans de sauvegarde](#) dans le Guide du AWS Backup développeur. Vous pouvez consulter toutes vos sauvegardes automatiques et modifier les paramètres du plan de sauvegarde EFS par défaut à l'aide de la [console AWS Backup](#).

Amazon EFS applique la clé d'identification système `aws:elasticfilesystem:default-backup` avec la valeur `enabled` aux systèmes de fichiers EFS lorsque les sauvegardes automatiques sont activées.

Après avoir créé un système de fichiers, vous pouvez activer ou désactiver les sauvegardes automatiques à l'aide de la console, de l' AWS CLI API EFS ou de l'API EFS.

Utilisation de la console

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Sur la page Systèmes de fichiers, choisissez le système de fichiers pour lequel vous souhaitez activer ou désactiver les sauvegardes automatiques et affichez la page des Détails du système de fichiers.
3. Choisissez Modifier dans le panneau des paramètres Général.
4.
 - Pour activer les sauvegardes automatiques, sélectionnez Activer les sauvegardes automatiques.
 - Pour désactiver les sauvegardes automatiques, sélectionnez Activer les sauvegardes automatiques.
5. Sélectionnez Enregistrer les modifications.

À l'aide du AWS CLI

- Utilisez la commande d'interface de ligne de commande `put-backup-policy` (l'opération d'API correspondante est [PutBackupPolicy](#)) pour activer ou désactiver les sauvegardes automatiques pour un système de fichiers existant.

- Utilisez la commande suivante pour activer les sauvegardes automatiques.

```
$ aws efs put-backup-policy --file-system-id fs-01234567 \  
--backup-policy Status="ENABLED"
```

Amazon EFS répond avec la nouvelle politique de sauvegarde.

```
{  
  "BackupPolicy": {  
    "Status": "ENABLING"  
  }  
}
```

- Utilisez la commande suivante pour désactiver les sauvegardes automatiques.

```
$ aws efs put-backup-policy --file-system-id fs-01234567 \  
--backup-policy Status="DISABLED"
```

Amazon EFS répond avec la nouvelle politique de sauvegarde.

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

Réplication de systèmes de fichiers EFS

Pour une résilience et une protection des données accrues, vous pouvez répliquer votre système de fichiers EFS dans un Région AWS. Lorsque vous activez la réplication sur un système de fichiers EFS, Amazon EFS réplique automatiquement et de manière transparente les données et les métadonnées du système de fichiers source vers un système de fichiers de destination. En cas de sinistre ou lorsque vous effectuez des exercices le jour du match, vous pouvez basculer vers

vosre système de fichiers de réplique. Pour reprendre les opérations, vous pouvez ensuite revenir au système de fichiers principal.

Pour gérer le processus de création du système de fichiers de destination et le synchroniser avec le système de fichiers source, Amazon EFS utilise une configuration de réplique.

Après avoir créé la configuration de réplique, Amazon EFS synchronise automatiquement les systèmes de fichiers source et de destination. Les modifications apportées au système de fichiers source ne sont pas transférées de manière point-in-time cohérente vers le système de fichiers de destination. Ils sont plutôt transférés en fonction de l'heure de dernière synchronisation pour la réplique. L'Heure de la dernière synchronisation indique la date à laquelle la dernière synchronisation réussie entre la source et la destination s'est terminée. Les modifications apportées à votre système de fichiers source lors de la dernière synchronisation sont répliquées sur le système de fichiers de destination, tandis que les Modifications apportées au système de fichiers source après la dernière synchronisation risquent de ne pas être répliquées. Pour de plus amples informations, veuillez consulter [Affichage des détails de réplique](#).

La réplique est disponible Régions AWS dans tous les pays où Amazon EFS est disponible. Pour répliquer un système de fichiers EFS dans une région désactivée par défaut, vous devez d'abord vous connecter à la région. Pour plus d'informations, voir [Spécifier les comptes que Régions AWS votre compte peut utiliser](#) dans le Guide de référence AWS général. Si vous vous désabonnez ultérieurement d'une région, Amazon EFS suspend toutes les activités de réplique pour cette région. Pour reprendre les activités de réplique pour la région, Région AWS réinscrivez-vous.

Note

La réplique EFS ne prend pas en charge l'utilisation de balises pour le Contrôle d'accès par attributs (ABAC).

Rubriques

- [Coûts](#)
- [Performance de réplique](#)
- [Autorisations IAM requises](#)
- [Configuration de la réplique vers le nouveau système de fichiers EFS](#)
- [Configuration de la réplique vers un système de fichiers EFS existant](#)
- [Réplique des systèmes de fichiers EFS sur plusieurs comptes AWS](#)

- [Affichage des détails de réplication](#)
- [Supprimer des configuration de réplication](#)
- [Utilisation de la réplique](#)

Coûts

Pour faciliter la réplication, Amazon EFS crée des répertoires et des métadonnées cachés sur le système de fichiers de destination. Cela équivaut à environ 12 mégaoctets (MiB) de données mesurées pour lesquelles vous êtes facturé. Pour plus d'informations sur le calcul de la capacité de stockage du système de fichiers, consultez [Comment Amazon EFS indique les tailles des systèmes de fichiers et des objets](#).

Performance de réplication

Lorsque vous créez de nouvelles réplications ou que vous inversez le sens des réplications existantes pendant le processus failback, Amazon EFS effectue une synchronisation initiale, qui inclut une série d'actions de configuration uniques pour prendre en charge la réplication. Le temps nécessaire à la synchronisation initiale dépend de facteurs tels que la taille du système de fichiers source et le nombre de fichiers qu'il contient.

Une fois la réplication initiale terminée, Amazon EFS maintient un Objectif de point de reprise (RPO) de 15 minutes pour la plupart des systèmes de fichiers. Toutefois, si le système de fichiers source contient des fichiers qui changent très fréquemment et compte plus de 100 millions de fichiers ou des fichiers de plus de 100 Go, la réplication peut prendre plus de 15 minutes. Pour plus d'informations sur la surveillance de la fin réussie de la dernière réplication, consultez [Affichage des détails de réplication](#).

Vous pouvez surveiller la date de la dernière synchronisation réussie à l'aide de la console, du AWS Command Line Interface (AWS CLI), de l'API et d'Amazon CloudWatch. Dans CloudWatch, utilisez la métrique [TimeSinceLastSyncEFS](#). Pour de plus amples informations, veuillez consulter [Affichage des détails de réplication](#).

Autorisations IAM requises

Amazon EFS utilise le rôle lié au service EFS nommé `AWSServiceRoleForAmazonElasticFileSystem` ou le rôle IAM que vous spécifiez pour synchroniser la réplication entre les systèmes de fichiers source et de destination. Pour fournir un rôle IAM, l'utilisateur ou le rôle IAM qui crée la configuration de réplication doit disposer `iam:PassRole`

d'une autorisation. Pour plus d'informations, voir [Accorder à un utilisateur l'autorisation de transmettre un rôle à un AWS service](#) dans le Guide de AWS Identity and Access Management l'utilisateur.

- Pour plus d'informations sur `iam:CreateServiceLinkedRole`, consultez l'exemple dans [Utilisation des rôles liés à un service pour Amazon EFS](#).
- Pour plus d'informations sur un rôle IAM personnalisé, consultez [Création d'un rôle IAM avec une politique de confiance personnalisée](#).

Note

Si vous effectuez une réplication entre comptes, vous devez fournir un rôle IAM lorsque vous créez la configuration de réplication. L'utilisation du rôle lié au service n'est pas autorisée. Pour de plus amples informations, veuillez consulter [Réplication des systèmes de fichiers EFS sur plusieurs comptes AWS](#).

Le rôle lié au service ou le rôle IAM que vous fournissez lors de la création de la configuration de réplication doit disposer des autorisations suivantes pour la réplication.

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

Vous pouvez utiliser la politique `AmazonElasticFileSystemFullAccess` gérée pour obtenir automatiquement toutes les autorisations EFS requises. Pour de plus amples informations, veuillez consulter [AWS politique gérée : AmazonElasticFileSystemFullAccess](#).

Configuration de la réplication vers le nouveau système de fichiers EFS

Amazon EFS crée automatiquement un nouveau système de fichiers et copie les données et les métadonnées du système de fichiers source vers un nouveau système de fichiers de destination en lecture seule dans la Région AWS système de fichiers de votre choix. Lorsque vous répliquez vers un nouveau système de fichiers, vous choisissez le type de système de fichiers et la clé AWS Key Management Service (AWS KMS) à utiliser pour le chiffrement. En outre, Amazon EFS ne crée

aucune cible de montage lors de la création du système de fichiers de destination. Après avoir créé la configuration de réplication, vous devez [créer une ou plusieurs cibles de montage](#) pour [monter un système de fichiers de destination](#).

 Note

Un système de fichiers ne peut faire partie que d'une seule configuration de réplication. Vous ne pouvez pas utiliser un système de fichiers de destination comme système de fichiers source dans une autre configuration de réplication.

- Le type de système de fichiers détermine la disponibilité et la durabilité nécessaire pour qu'un système de fichiers Amazon EFS stocke les données dans un Région AWS.
- Choisissez Régional pour créer un système de fichiers qui stocke les données et les métadonnées de manière redondante dans toutes les Zones de disponibilité d'une Région AWS.
- Choisissez Zone unique pour créer un système de fichiers qui stocke les données et les métadonnées de manière redondante dans une seule Zone de disponibilité.

Pour plus d'informations sur les types de systèmes de fichiers, consultez [Types de système de fichiers EFS](#).

- Chiffrement : tous les systèmes de fichiers de destination sont créés avec le chiffrement au repos activé. Vous pouvez spécifier la AWS KMS clé utilisée pour chiffrer le système de fichiers de destination. Si vous ne spécifiez pas de clé KMS, c'est votre clé KMS gérée par le service pour Amazon EFS qui sera utilisée.

 Important

Une fois le système de fichiers de destination créé, vous ne pouvez pas Modifier la clé KMS.

Le système de fichiers de destination est créé avec des paramètres par défaut basés sur votre système de fichiers source. Des paramètres supplémentaires peuvent être modifiés après la création.

- Sauvegardes automatiques : pour les systèmes de fichiers de destination utilisant le stockage Zone unique, les sauvegardes automatiques sont activées par défaut. Une fois le système de fichiers créé, vous pouvez Modifier le paramètre de sauvegarde automatique. Pour de plus amples

informations, veuillez consulter [Gestion des sauvegardes automatiques des systèmes de fichiers EFS](#).

- **Mode performance** : le mode de performance du système de fichiers de destination correspond à celui du système de fichiers source, sauf si le système de fichiers de destination utilise le stockage One Zone. Dans ce cas, le mode General Purpose est utilisé. Le mode Performance ne peut pas être modifié.
- **Mode débit** : le mode de débit du système de fichiers de destination correspond à celui du système de fichiers source. Une fois le système de fichiers créé, vous pouvez modifier le mode.

Si le mode de débit du système de fichiers source est Provisionné, le débit provisionné du système de fichiers de destination correspond à celui du système de fichiers source, sauf si le montant provisionné du fichier source dépasse la limite de la région du système de fichiers de destination. Si la quantité allouée au système de fichiers source dépasse la limite de région pour le système de fichiers de destination, le débit alloué du système de fichiers de destination est la limite de région. Pour de plus amples informations, veuillez consulter [Les quotas Amazon EFS que vous pouvez augmenter](#).

- **Gestion du cycle de vie** : la gestion du cycle de vie n'est pas activée sur le système de fichiers de destination. Une fois le système de fichiers de destination créé, vous pouvez l'activer. Pour de plus amples informations, veuillez consulter [Gestion du cycle de vie du stockage](#).

Étape 1 : Création de la configuration de réplication

La première étape de la réplication vers un nouveau système de fichiers consiste à créer la configuration de réplication.

Utilisation de la console

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/efs/>.
2. Ouvrez le système de fichiers que vous souhaitez répliquer :
 - a. Dans le volet de navigation de gauche, choisissez **Systèmes de fichiers**.
 - b. Dans la liste des systèmes de fichiers, choisissez le système de fichiers que vous souhaitez répliquer. Le système de fichiers que vous choisissez ne peut pas être un système de fichiers source ou de destination dans une configuration de réplication existante.
3. Choisissez l'onglet **Réplication**.

4. Dans la section Réplication, choisissez Créer une réplication.
5. Dans la section Paramètres de réplication, définissez les paramètres de réplication :
 - a. Pour la configuration de la réplication, choisissez de répliquer vers un nouveau système de fichiers ou vers un système de fichiers existant.
 - b. Dans Destination Région AWS, choisissez le système de fichiers Région AWS dans lequel vous souhaitez répliquer le système de fichiers.
6. Dans la section Paramètres du système de fichiers de destination, définissez les paramètres du système de fichiers de destination.
 - a. Pour Type de système de fichiers, choisissez une option de stockage pour le système de fichiers :
 - Pour créer un système de fichiers qui stocke les données de manière redondante dans plusieurs zones de disponibilité géographiquement séparées au sein d'un Région AWS, choisissez Régional.
 - Pour créer un système de fichiers qui stocke les données de manière redondante dans une seule zone de disponibilité Région AWS, choisissez One Zone, puis sélectionnez la zone de disponibilité.

Pour de plus amples informations, veuillez consulter [Types de système de fichiers EFS](#).

 Note

Les classes de stockage Zone unique ne sont pas disponibles dans toutes les Zones de disponibilité dans le Régions AWS où Amazon EFS est disponible.

- b. Pour Chiffrement, le chiffrement des données au repos est automatiquement activé sur le système de fichiers de destination. Par défaut, Amazon EFS utilise votre AWS Key Management Service clé de service (aws/elasticfilesystem) ().AWS KMS Pour utiliser une autre clé KMS, choisissez la clé KMS ou entrez le nom de ressource Amazon (ARN) de la clé.

 Important

Vous ne pouvez pas Modifier ces propriétés après la création de la clé KMS.

Créez la configuration de réplication (AWS CLI)

Cette section fournit des exemples de création d'une configuration de réplication à l' AWS CLI aide de la `create-replication-configuration` commande. La commande API équivalente est [CreateReplicationConfiguration](#).

Exemple : Création d'une configuration de réplication pour un système de fichiers de destination régional

L'exemple suivant crée une configuration de réplication pour le système de fichiers `fs-0123456789abcdef1`. L'exemple utilise le `Region` paramètre pour créer un système de fichiers de destination dans le `eu-west-2` Région AWS. Le `KmsKeyId` paramètre indique l'ID de clé KMS à utiliser lors du chiffrement du système de fichiers de destination :

```
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\"}]"
```

Les AWS CLI réponses sont les suivantes :

```
{
  "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"
}
```

Exemple : Création d'une configuration de réplication pour un système de fichiers de Zone unique

L'exemple suivant crée une configuration de réplication pour le système de fichiers

fs-0123456789abcdef1. L'exemple utilise le `AvailabilityZoneName` paramètre pour créer un système de fichiers de destination One Zone dans la zone de *us-west-2a* disponibilité. Aucune clé KMS n'étant spécifiée, le système de fichiers de destination est chiffré à l'aide de la clé de AWS KMS service par défaut du compte (`aws/elasticfilesystem`).

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

Étape 2 : monter le système de fichiers de destination

Amazon EFS ne crée aucune cible de Montage lors de la création du système de fichiers de destination. Pour monter le système de fichiers de destination, vous devez créer une ou plusieurs cibles de montage. Pour de plus amples informations, veuillez consulter [Montage des systèmes de fichiers EFS](#).

Configuration de la réplication vers un système de fichiers EFS existant

Amazon EFS réplique les données et les métadonnées du système de fichiers source vers le système de fichiers de destination Région AWS que vous choisissez. Au cours de la réplication, Amazon EFS identifie les différences de données entre les systèmes de fichiers et applique ces différences au système de fichiers de destination.

Pour effectuer une réplication sur un système de fichiers existant, effectuez les opérations suivantes.

Rubriques

- [Étape 1 : désactiver la protection contre le remplacement de la réplication du système de fichiers](#)
- [Étape 2 : Création de la configuration de réplication](#)

Note

Un système de fichiers ne peut faire partie que d'une seule configuration de réplication. Vous ne pouvez pas utiliser un système de fichiers de destination comme système de fichiers source dans une autre configuration de réplication.

Étape 1 : désactiver la protection contre le remplacement de la réplication du système de fichiers

Lorsque vous créez un système de fichiers Amazon EFS, sa protection contre le remplacement de la réplication est activée par défaut. La protection contre le remplacement de la réplication empêche le système de fichiers d'être utilisé comme destination dans une configuration de réplication. Avant de pouvoir utiliser le système de fichiers comme destination dans une configuration de réplication, vous devez désactiver la protection. Si vous supprimez la configuration de réplication, la protection contre le remplacement par réplication du système de fichiers est réactivée et le système de fichiers devient inscriptible.

L'état de la protection contre l'écrasement par réplication pour un système de fichiers Amazon EFS peut avoir l'une des valeurs décrites dans le tableau suivant.

État du système de fichiers	Description
ENABLED	Le système de fichiers ne peut pas être utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est inscriptible. La protection contre le remplacement de la réplication est ENABLED par défaut.
DISABLED	Le système de fichiers ne peut pas être utilisé comme système de fichiers de destination dans une configuration de réplication.
Réplication	Le système de fichiers est utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est en lecture seule et n'est Modifié que par Amazon EFS lors de la réplication.

Autorisation obligatoire

La désactivation de la protection contre le remplacement de la réplication nécessite des autorisations pour cette action `elasticfilesystem:UpdateFileSystemProtection`. Pour de plus amples informations, veuillez consulter [AWS politique gérée : AmazonElasticFileSystemFullAccess](#).

Utilisation de la console

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/efs/>.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers.
3. Dans la liste des Systèmes de fichiers, choisissez le système de fichiers Amazon EFS que vous souhaitez utiliser comme système de fichiers de destination dans une configuration de réplication.
4. Dans la section Protection du système de fichiers, désactivez la Protection contre le remplacement de la réplication.

Pour désactiver la protection contre le remplacement de la réplication (AWS CLI)

Dans l'exemple suivant, la commande `update-file-system-protection` CLI désactive la protection contre le remplacement de la réplication pour le système de fichiers spécifié. La commande API équivalente est [UpdateFileSystemProtection](#).

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

Les AWS CLI réponses sont les suivantes.

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

Étape 2 : Création de la configuration de réplication

Après avoir désactivé la protection contre le remplacement de la réplication sur le système de fichiers de destination, vous pouvez créer la configuration de réplication. Lors de la réplication vers un système de fichiers existant, le système de fichiers de destination peut se trouver dans le même compte ou dans un compte différent de celui du système de fichiers source.

Si le système de fichiers source est chiffré, le système de fichiers de destination doit l'être également. En outre, si le fichier source n'est pas chiffré et que le système de fichiers de destination l'est, vous ne pouvez pas revenir à la destination source après avoir effectué le basculement. iPour de plus

amples informations sur le chiffrement, veuillez consulter [Chiffrement des données dans Amazon EFS](#).

 Note

Lorsque vous configurez initialement la réplication vers un système de fichiers existant, Amazon EFS écrit des données dans le système de fichiers de destination ou en supprime des données existantes afin qu'elles correspondent aux données du système de fichiers source. Si vous ne souhaitez pas modifier les données du système de fichiers de destination, vous devez plutôt les répliquer vers un nouveau système de fichiers. Pour de plus amples informations, veuillez consulter [Configuration de la réplication vers le nouveau système de fichiers EFS](#).

Prérequis

Disposez d'une copie de l'ID du système de fichiers de destination (pour la réplication sur le même compte) ou de l'ARN du système de fichiers de destination (pour la réplication entre comptes) que vous souhaitez utiliser.

Si le système de fichiers de destination se trouve dans un système de fichiers Compte AWS différent du système de fichiers source, créez un rôle IAM qui permet à Amazon EFS d'effectuer la réplication et d'attribuer des politiques de ressources aux systèmes de fichiers. Pour de plus amples informations, veuillez consulter [Réplication des systèmes de fichiers EFS sur plusieurs comptes AWS](#).

Utilisation de la console

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/efs/>.
2. Ouvrez le système de fichiers que vous souhaitez répliquer :
 - a. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers.
 - b. Dans la liste des systèmes de fichiers, choisissez le système de fichiers Amazon EFS que vous souhaitez répliquer. Le système de fichiers que vous choisissez ne peut pas être un système de fichiers source ou de destination dans une configuration de réplication existante.
3. Choisissez l'onglet Réplication.
4. Dans la section Réplication, choisissez Créer une réplication.

5. Pour la configuration de la réplication, choisissez le système de fichiers existant.
 6. Choisissez le système de fichiers de destination.
 - Pour effectuer une réplication vers un système de fichiers identique au système de fichiers source Compte AWS , procédez comme suit :
 1. Sélectionnez Choisir un système de fichiers dans ce compte et, dans Destination Région AWS, sélectionnez le système de fichiers Région AWS vers lequel vous souhaitez répliquer le système de fichiers.
 2. Choisissez Browse EFS, puis sélectionnez le système de fichiers. Le chemin d'accès au fichier de destination apparaît dans la zone Destination.
 - Pour effectuer une réplication vers un système de fichiers situé dans un autre système Compte AWS que le système de fichiers source, procédez comme suit :
 1. Choisissez Spécifier un système de fichiers dans un autre compte.
 2. Pour l'ARN du système de fichiers de destination, entrez le nom de ressource Amazon (ARN) du système de fichiers de destination.
-  **Note**

Si la protection contre le remplacement de la réplication est activée sur le système de fichiers, un avertissement s'affiche. Choisissez Désactiver la protection pour ouvrir le système de fichiers dans un nouvel onglet et désactiver sa protection contre le remplacement par réplication. Après avoir désactivé la protection, retournez dans l'onglet Créer une réplication et cliquez sur le bouton Actualiser pour effacer le message.
7. Pour le rôle IAM, entrez l'ARN du rôle IAM qui permet à Amazon EFS de se répliquer vers le système de fichiers de destination. Cela est facultatif pour la réplication entre comptes identiques, mais obligatoire pour la réplication entre comptes. Pour de plus amples informations, veuillez consulter [Réplication des systèmes de fichiers EFS sur plusieurs comptes AWS](#).
 8. Choisissez Créer une réplication, tapez confirmer dans le champ de saisie du message de confirmation, puis choisissez Créer une réplication. La section Réplication présente les détails de la réplication.

Pour créer la configuration de réplication (AWS CLI)

Cette section fournit des exemples de création d'une configuration de réplication à l' AWS CLI aide de la `create-replication-configuration` commande. La commande API équivalente est [CreateReplicationConfiguration](#).

Exemple : créer une configuration de réplication vers un système de fichiers de destination existant dans une autre région

L'exemple suivant crée une configuration de réplication dans laquelle l'ID du système de fichiers `fs-0123456789abcdef1` est répliqué sur l'ID du système de fichiers `fs-0a8b2be428114d97c` dans le `eu-west-2` Région AWS.

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

Les AWS CLI réponses sont les suivantes :

```
{
  "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"
}
```

Exemple : créer une configuration de réplication entre comptes

L'exemple suivant crée une configuration de réplication dans laquelle les systèmes de fichiers source et de destination sont différents Comptes AWS. L'ID du système de fichiers source

fs-0123456789abcdef1 dans le compte *555666777888* est répliqué sur l'ID du système de fichiers *fs-0a8b2be428114d97c* dans le compte *123456789012*. L'exemple indique le nom de ressource Amazon (ARN) du système de fichiers de destination et l'ARN du rôle IAM dans le compte source qui permet à Amazon EFS d'effectuer la réplication en son nom. Aucune clé KMS n'étant spécifiée, le système de fichiers de destination est chiffré à l'aide de la clé de AWS KMS service par défaut du compte (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
```

Les AWS CLI réponses sont les suivantes :

```
{
  "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"
}
```

Réplication des systèmes de fichiers EFS sur plusieurs comptes AWS

Vous pouvez répliquer les systèmes de fichiers EFS entre eux. Comptes AWS La réplication entre comptes améliore la résilience et la fiabilité globales de vos stratégies de reprise après sinistre (DR) et peut vous aider à respecter les obligations de conformité de l'entreprise.

Par exemple, les politiques de conformité peuvent vous obliger à utiliser différents comptes pour différents environnements (tels que la production, la préparation et la reprise après sinistre (DR)). Vous pouvez également constater que la réplication entre différents systèmes renforce l'isolation, Comptes AWS permet un contrôle plus précis des autorisations et des politiques d'accès et simplifie l'audit des ressources. Si le compte de production est compromis (par exemple en raison de failles de sécurité, d'une mauvaise configuration ou de menaces internes), le fait de placer les serveurs DR dans un compte distinct peut empêcher l'attaquant d'y accéder, réduire la portée des incidents de sécurité et minimiser le risque de modifications non autorisées.

La réplication interdisciplinaire Comptes AWS nécessite une sécurité et une configuration de politiques supplémentaires. Au lieu d'utiliser des rôles liés à un service pour effectuer une réplication entre comptes, vous devez créer un rôle IAM qui autorise Amazon EFS à effectuer la réplication dans le compte de destination. Vous devez également créer des politiques sur les systèmes de fichiers que vous souhaitez partager entre les comptes. Une fois le rôle IAM et les politiques du système de fichiers créés, vous créez la configuration de réplication.

Rubriques

- [Création d'un rôle IAM avec une politique de confiance personnalisée](#)
- [Créez des politiques sur les systèmes de fichiers source et de destination](#)
- [Création de la configuration de réplication](#)

Création d'un rôle IAM avec une politique de confiance personnalisée

Pour qu'Amazon EFS puisse effectuer une réplication entre comptes au nom du compte source, un rôle IAM doit être créé sur le compte source. Le rôle doit disposer d'une politique de `elasticfilesystem.amazonaws.com` confiance permettant à Amazon EFS d'assumer le rôle et d'agir en tant que principal du service. Le rôle doit contenir toutes les autorisations IAM requises pour effectuer la réplication (voir [Autorisations IAM requises](#)) et accorder l'autorisation explicite de répliquer vers le système de fichiers du compte de destination.

Prérequis

Vous devez créer à la fois le système de fichiers source et le système de fichiers de destination dans la configuration de réplication avant de pouvoir créer le rôle IAM pour le compte source. Amazon EFS ne peut pas créer le système de fichiers de destination pour vous pendant la réplication. En outre, vous devez connaître et fournir le nom de ressource Amazon (ARN) pour chaque système de fichiers.

Pour créer le rôle IAM pour la réplication entre comptes

Voici les étapes générales de création d'un rôle IAM avec des politiques de confiance personnalisées pour la réplication entre comptes avec Amazon EFS. Pour step-by-step obtenir des instructions sur la création d'un rôle IAM, voir [Création d'un rôle à l'aide de politiques de confiance personnalisées](#) dans le Guide de l'AWS Identity and Access Management utilisateur.

1. Dans la AWS Identity and Access Management console du compte source, créez un rôle IAM qui utilise la politique de confiance suivante. Pour obtenir des instructions, consultez la section [Créer un rôle à l'aide de politiques de confiance personnalisées](#) dans le guide de l'utilisateur d'AWS Identity and Access Management.

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

2. Après avoir créé le rôle, attribuez-lui les autorisations suivantes. Remplacez DESTINATION_FILE_SYSTEM_ARN par l'ARN du système de fichiers de destination et remplacez SOURCE_FILE_SYSTEM_ARN par l'ARN du système de fichiers source. Pour obtenir des instructions sur l'attribution d'autorisations au rôle, consultez la section [Création de politiques à l'aide de l'éditeur 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. Copiez ou notez l'ARN du rôle IAM. Vous devez fournir l'ARN lorsque vous créez la configuration de réplication.

Créez des politiques sur les systèmes de fichiers source et de destination

Pour partager des systèmes de fichiers entre comptes dans Amazon EFS, vous devez attribuer des politiques aux systèmes de fichiers source et de destination. Les politiques accordent ou limitent l'accès entre les comptes au système de fichiers auquel elles sont appliquées. Seuls les propriétaires de comptes autorisés à modifier les systèmes de fichiers peuvent attribuer des politiques au système de fichiers de leur compte.

Important

En plus d'accorder ou de restreindre l'accès entre les comptes, les politiques doivent accorder d'autres autorisations requises pour que les clients puissent utiliser les systèmes de fichiers, telles que `elasticfilesystem:ClientMount`. Dans le cas contraire, le système de fichiers risque d'être inaccessible aux clients. Pour obtenir des exemples de stratégies, consultez la section [Exemples de politiques basées sur les ressources pour Amazon EFS](#).

Politique pour le système de fichiers de destination

Pour autoriser le compte source à effectuer une réplication sur le système de fichiers de destination et à supprimer la configuration de réplication du compte de destination, la politique suivante doit être créée sur le système de fichiers de destination. Remplacez `SOURCE_ACCOUNT_ROOT` par l'ID du compte propriétaire du système de fichiers source.

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

Politique pour le système de fichiers source

Pour autoriser le compte de destination à supprimer la configuration de réplication du compte source, vous devez attribuer la politique suivante au système de fichiers source. Remplacez `DESTINATION_ACCOUNT_ROOT` par l'ID du compte propriétaire du système de fichiers de destination.

```
{
  "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"
    }
]
```

Pour créer la politique du système de fichiers

Effectuez les étapes suivantes pour le système de fichiers de destination et le système de fichiers source, en utilisant les politiques décrites dans la section précédente.

1. Connectez-vous au AWS Management Console avec le compte propriétaire du système de fichiers, puis ouvrez la console Amazon EFS sur la console [Amazon EFS](#).
2. Ouvrez le système de fichiers :
 - a. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers.
 - b. Dans la liste des systèmes de fichiers, sélectionnez le système de fichiers.
3. Dans l'onglet Stratégie du système de fichiers, choisissez Modifier.
4. Collez la politique dans l'éditeur de politiques {Json}, puis choisissez Enregistrer.

Création de la configuration de réplication

Après avoir créé le rôle IAM et ajouté les politiques du système de fichiers aux systèmes de fichiers source et de destination, suivez les instructions [Configuration de la réplication vers un système de fichiers EFS existant](#) pour créer la configuration de réplication.

Affichage des détails de réplication

Vous pouvez surveiller l'heure à laquelle la dernière synchronisation réussie s'est terminée dans une configuration de réplication. Toutes les Modifications apportées aux données du système de fichiers source avant cette date ont été correctement répliquées sur le système de fichiers de destination. Les Modifications survenues après cette période risquent de ne pas être entièrement répliquées. Pour savoir quand la dernière réplication s'est terminée avec succès, vous pouvez utiliser la console Amazon EFS AWS CLI, l'API ou Amazon CloudWatch.

- Dans la console EFS, la propriété Dernière synchronisation dans la section Détails du système de fichiers > Réplication indique l'heure à laquelle la dernière synchronisation réussie entre la source et la destination s'est terminée.
- Dans l'API AWS CLI or : la LastReplicatedTimestamp propriété de l'Destinationobjet indique l'heure à laquelle la dernière synchronisation réussie s'est terminée. Pour accéder à cette propriété, utilisez la commande describe-replication-configurations CLI. [DescribeReplicationConfigurations](#) est l'opération d'API équivalente.
- Dans CloudWatch — La TimeSinceLastSync CloudWatch métrique d'Amazon EFS indique le temps écoulé depuis la fin de la dernière synchronisation réussie. Pour de plus amples informations, veuillez consulter [CloudWatch métriques pour Amazon EFS](#).

Une configuration de réplication peut avoir l'une des valeurs d'état décrites dans le tableau suivant.

État de réplication	Description
ENABLED	La configuration de réplication est saine et prête à être utilisée.
ENABLING	Amazon EFS est en train de créer la configuration de réplication.
DELETING	Amazon EFS supprime la configuration de réplication en réponse à une demande de suppression initiée par l'utilisateur.
PAUSING	Amazon EFS est en train de suspendre la réplication.
PAUSED	La réplication est suspendue en raison d'un problème de configuration. Des informations supplémentaires sur le problème sont fournies.

Parmi les problèmes à l'origine de l'interruption de la réplication, citons :

- Erreur d'autorisation. Des problèmes d'autorisations empêchent Amazon EFS d'effectuer la réplication. Assurez-vous que le rôle IAM utilisé pour créer la configuration de réplication est autorisé à effectuer la réplication. Assurez-vous également que les politiques du système de fichiers sont correctes.
- AWS le compte n'est pas disponible. Assurez-vous que les comptes source et de destination sont activés de manière appropriée Régions AWS et qu'ils ne sont pas suspendus. Pour plus d'informations, voir [Spécifier les comptes](#)

État de réplication	Description
	que Régions AWS votre compte peut utiliser dans le Guide de référence AWS général. La clé KMS du système de fichiers source ou de destination n'est pas accessible. Assurez-vous que la clé KMS attribuée à chaque système de fichiers est accessible. Pour de plus amples informations, veuillez consulter Gestion des clés KMS pour les systèmes de fichiers EFS.
ERROR	La configuration de réplication est en état d'échec et est irrécupérable. Vous devez supprimer la configuration de réplication et en créer une nouvelle. Des informations supplémentaires sur le problème sont fournies. Pour la réplication entre comptes ou entre régions, l'erreur peut être due au fait que la configuration de réplication a été supprimée de l'autre Compte AWS ou. Région AWS

Utilisation de la console

- Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
- Dans le volet de navigation de gauche, choisissez Systèmes de fichiers.
- Choisissez un système de fichiers dans la liste.
- Choisissez l'onglet Réplication pour afficher la section Réplication.

Dans la section Réplication, vous pouvez consulter les informations suivantes concernant la configuration de réplication :

- L'État de réplication peut être Activation, Activé, Suppression, Suspension, Suspendu ou Erreur. Amazon EFS affiche des informations sur la cause de l'état de pause ou d'erreur.
- Direction de réplication indique la direction dans laquelle les données sont répliquées. Le premier système de fichiers répertorié est la source, et ses données sont répliquées vers le second système de fichiers répertorié, qui est la destination.
- Dernière synchronisation indique la date à laquelle la dernière synchronisation réussie s'est produite sur le système de fichiers de destination. Toutes les Modifications apportées aux données du système de fichiers source avant cette date ont été correctement répliquées sur le

système de fichiers de destination. Les Modifications survenues après cette période risquent de ne pas être entièrement répliquées.

- Les systèmes de fichiers de réplication répertorient chaque système de fichiers de la configuration de réplication en fonction de son ID de système de fichiers, de son rôle Région AWS dans la configuration de réplication (source ou destination), de son emplacement et de son autorisation. Un système de fichiers source possède l'autorisation Accessibles en écriture, tandis qu'un système de fichiers de destination possède l'autorisation Lecture seule.

En utilisant le AWS CLI

Pour afficher une configuration de réplication, utilisez la `describe-replication-configurations` commande. Vous pouvez consulter la configuration de réplication d'un système de fichiers spécifique ou toutes les configurations de réplication d'un système de fichiers spécifique Compte AWS dans un Région AWS. La commande API équivalente est [DescribeReplicationConfigurations](#).

Si l'état de la configuration de réplication est `PAUSED` ou `ERROR`, les informations relatives à la cause du problème et à la manière de le résoudre sont renvoyées dans le `StatusMessage` paramètre.

Exemple : Afficher la configuration de réplication pour un système de fichiers spécifique

L'exemple suivant décrit la configuration de réplication pour le système de fichiers `fs-0123456789abcdef1`.

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

Les AWS CLI réponses sont les suivantes.

```
{
  "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"
      }
    ]
  }
}

```

Exemple : Afficher la configuration de réplication pour toutes les configurations de réplication d'un compte

L'exemple suivant décrit la configuration de réplication pour toutes les configurations de réplication d'un compte dans un système Région AWS de fichiers.

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

Les AWS CLI réponses sont les suivantes.

```

{
  "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
      }
    ]
  }
]
}

```

Supprimer des configuration de réplication

Si vous devez basculer vers le système de fichiers de destination, supprimez la configuration de réplication dont il est membre. Après avoir supprimé une configuration de réplication, le système de fichiers de destination devient inscriptible et sa protection contre le remplacement de la réplication est réactivée. Pour de plus amples informations, veuillez consulter [Utilisation de la réplique](#).

La suppression d'une configuration de réplication et la Modification du système de fichiers de destination pour qu'il soit accessible en écriture peuvent prendre plusieurs minutes. Une fois la configuration supprimée, Amazon EFS peut écrire des données dans un `lost+found` répertoire du répertoire racine du système de fichiers de destination, en utilisant la convention de dénomination suivante :

```
efs-replication-lost+found-source-file-system-id-TIMESTAMP
```

Note

Vous ne pouvez pas supprimer un système de fichiers faisant partie d'une configuration de réplication. Vous devez supprimer la configuration de réplication avant de supprimer le système de fichiers.

Vous pouvez supprimer une configuration de réplication existante du système de fichiers source ou de destination à l'aide de la console Amazon EFS, de l' AWS CLI API ou de l'API.

Pour les réplications entre comptes ou entre régions, Amazon EFS supprime la configuration de réplication des comptes ou régions source et de destination. Si un problème de configuration ou d'autorisation empêche Amazon EFS de supprimer la configuration de réplication des deux côtés, vous pouvez supprimer la configuration uniquement du côté local (le compte ou la région à partir duquel la suppression est effectuée). La suppression de la configuration locale rend la configuration de l'autre compte ou de l'autre région irrécupérable.

Utilisation de la console

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers.
3. Choisissez le système de fichiers source ou de destination figurant dans la configuration de réplication que vous souhaitez supprimer.
4. Choisissez l'onglet Réplication pour afficher la section Réplication.
5. Choisissez Supprimer la réplication pour supprimer la configuration de réplication. Lorsque vous y êtes invité, confirmez votre choix.

Si vous supprimez une configuration de réplication entre comptes et qu'un problème vous empêche de supprimer la configuration à la fois du côté source et du côté destination, vous pouvez choisir de supprimer uniquement la configuration de ce système de fichiers.

Note

Supprimez la configuration du système de fichiers uniquement si Amazon EFS n'est pas en mesure de supprimer la configuration de réplication dans le compte ou la région source et de destination. La suppression de la configuration locale rend la configuration de l'autre compte ou de l'autre région irrécupérable.

En utilisant le AWS CLI

Pour supprimer une configuration de réplication, utilisez la `delete-replication-configuration` CLI. La commande API équivalente est [DeleteReplicationConfiguration](#).

L'exemple suivant supprime la configuration de réplication du système `fs-0123456789abcdef1` de fichiers source.

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

Si un problème de configuration ou d'autorisations empêche Amazon EFS de supprimer la configuration de réplication des deux côtés, vous pouvez supprimer la configuration uniquement du côté local (le compte ou la région à partir duquel la suppression est effectuée). La suppression de la configuration locale rend la configuration de l'autre compte ou de l'autre région irrécupérable. Le paramètre d'API équivalent est `DeletionMode` et la valeur est `LOCAL_CONFIGURATION_ONLY`.

L'exemple suivant supprime la configuration de réplication du système **fs-0123456789abcdef1** de fichiers source uniquement du côté local.

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

Utilisation de la réplique

En cas de sinistre ou lorsque vous effectuez des exercices le jour du match, vous pouvez basculer vers votre système de fichiers de réplique en supprimant sa configuration de réplication. Une fois la configuration de réplication supprimée, la réplique devient inscriptible et vous pouvez commencer à l'utiliser dans le flux de travail de votre application. Lorsque le sinistre est atténué ou que l'exercice du jour de jeu est terminé, vous pouvez continuer à utiliser la réplique comme système de fichiers principal ou effectuer un retour en arrière pour reprendre les opérations sur votre système de fichiers principal d'origine.

Au cours du processus de rétrogradation, vous pouvez choisir de supprimer les Modifications apportées à votre système de fichiers de réplique ou de les conserver en les copiant à nouveau sur votre système de fichiers principal.

- Pour ignorer les Modifications apportées à votre réplique lors du basculement, recréez la configuration de réplication d'origine sur votre système de fichiers principal, où le système de fichiers de réplique est la destination de réplication. Pendant la réplication, Amazon EFS synchronise les systèmes de fichiers en mettant à jour les données de votre système de fichiers répliqué pour qu'elles correspondent à celles de votre système de fichiers principal.
- Pour ignorer les Modifications apportées à votre réplique lors du basculement, recréez la configuration de réplication d'origine sur votre système de fichiers principal, où le système de fichiers de réplique est la destination de réplication. Au cours de la réplication, Amazon EFS

identifie et transfère les différences entre votre système de fichiers de réplique et le renvoie au système de fichiers principal. Une fois la réplication terminée, vous pouvez reprendre la réplication du système de fichiers principal en recréant la configuration de réplication d'origine ou en créant une nouvelle configuration.

Le temps nécessaire à Amazon EFS pour terminer le processus de réplication varie et dépend de facteurs tels que la taille du système de fichiers et le nombre de fichiers qu'il contient. Pour de plus amples informations, veuillez consulter [Performance de réplication](#).

Sécurisation de vos données dans Amazon EFS

Le [modèle de responsabilité AWS partagée](#) s'applique à la protection des données dans Amazon Elastic File System. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez [Questions fréquentes \(FAQ\) sur la confidentialité des données](#). Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog [Modèle de responsabilité partagée AWS et RGPD \(Règlement général sur la protection des données\)](#) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez [Norme FIPS \(Federal Information Processing Standard\) 140-3](#).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que

le champ Nom. Cela inclut lorsque vous travaillez avec EFS ou autre Services AWS à l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Rubriques

- [Chiffrement des données dans Amazon EFS](#)
- [Gestion des identités et des accès pour Amazon EFS](#)
- [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#)
- [Contrôle de l'accès réseau aux systèmes de fichiers EFS pour les clients NFS](#)
- [Utilisateurs, groupes et autorisations au niveau du système de fichiers réseau \(NFS\)](#)
- [Utilisation des points d'accès](#)
- [Blocage de l'accès public aux systèmes de fichiers EFS](#)
- [Validation de conformité pour Amazon EFS](#)
- [Résilience dans Amazon EFS](#)
- [Isolation du réseau pour Amazon EFS](#)

Chiffrement des données dans Amazon EFS

Amazon EFS prend en charge deux formes de chiffrement pour les systèmes de fichiers, le chiffrement des données en transit et le chiffrement des données au repos. Vous pouvez activer le chiffrement des données au repos lors de la création du système de fichiers Amazon EFS. Vous pouvez activer le chiffrement des données en transit lors du montage du système de fichiers.

Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 lors de l'accès AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez [Federal Information Processing Standard \(FIPS\) 140-2](#) (Normes de traitement de l'information fédérale).

Si votre organisation est soumise à des politiques d'entreprise ou des réglementations nécessitant le chiffrement des données et des métadonnées au repos, nous vous recommandons de créer un

système de fichiers qui est chiffré au repos, et en montant votre système de fichiers à l'aide du chiffrement des données en transit.

Rubriques

- [AWS KMS](#)
- [Chiffrement de données au repos](#)
- [chiffrement des données en transit](#)
- [Résolution des problèmes de chiffrement](#)

AWS KMS

Amazon EFS s'intègre à AWS Key Management Service (AWS KMS) pour la gestion des clés. Amazon EFS utilise des clés principales client (clés CMK) pour chiffrer votre système de fichiers de la façon suivante :

- Chiffrement des métadonnées au repos – Amazon EFS utilise Clé gérée par AWS pour Amazon EFS, `aws/elasticfilesystem`, pour chiffrer et déchiffrer les métadonnées du système de fichiers (c'est-à-dire les noms de fichiers, les noms de répertoires et le contenu des répertoires).
- Chiffrement de données au repos de fichier – Vous choisissez la clé gérée par le client utilisée pour chiffrer et déchiffrer les données des fichiers (c'est-à-dire le contenu de vos fichiers). Vous pouvez activer, désactiver ou révoquer les subventions sur cette clé gérée par le client. Cette clé gérée côté client peut être l'un des deux types suivants :
 - Clé gérée par AWS pour Amazon EFS — Il s'agit de la clé gérée par le client par défaut, `aws/elasticfilesystem`. La création et le stockage d'une clé gérée par le client ne sont pas facturés, mais il y a des frais d'utilisation. Pour en savoir plus, consultez la page [Tarification AWS Key Management Service](#).
 - Clé gérée par le client – Il s'agit de la clé KMS la plus souple à utiliser, car vous pouvez configurer ses stratégies de clé et ses octrois pour plusieurs utilisateurs ou services. Pour plus d'informations sur la création de clés gérées par le client, consultez la section [Création de clés](#) dans le guide du AWS Key Management Service développeur.

Vous pouvez activer la rotation des clés si vous utilisez une clé gérée par le client pour le chiffrement des données et le déchiffrement des données des fichiers. Lorsque vous activez la rotation des clés, elle fait AWS KMS automatiquement pivoter votre clé une fois par an. De plus, avec une clé gérée par le client, vous pouvez choisir à tout moment de désactiver, réactiver,

supprimer ou révoquer l'accès à votre clé gérée par le client. Pour de plus amples informations, veuillez consulter [Gestion de l'accès aux systèmes de fichiers chiffrés](#).

 Important

Amazon EFS accepte uniquement les clés symétriques gérées côté client. Vous ne pouvez pas utiliser de clés asymétriques gérées par le client avec Amazon EFS.

Le chiffrement et le déchiffrement des données au repos sont gérés de façon transparente. Cependant, les AWS comptes IDs spécifiques à Amazon EFS apparaissent dans vos AWS CloudTrail journaux relatifs aux AWS KMS actions. Pour de plus amples informations, veuillez consulter [Entrées du fichier journal Amazon EFS pour les systèmes de encrypted-at-rest fichiers](#).

Politiques clés d'Amazon EFS pour AWS KMS

Les stratégies de clé constituent le principal moyen de contrôler l'accès aux clés gérées par le client. Pour plus d'informations sur les stratégie de clé, consultez [Stratégie de clé AWS KMS](#) dans le AWS Key Management Service Guide du développeur. La liste suivante décrit toutes les autorisations liées au AWS KMS qui sont requises ou prises en charge par Amazon EFS pour les systèmes de fichiers chiffrés au repos :

- kms:Encrypt - (Facultatif) Chiffre le texte brut en texte chiffré. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms:Decrypt - (Obligatoire) Déchiffre le texte chiffré. Le texte chiffré est du texte brut qui a été précédemment chiffré. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : ReEncrypt — (Facultatif) Chiffre les données côté serveur avec une nouvelle clé gérée par le client, sans exposer le texte clair des données côté client. Les données sont d'abord déchiffrées, puis chiffrées à nouveau. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : GenerateDataKeyWithoutPlaintext — (Obligatoire) Renvoie une clé de chiffrement des données chiffrée sous une clé gérée par le client. Cette autorisation est incluse dans la politique clé par défaut sous kms : GenerateDataKey *.
- kms : CreateGrant — (Obligatoire) Ajoute une autorisation à une clé pour spécifier qui peut utiliser la clé et dans quelles conditions. Les octrois sont des mécanismes d'autorisation alternatifs aux stratégies de clé. Pour plus d'informations sur les subventions, consultez la section [Subventions AWS KMS dans](#) le guide du AWS Key Management Service développeur. Cette autorisation est incluse dans la stratégie de clé par défaut.

- kms : DescribeKey — (Obligatoire) Fournit des informations détaillées sur la clé gérée par le client spécifiée. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : ListAliases — (Facultatif) Répertoire tous les alias clés du compte. Lorsque vous utilisez la console pour créer un système de fichiers chiffré, cette autorisation renseigne la liste Sélectionner une clé principale KMS. Nous vous recommandons d'utiliser cette autorisation pour offrir un confort d'utilisation maximal. Cette autorisation est incluse dans la stratégie de clé par défaut.

Clé gérée par AWS pour la politique KMS d'Amazon EFS

La politique JSON de politique KMS Clé gérée par AWS pour Amazon EFS `aws/elasticfilesystem` est la suivante :

```
{
  "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": "*"
  }
]
```

Chiffrement de données au repos

Vous pouvez créer des systèmes de fichiers chiffrés à l'aide du AWS Management Console AWS CLI, ou par programmation via l'API Amazon EFS ou l'un des AWS SDKs. Votre organisation peut exiger le chiffrement de toutes les données qui répondent à une classification spécifique ou qui sont associées à une application, une charge de travail ou un environnement spécifique.

Une fois que vous avez créé un système de fichiers EFS, vous ne pouvez pas modifier ses paramètres de chiffrement. Cela signifie que vous ne pouvez pas modifier un système de fichiers non chiffré pour le chiffrer. À la place, vous devez créer un système de fichiers chiffré.

Note

L'infrastructure de gestion des AWS clés utilise des algorithmes cryptographiques approuvés par les Federal Information Processing Standards (FIPS) 140-2. Cette infrastructure est conforme aux recommandations NIST (National Institute of Standards and Technology) 800-57.

Imposer la création de systèmes de fichiers EFS chiffrés au repos

Vous pouvez utiliser la clé de condition `elasticfilesystem:Encrypted` IAM dans les politiques basées sur l'identité AWS Identity and Access Management (IAM) pour contrôler si les utilisateurs peuvent créer des systèmes de fichiers Amazon EFS chiffrés au repos. Pour de plus amples

informations sur l'utilisation de la clé de condition , veuillez consulter [Exemple : imposer la création de systèmes de fichiers chiffrés](#).

Vous pouvez également définir des politiques de contrôle des services (SCPs) internes AWS Organizations pour appliquer le chiffrement EFS à tous les Compte AWS membres de votre organisation. Pour plus d'informations sur les politiques de contrôle des services dans AWS Organizations, voir [Politiques de contrôle des services](#) dans le Guide de AWS Organizations l'utilisateur.

Chiffrement d'un système de fichiers au repos à l'aide de la console

Lorsque vous créez un nouveau système de fichiers à l'aide de la console Amazon EFS, le chiffrement au repos est activé par défaut.

Note

Le chiffrement au repos n'est pas activé par défaut lors de la création d'un nouveau système de fichiers à l' AWS CLI aide de l'API et SDKs. Pour de plus amples informations, veuillez consulter [Créez à l'aide du AWS CLI](#).

Comment fonctionne le chiffrement au repos ?

Dans un système de fichiers chiffré, les données et les métadonnées sont automatiquement chiffrées avant d'être écrites dans le système de fichiers. De même, au fur et à mesure que les données et les métadonnées sont lues, elles sont automatiquement déchiffrées avant d'être présentées à l'application. Ces processus sont gérés de façon transparente par Amazon EFS. Vous n'avez donc pas besoin de modifier vos applications.

Amazon EFS utilise l'algorithme de chiffrement AES-256 standard pour chiffrer les données et métadonnées EFS au repos. Pour plus d'informations, consultez les [éléments essentiels de AWS KMS la cryptographie](#) dans le guide du AWS Key Management Service développeur.

chiffrement des données en transit

L'activation du chiffrement des données en transit pour votre système de fichiers EFS s'effectue en activant le protocole TLS (Transport Layer Security) lorsque vous montez votre système de fichiers à l'aide de l'assistant de montage Amazon EFS. Pour de plus amples informations, veuillez consulter [Montage de systèmes de fichiers EFS à l'aide de l'assistant de montage EFS](#).

Lorsque le chiffrement des données en transit est déclaré en tant qu'option de montage pour votre système de fichiers Amazon EFS, l'assistant de montage initialise un processus `stunnel` client. `Stunnel` est un relais réseau multifonctionnel en open source. Le processus `stunnel` client écoute le trafic entrant sur un port local et l'assistant de montage redirige le trafic client NFS vers ce port. L'assistant de montage utilise la version 1.2 de TLS pour communiquer avec votre système de fichiers.

Comment fonctionne le chiffrement des données en transit ?

Pour activer le chiffrement des données en transit, connectez-vous à Amazon EFS avec TLS. Nous vous recommandons d'utiliser l'assistant de montage EFS pour monter votre système de fichiers, car il simplifie le processus de montage par rapport au montage avec le `NFS mount`. L'assistant de montage EFS gère le processus à l'aide du `stunnel` pour TLS. Vous pouvez tout de même activer le chiffrement des données en transit sans utiliser l'assistant de montage. Les étapes générales à suivre sont les suivantes :

Pour activer le chiffrement des données en transit sans l'aide de l'assistant de montage EFS

1. Téléchargez et installez `stunnel`, et notez le port sur lequel l'application est à l'écoute. Pour plus d'instructions, consultez [Mise à niveau d'`stunnel`](#).
2. Exécutez `stunnel` pour vous connecter à votre système de fichiers EFS sur le port 2049 à l'aide du protocole TLS.
3. En utilisant le client NFS, montez `localhost :port`, où `port` est le port que vous avez noté au cours de la première étape.

Étant donné que le chiffrement des données en transit est configuré en mode par connexion, chaque montage configuré possède un processus `stunnel` dédié s'exécutant sur l'instance. Par défaut, le processus `stunnel` est utilisé par l'assistant de montage EFS écoute sur un port local compris entre 20049 et 21049, et se connecte à Amazon EFS sur le port 2049.

Note

Par défaut, lorsque vous utilisez l'assistant de montage Amazon EFS avec TLS, celui-ci procède à la vérification du nom d'hôte du certificat. L'assistant de montage utilise le programme `stunnel` pour sa fonctionnalité TLS. Certaines versions de Linux n'incluent pas une version de `stunnel` prenant en charge ces fonctionnalités TLS par défaut. Lorsque vous utilisez l'une de ces versions de Linux, le montage d'un système de fichiers EFS à l'aide du protocole TLS échoue.

Après avoir installé le `amazon-efs-utils` package, pour mettre à niveau la version de Stunnel de votre système, consultez [Mise à niveau d'stunnel](#).

Pour tout problème lié au chiffrement, consultez [Résolution des problèmes de chiffrement](#).

Lorsque vous utilisez le chiffrement des données en transit, la configuration du client NFS est modifiée. Lorsque vous examinez vos systèmes de fichiers montés, vous en voyez un monté sur `127.0.0.1`, ou `localhost`, comme dans l'exemple suivant :

```
$ mount | column -t
127.0.0.1:/ on /home/ec2-user/efs          type nfs4
(rw,relatime,vers=4.1,rsize=1048576,wsiz=1048576,namlen=255,hard,proto=tcp,port=20127,timeo=600)
```

Lorsque vous effectuez le montage avec TLS et avec l'assistant de montage Amazon EFS vous reconfigurez en fait votre client NFS pour le monter sur un port local. L'assistant de montage démarre un processus client `stunnel` qui est à l'écoute de ce port local et `stunnel` ouvre une connexion chiffrée avec EFS à l'aide du protocole TLS. L'assistant de montage EFS est responsable de la configuration et de la gestion de cette connexion chiffrée et de la configuration associée.

Pour déterminer quel ID de système de fichiers EFS correspond à quel point de montage local, vous pouvez utiliser la commande suivante. Remplacez *efs-mount-point* par le chemin local sur lequel vous avez monté votre système de fichiers.

```
grep -E "Successfully mounted.*efs-mount-point" /var/log/amazon/efs/mount.log | tail -1
```

Lorsque vous utilisez l'assistant de montage pour le chiffrement des données en transit, il crée également un processus appelé `amazon-efs-mount-watchdog`. Ce processus garantit que le processus Stunnel de chaque montage est en cours d'exécution et arrête le Stunnel lorsque le système de fichiers EFS est démonté. Si, pour une raison quelconque, un processus stunnel est interrompu de manière inattendue, le processus de surveillance le redémarre.

Résolution des problèmes de chiffrement

Vous trouverez ci-dessous des informations sur le dépannage des problèmes de chiffrement pour Amazon EFS.

- [Le montage avec chiffrement des données en transit échoue](#)
- [Le montage avec chiffrement des données en transit est interrompu](#)
- [Encrypted-at-rest le système de fichiers ne peut pas être créé](#)

- [Système de fichiers chiffré inutilisable](#)

Le montage avec chiffrement des données en transit échoue

Par défaut, lorsque vous utilisez l'assistant de montage Amazon EFS avec le protocole TLS (Transport Layer Security), celui-ci procède à la vérification du nom d'hôte. Certains systèmes ne prennent pas en charge cette fonction, par exemple lorsque vous utilisez Red Hat Enterprise Linux ou CentOS. Dans ce cas, le montage d'un système de fichiers EFS à l'aide de TLS échoue.

Action à exécuter

Nous vous recommandons de mettre à niveau la version de stunnel sur votre client pour la prise en charge de la vérification du nom d'hôte. Pour de plus amples informations, veuillez consulter [Mise à niveau d'stunnel](#).

Le montage avec chiffrement des données en transit est interrompu

Il est possible, bien que peu probable, que la connexion chiffrée vers votre système de fichiers Amazon EFS soit suspendue ou interrompue par des événements côté client.

Action à exécuter

Si la connexion à votre système de fichiers Amazon EFS avec chiffrement des données en transit est interrompue, procédez comme suit :

1. Assurez-vous que le service stunnel est en cours d'exécution sur le client.
2. Vérifiez que l'application de surveillance amazon-efs-mount-watchdog est en cours d'exécution sur le client. Vous pouvez déterminer si cette application est en cours d'exécution à l'aide de la commande suivante :

```
ps aux | grep [a]mazon-efs-mount-watchdog
```

3. Consultez vos journaux de support. Pour de plus amples informations, veuillez consulter [Obtention de journaux de support](#).
4. Le cas échéant, vous pouvez activer vos journaux stunnel et consulter les informations qu'ils contiennent. Vous pouvez modifier la configuration de vos journaux dans `/etc/amazon/efs/efs-utils.conf` afin d'activer les journaux stunnel. Toutefois, cette opération nécessite le démontage, puis le remontage du système de fichiers à l'aide de l'assistant de montage pour que les modifications prennent effet.

 Important

Sachez que l'activation des journaux stunnel risque d'utiliser une quantité d'espace non négligeable sur votre système de fichiers.

Si les interruptions persistent, contactez le AWS Support.

Encrypted-at-rest le système de fichiers ne peut pas être créé

Vous avez essayé de créer un nouveau système de encrypted-at-rest fichiers. Cependant, un message d'erreur s'affiche indiquant que ce AWS KMS n'est pas disponible.

Action à exécuter

Cette erreur peut se produire dans les rares cas d' AWS KMS indisponibilité temporaire dans votre Région AWS. Dans ce cas, attendez le AWS KMS retour à la pleine disponibilité, puis réessayez de créer le système de fichiers.

Système de fichiers chiffré inutilisable

Un système de fichiers chiffré renvoie systématiquement des erreurs de serveur NFS. Ces erreurs peuvent se produire lorsque EFS ne parvient pas à récupérer votre clé principale AWS KMS pour l'une des raisons suivantes :

- La clé a été désactivée.
- La clé a été supprimée.
- L'autorisation d'Amazon EFS d'utiliser la clé a été révoquée.
- AWS KMS est temporairement indisponible.

Action à exécuter

Vérifiez d'abord que la AWS KMS clé est activée. Vous pouvez le faire en affichant les clés dans la console. Pour plus d'informations, consultez [Affichage des clés](#) dans le AWS Key Management Service Guide du développeur.

Si la clé n'est pas activée, activez-la. Pour de plus amples informations, veuillez consulter [Activation et désactivation des clés](#) du AWS Key Management Service Guide du développeur.

Si la clé est en attente de suppression, ce statut désactive la clé. Vous pouvez annuler la suppression, puis réactiver la clé. Pour de plus amples informations, consultez [Planification et annulation d'une suppression de clé](#) dans le AWS Key Management Service Guide du développeur.

Si la clé est activée et que le problème persiste, ou si vous rencontrez un problème pour la réactiver, contactez le AWS Support.

Gestion des identités et des accès pour Amazon EFS

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Des administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (disposant d'autorisations) à utiliser des ressources Amazon EFS. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion des accès à l'aide de politiques](#)
- [Comment Amazon Elastic File System fonctionne avec IAM](#)
- [Exemples de stratégies basées sur l'identité pour Amazon Elastic File System](#)
- [Exemples de politiques basées sur les ressources pour Amazon EFS](#)
- [AWS politiques gérées pour Amazon EFS](#)
- [Utilisation des balises avec Amazon EFS](#)
- [Utilisation des rôles liés à un service pour Amazon EFS](#)
- [Résolution de problèmes pour l'identité et l'accès Amazon Elastic File System](#)

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon EFS.

Utilisateur du service – Si vous utilisez le service Amazon EFS service pour accomplir votre tâche, votre administrateur vous fournira les informations d'identification et les autorisations

nécessaires. Vous pourrez avoir besoin d'autorisations supplémentaires si vous utilisez davantage de fonctions Amazon EFS. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Amazon EFS, veuillez consulter [Résolution de problèmes pour l'identité et l'accès Amazon Elastic File System](#).

Administrateur du service – Si vous êtes le responsable des ressources Amazon EFS de votre entreprise, vous bénéficiez probablement d'un accès total à Amazon EFS. C'est à vous de déterminer les fonctions et les ressources Amazon EFS auxquelles vos utilisateurs des services pourront accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour découvrir la façon dont votre entreprise peut utiliser IAM avec Amazon EFS, veuillez consulter [Comment Amazon Elastic File System fonctionne avec IAM](#).

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaitez peut-être obtenir des informations sur la façon dont vous pouvez écrire des politiques pour gérer l'accès à Amazon EFS. Pour afficher des exemples de politiques basées sur l'identité Amazon EFS que vous pouvez utiliser dans IAM, consultez [Exemples de stratégies basées sur l'identité pour Amazon Elastic File System](#) (Exemples de politiques basées sur l'identité pour Amazon Simple Notification Service).

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section [Comment vous connecter à votre compte Compte AWS dans](#) le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d'AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez [AWS Signature Version 4 pour les demandes d'API](#) dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez [Authentification multifactorielle](#) dans le Guide de l'utilisateur AWS IAM Identity Center et [Authentification multifactorielle AWS dans IAM](#) dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez [Tâches nécessitant des informations d'identification d'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède en utilisant les informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez

vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez [Qu'est-ce que IAM Identity Center ?](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un [utilisateur IAM](#) est une identité au sein de votre Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification](#) dans le Guide de l'utilisateur IAM.

Un [groupe IAM](#) est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez [Cas d'utilisation pour les utilisateurs IAM](#) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un [rôle IAM](#) est une identité au sein de votre Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez [passer d'un rôle d'utilisateur à un rôle IAM \(console\)](#). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez [Méthodes pour endosser un rôle](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- **Accès utilisateur fédéré** : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez [Jeux d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .
- **Autorisations d'utilisateur IAM temporaires** : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- **Accès intercompte** : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.
- **Accès multiservices** — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- **Sessions d'accès direct (FAS)** : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions d'accès](#).
- **Rôle de service** : il s'agit d'un [rôle IAM](#) attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM.

Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.

- **Rôle lié à un service** — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- **Applications exécutées sur Amazon EC2** : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez [Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez [Choix entre les politiques gérées et les politiques en ligne](#) dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la [présentation de la liste de contrôle d'accès \(ACL\)](#) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- **Limite d'autorisations** : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.
- **Politiques de contrôle des services (SCPs)** : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les [politiques de contrôle des services](#) dans le Guide de AWS Organizations l'utilisateur.
- **Politiques de contrôle des ressources (RCPs)** : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les

autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section [Resource control policies \(RCPs\)](#) dans le guide de AWS Organizations l'utilisateur.

- **Politiques de séance** : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez [Politiques de session](#) dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section [Logique d'évaluation des politiques](#) dans le guide de l'utilisateur IAM.

Comment Amazon Elastic File System fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon EFS, découvrez les fonctionnalités IAM qui peuvent être utilisées avec Amazon EFS.

Fonctions IAM que vous pouvez utiliser avec Amazon Elastic File System

Fonctionnalité IAM	Support Amazon EFS
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui

Fonctionnalité IAM	Support Amazon EFS
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Amazon EFS et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les [AWS services compatibles avec IAM](#) dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Amazon EFS

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez [Références des éléments de politique JSON](#) dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur une identité pour Amazon EFS

Pour voir des exemples de politiques Amazon EFS basées sur l'identité, consultez [Exemples de stratégies basées sur l'identité pour Amazon Elastic File System](#).

Politiques basées sur les ressources au sein d'Amazon EFS

Prend en charge les politiques basées sur les ressources : oui

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Pour en savoir plus sur l'utilisation d'une politique de ressources pour contrôler l'accès aux données du système de fichiers, consultez [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#). Pour savoir comment attacher une stratégie basée sur les ressources à un système de fichiers, consultez [Création de politiques de système de fichiers](#).

Exemples de politiques basées sur les ressources au sein d'Amazon EFS

Pour consulter des exemples de politiques basées sur les ressources Amazon EFS, consultez [Exemples de politiques basées sur les ressources pour Amazon EFS](#).

Actions de politique pour Amazon EFS

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour afficher la liste des actions Amazon EFS, consultez [Actions définies par Amazon Elastic File System](#) dans Référence de l'autorisation de service.

Les actions de politique dans Amazon EFS utilisent le préfixe suivant avant l'action :

```
elasticfilesystem
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [  
    "elasticfilesystem:action1",  
    "elasticfilesystem:action2"  
]
```

Pour voir des exemples de politiques Amazon EFS basées sur l'identité, consultez [Exemples de stratégies basées sur l'identité pour Amazon Elastic File System](#).

Ressources de politique pour Amazon EFS

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources Amazon EFS et leurs caractéristiques ARNs, consultez la section [Ressources définies par Amazon Elastic File System](#) dans le Service Authorization Reference. Pour connaître les actions avec lesquelles vous pouvez spécifier l'ARN de chaque ressource, consultez [Actions définies par Amazon Elastic File System](#).

Pour voir des exemples de politiques Amazon EFS basées sur l'identité, consultez [Exemples de stratégies basées sur l'identité pour Amazon Elastic File System](#).

Clés de condition de politique pour Amazon EFS

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des [opérateurs de condition](#), tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération AND logique. Si vous spécifiez

plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez [Éléments d'une politique IAM : variables et identifications](#) dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

Pour afficher la liste des clés de condition Amazon EFS, consultez [Clés de condition pour Amazon Elastic File System](#) dans Référence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez [Actions définies par Amazon Elastic File System](#).

Pour voir des exemples de politiques Amazon EFS basées sur l'identité, consultez [Exemples de stratégies basées sur l'identité pour Amazon Elastic File System](#).

ACLs dans Amazon EFS

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Amazon EFS

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'[élément de condition](#) d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez [Définition d'autorisations avec l'autorisation ABAC](#) dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez [Utilisation du contrôle d'accès basé sur les attributs \(ABAC\)](#) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Amazon EFS

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation [d'IAM](#) dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez [Passage d'un rôle utilisateur à un rôle IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez [Informations d'identification de sécurité temporaires dans IAM](#).

Autorisations de principal entre services pour Amazon EFS

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions d'accès](#).

Fonctions du service pour Amazon EFS

Prend en charge les rôles de service : oui

Un rôle de service est un [rôle IAM](#) qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.

Warning

La modification des autorisations d'une fonction du service peut altérer la fonctionnalité d'Amazon EFS. Ne modifiez des rôles de service que quand Amazon EFS vous le conseille.

Rôles liés à un service pour Amazon EFS

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service Amazon EFS service, veuillez consulter [Utilisation des rôles liés à un service pour Amazon EFS](#).

Exemples de stratégies basées sur l'identité pour Amazon Elastic File System

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon EFS. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez [Création de politiques IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Pour en savoir plus sur les actions et les types de ressources définis par Amazon EFS, y compris le ARNs format de chaque type de ressource, consultez la section [Actions, ressources et clés de condition pour Amazon Elastic File System](#) dans le Service Authorization Reference.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Utilisation de la console Amazon EFS](#)
- [Exemple : Autoriser les utilisateurs à afficher leurs propres autorisations](#)
- [Exemple : imposer la création de systèmes de fichiers chiffrés](#)
- [Exemple : imposer la création de systèmes de fichiers déchiffrés](#)

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Amazon EFS dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à

vos cas d'utilisation. Pour plus d'informations, consultez [politiques gérées par AWS](#) ou [politiques gérées par AWS pour les activités professionnelles](#) dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez [Validation de politiques avec IAM Access Analyzer](#) dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Sécurisation de l'accès aux API avec MFA](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez [Bonnes pratiques de sécurité dans IAM](#) dans le Guide de l'utilisateur IAM.

Utilisation de la console Amazon EFS

Pour accéder à la console Amazon Elastic File System, vous devez disposer d'un jeu minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon EFS de votre Compte AWS. Si vous créez une

politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Amazon EFS, associez également la politique `AmazonElasticFileSystemReadOnlyAccess` AWS gérée Amazon EFS aux entités. Pour plus d'informations, consultez [Ajout d'autorisations à un utilisateur](#) dans le Guide de l'utilisateur IAM.

Vous pouvez consulter `AmazonElasticFileSystemReadOnlyAccess` et les autres politiques relatives aux services gérés Amazon EFS dans [AWS politiques gérées pour Amazon EFS](#).

Exemple : Autoriser les utilisateurs à afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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": "*"
  }
]
}

```

Exemple : imposer la création de systèmes de fichiers chiffrés

L'exemple suivant illustre une stratégie basée sur l'identité qui autorise les principaux à créer des systèmes de fichiers chiffrés uniquement.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "elasticfilesystem:CreateFileSystem",
      "Condition": {
        "Bool": {
          "elasticfilesystem:Encrypted": "true"
        }
      },
      "Resource": "*"
    }
  ]
}

```

Si cette politique est attribuée à un utilisateur qui tente de créer un système de fichiers non chiffré, la demande échoue. L'utilisateur voit un message similaire au suivant, qu'il utilise le AWS Management Console AWS CLI, l' AWS API ou le SDK :

```

User: arn:aws:iam::111122223333:user/username is not authorized to
perform: elasticfilesystem:CreateFileSystem on the specified resource.

```

Exemple : imposer la création de systèmes de fichiers déchiffrés

L'exemple suivant illustre une stratégie basée sur l'identité qui autorise les principaux à créer des systèmes de fichiers non déchiffrés uniquement.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "elasticfilesystem:CreateFileSystem",
      "Condition": {
        "Bool": {
          "elasticfilesystem:Encrypted": "false"
        }
      },
      "Resource": "*"
    }
  ]
}
```

Si cette politique est attribuée à un utilisateur qui tente de créer un système de fichiers non déchiffré, la demande échoue. L'utilisateur voit un message similaire au suivant, qu'il utilise le AWS Management Console AWS CLI, l' AWS API ou le SDK :

```
User: arn:aws:iam::111122223333:user/username is not authorized to
perform: elasticfilesystem:CreateFileSystem on the specified resource.
```

Vous pouvez également imposer la création de systèmes de fichiers Amazon EFS chiffrés ou non chiffrés en créant une politique de contrôle des AWS Organizations services (SCP). Pour plus d'informations sur les politiques de contrôle des services dans AWS Organizations, voir [Politiques de contrôle des services](#) dans le Guide de AWS Organizations l'utilisateur.

Exemples de politiques basées sur les ressources pour Amazon EFS

Dans cette section, vous trouverez des exemples de stratégie de système de fichiers qui accordent ou refusent des autorisations pour diverses actions Amazon EFS. Les politiques du système de fichiers Amazon EFS sont limitées à 20 000 caractères. Pour plus d'informations sur les éléments

d'une stratégie basée sur les ressources, veuillez consulter [Politiques basées sur les ressources au sein d'Amazon EFS](#).

⚠ Important

Si vous accordez l'autorisation à un utilisateur IAM individuel ou à un rôle IAM dans une stratégie de système de fichiers, ne supprimez pas ou ne recréez pas cet utilisateur ou ce rôle tant que la stratégie est en vigueur sur le système de fichiers. Dans ce cas, l'utilisateur ou le rôle ne pourrait plus accéder au système de fichiers. Pour de plus amples informations, veuillez consulter [Spécification d'un principal](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur la création d'une stratégie de système de fichiers, consultez [Création de politiques de système de fichiers](#).

Rubriques

- [Exemple : accorder un accès en lecture et en écriture à un AWS rôle spécifique](#)
- [Exemple : Accorder l'accès en lecture seule](#)
- [Exemple : garantir que les clients connectés conservent l'accès après avoir configuré la réplication entre comptes](#)
- [Exemple : accorder l'accès à un point d'accès EFS](#)

Exemple : accorder un accès en lecture et en écriture à un AWS rôle spécifique

Cet exemple de stratégie de système de fichiers EFS présente les caractéristiques suivantes :

- L'effet est Allow.
- Le principal est défini sur le Testing_Role dans le Compte AWS.
- L'action est définie sur ClientMount (lecture) et ClientWrite.
- La condition d'octroi des autorisations est définie sur 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"
        }
    }
}
]
}

```

Exemple : Accorder l'accès en lecture seule

La politique de système de fichiers suivante accorde uniquement des autorisations `ClientMount`, ou des autorisations en lecture seule, au rôle `EfsReadOnly` IAM.

```

{
  "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"
    }
  ]
}

```

Pour apprendre à définir des stratégies de système de fichiers supplémentaires, notamment en refusant l'accès racine à tous les principaux IAM à l'exception d'une station de travail de gestion

spécifique, veuillez consulter [Activer l'écrasement des racines à l'aide de l'autorisation IAM pour les clients NFS](#).

Exemple : garantir que les clients connectés conservent l'accès après avoir configuré la réplication entre comptes

Vous pouvez utiliser la politique basée sur les ressources suivante pour garantir que tous les clients connectés au système de fichiers conservent l'accès après avoir configuré la réplication entre comptes pour le système de fichiers. Pour plus d'informations sur la réplication entre comptes, voir [Réplication des systèmes de fichiers EFS sur plusieurs comptes AWS](#)

Les exigences suivantes s'appliquent lors de la création de la politique.

- Utilisez l'assistant de montage EFS pour monter le système de fichiers. Si le système de fichiers est monté à l'aide du client NFS, les clients connectés se verront refuser l'accès en raison d'erreurs du serveur.
- Utilisez l'option `-o iam` ou `-o tls` dans la commande `mount` pour transmettre vos informations d'identification à la cible de montage 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"
        }
      }
    }
  ]
}
```

```

    }
  ]
}
```

Exemple : accorder l'accès à un point d'accès EFS

Une stratégie d'accès EFS permet de fournir à un client NFS une vue spécifique à une application des ensembles de données basés sur des fichiers partagés sur un système de fichiers EFS. Vous accordez les autorisations de point d'accès sur le système de fichiers à l'aide d'une stratégie de système de fichiers.

Cet exemple de stratégie de fichier utilise un élément de condition pour accorder à un point d'accès spécifique identifié par son ARN l'accès complet au système de fichiers.

Pour plus d'informations sur l'utilisation des points d'accès EFS, consultez [Utilisation des points d'accès](#).

```

{
  "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 politiques gérées pour Amazon EFS

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation

courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des [politiques gérées par le client](#) qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSService RoleForAmazonElasticFileSystem

Amazon EFS utilise le rôle lié au service nommé `AWSServiceRoleForAmazonElasticFileSystem` pour permettre à Amazon EFS de gérer les AWS ressources en votre nom. Ce rôle fait confiance au `elasticfilesystem.amazonaws.com` service pour assumer le rôle. Pour de plus amples informations, veuillez consulter [Utilisation des rôles liés à un service pour Amazon EFS](#).

AWS politique gérée : AmazonElasticFileSystemFullAccess

Vous pouvez associer la politique `AmazonElasticFileSystemFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès complet à Amazon EFS et l'accès aux AWS services associés via le AWS Management Console.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `elasticfilesystem` – Permet aux principaux d'effectuer toutes les actions dans la console Amazon EFS. Il permet également aux principaux de créer (`elasticfilesystem:Backup`) et de restaurer (`elasticfilesystem:Restore`) des sauvegardes à l'aide AWS Backup de.
- `cloudwatch`— Permet aux principaux de décrire les métriques CloudWatch du système de fichiers Amazon et les alarmes associées à une métrique dans la console Amazon EFS.

- `ec2`— Permet aux principaux de créer, de supprimer et de décrire des interfaces réseau, de décrire et de modifier les attributs des interfaces réseau, de décrire les zones de disponibilité, les groupes de sécurité, les sous-réseaux, les clouds privés virtuels (VPCs) et les attributs VPC associés à un système de fichiers EFS dans la console Amazon EFS.
- `kms`— Permet aux principaux de répertorier les alias des clés AWS Key Management Service (AWS KMS) et de décrire les clés KMS dans la console Amazon EFS.
- `iam`— Accorde l'autorisation de créer un rôle lié à un service qui permet à Amazon EFS de gérer les AWS ressources pour le compte de l'utilisateur.
- `iam:PassRole`— Accorde l'autorisation de transmettre un rôle IAM à Amazon EFS.

Pour consulter les autorisations associées à cette politique, consultez

[AmazonElasticFileSystemFullAccess](#) le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonElasticFileSystemReadOnlyAccess

Vous pouvez associer la politique `AmazonElasticFileSystemReadOnlyAccess` à vos identités IAM.

Cette politique accorde un accès en lecture seule à Amazon EFS via le AWS Management Console.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `elasticfilesystem` – Permet aux responsables de décrire les attributs des systèmes de fichiers Amazon EFS, notamment les préférences de compte, les politiques de sauvegarde et de système de fichiers, la configuration du cycle de vie, les cibles de montage et leurs groupes de sécurité, les balises et les points d'accès dans la console Amazon EFS.
- `cloudwatch`— Permet aux principaux de récupérer les CloudWatch métriques et de décrire les alarmes relatives aux métriques dans la console Amazon EFS.
- `ec2`— Permet aux principaux d'afficher les zones de disponibilité, les interfaces réseau et leurs attributs, les groupes de sécurité, les sous-réseaux VPCs et leurs attributs dans la console Amazon EFS.
- `kms`— Permet aux principaux de répertorier les alias des AWS KMS clés dans la console Amazon EFS.

Pour consulter les autorisations associées à cette politique, consultez [AmazonElasticFileSystemReadOnlyAccess](#) le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonElasticFileSystemClientFullAccess

Vous pouvez attacher la politique AmazonElasticFileSystemClientFullAccess à une entité IAM.

Cette politique accorde aux clients l'accès en lecture et en écriture aux systèmes de fichiers EFS. Cette politique permet aux clients NFS de monter, de lire et d'écrire sur les systèmes de fichiers EFS.

Pour consulter les autorisations associées à cette politique, consultez [AmazonElasticFileSystemFullAccess](#) le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonElasticFileSystemClientReadWriteAccess

Vous pouvez attacher la politique AmazonElasticFileSystemClientReadWriteAccess à une entité IAM.

Cette politique accorde aux clients l'accès en lecture et en écriture aux systèmes de fichiers EFS. Cette politique permet aux clients NFS de monter, de lire et d'écrire sur les systèmes de fichiers EFS.

Pour consulter les autorisations associées à cette politique, consultez [AmazonElasticFileSystemClientReadWriteAccess](#) le Guide de référence des politiques AWS gérées.

Amazon EFS met à jour les politiques AWS gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon EFS depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page [Historique du document](#) Amazon EFS.

Modification	Description	Date
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemFullAccess Amazon EFS a ajouté ce qui suit : ReplicationRead et ReplicationWrite pour autoriser la lecture et l'écriture des données du système de fichiers à des fins de réplication.	7 novembre 2024

Modification	Description	Date
	• <code>iam:PassRole</code> pour autoriser Amazon EFS à créer des configurations de réplication.	
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemServiceRolePolicy Amazon EFS a ajouté <code>ReplicationRead</code> et <code>ReplicationWrite</code> pour autoriser la lecture et l'écriture des données du système de fichiers à des fins de réplication.	7 novembre 2024
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemReadOnlyAccess Amazon EFS a ajouté l'<code>ReplicationRead</code> action permettant de lire les données du système de fichiers à des fins de réplication.	7 novembre 2024
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemReadOnlyAccess Amazon EFS a ajouté de nouvelles autorisations qui permettent aux comptes source et de destination d'accéder aux systèmes de fichiers pour les répliquons entre comptes.	7 août 2024
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemFullAccess Amazon EFS a ajouté une nouvelle autorisation permettant aux principaux de désactiver et d'activer la protection sur un système de fichiers. Les autorisations sont requises pour permettre à Amazon EFS de se répliquer sur un système de fichiers existant.	27 novembre 2023

Modification	Description	Date
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemServiceRolePolicy Amazon EFS a ajouté de nouvelles autorisations pour permettre aux principaux de créer, de décrire et de supprimer des répliquions Amazon EFS, ainsi que de créer des systèmes de fichiers Amazon EFS. Les autorisations sont requises pour permettre à Amazon EFS de gérer les configurations de répliquion des systèmes de fichiers au nom de l'utilisateur.	25 janvier 2022
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemReadOnlyAccess Amazon EFS a ajouté une nouvelle autorisation permettant aux principaux de décrire les répliquions Amazon EFS. Les autorisations sont requises pour permettre aux utilisateurs de visualiser les configurations de répliquion des systèmes de fichiers.	25 janvier 2022
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemFullAccess Amazon EFS a ajouté de nouvelles autorisations pour permettre aux principaux de créer, de décrire et de supprimer des répliquions Amazon EFS. Les autorisations sont requises pour permettre aux utilisateurs de gérer les configurations de répliquion des systèmes de fichiers.	25 janvier 2022
Démarrage de la politique de suivi	Stratégie : AmazonElasticFileSystemClientReadWriteAccess Accorde des privilèges de lecture et d'écriture sur les systèmes de fichiers Amazon EFS aux clients NFS.	3 janvier 2022

Modification	Description	Date
Démarrage de la politique de suivi	Stratégie : AmazonElasticFileSystemServiceRolePolicy Autorisations du rôle lié à un service pour Amazon EFS.	8 octobre 2021
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemFullAccess Amazon EFS a ajouté de nouvelles autorisations pour permettre aux principaux de modifier et de décrire les préférences des comptes Amazon EFS. Les autorisations sont requises pour permettre aux utilisateurs de consulter et de définir les paramètres des préférences du compte dans la console Amazon EFS.	7 mai 2021
Mise à jour d'une stratégie existante	Stratégie : AmazonElasticFileSystemReadOnlyAccess Amazon EFS a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les préférences des comptes Amazon EFS. Les autorisations sont requises pour permettre aux utilisateurs de consulter les paramètres des préférences du compte dans la console Amazon EFS.	7 mai 2021
Amazon EFS a commencé à assurer le suivi des modifications	Amazon EFS a commencé à suivre les modifications apportées AWS à ses politiques gérées.	7 mai 2021

Utilisation des balises avec Amazon EFS

Vous pouvez utiliser des balises pour contrôler l'accès aux ressources Amazon EFS et pour implémenter le contrôle d'accès basé sur les attributs (ABAC). Pour plus d'informations, consultez :

- [Marquage des ressources EFS](#)
- [Contrôle de l'accès en fonction des balises sur une ressource](#)
- [À quoi sert ABAC ? AWS](#) dans le guide de l'utilisateur IAM

 Note

La réplication EFS ne prend pas en charge l'utilisation de balises pour le Contrôle d'accès par attributs (ABAC).

Pour appliquer des balises aux ressources Amazon EFS lors de leur création, les utilisateurs doivent disposer de certaines autorisations (IAM) AWS Identity and Access Management .

Octroi de les autorisations de baliser les ressources lors de la création

Les actions de balisage lors de la création d'API Amazon EFS suivantes vous permettent de spécifier des balises lorsque vous créez la ressource.

- `CreateAccessPoint`
- `CreateFileSystem`

Pour permettre aux utilisateurs d'attribuer des balises aux ressources au moment de la création, ils doivent avoir les autorisations d'utiliser l'action qui crée les ressources (par exemple, `elasticfilesystem:CreateAccessPoint` ou `elasticfilesystem:CreateFileSystem`). Si des balises sont spécifiées dans l'action de création de ressources, octroie AWS une autorisation supplémentaire à `elasticfilesystem:TagResource` pour vérifier si les utilisateurs sont autorisés à créer des balises. Par conséquent, les utilisateurs doivent également avoir des autorisations explicites d'utiliser l'action `elasticfilesystem:TagResource`.

Dans la définition de stratégie IAM de l'action `elasticfilesystem:TagResource`, utilisez l'élément `Condition` avec la clé de condition `elasticfilesystem:CreateAction` pour accorder des autorisations de balisage à l'action qui crée la ressource.

Exemple stratégie : autoriser l'ajout de balises aux systèmes de fichiers uniquement lors de la création

L'exemple de stratégie suivant permet aux utilisateurs de créer des systèmes de fichiers et appliquer des balises aux lors de la création. Les utilisateurs ne sont pas autorisés à attribuer des balises aux

ressources existantes (ils ne peuvent pas appeler l'action `elasticfilesystem:TagResource` directement).

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

Utiliser des balises pour contrôler l'accès à vos ressources Amazon EFS

Pour contrôler l'accès aux ressources et actions Amazon EFS, vous pouvez utiliser des politiques IAM basées sur des balises. Vous pouvez fournir le contrôle de deux manières :

- Vous pouvez contrôler l'accès aux ressources Amazon EFS en fonction des balises de ces ressources.
- Vous pouvez contrôler les balises qui peuvent être transmises dans une condition de demande IAM.

Pour plus d'informations sur l'utilisation des balises pour contrôler l'accès aux AWS ressources, consultez la section [Contrôle de l'accès à l'aide de balises](#) dans le guide de l'utilisateur IAM.

Contrôle de l'accès en fonction des balises sur une ressource

Les balises permettent de contrôler les actions qu'un utilisateur ou un rôle peut effectuer sur une ressource Amazon EFS. Par exemple, vous pouvez autoriser ou refuser des opérations d'API spécifiques sur une ressource de système de fichiers en fonction de la paire clé-valeur de la balise sur la ressource.

Exemple politique : créer un système de fichiers uniquement lorsqu'une balise spécifique est utilisée

L'exemple de politique suivant permet à l'utilisateur de créer un système de fichiers uniquement s'il le balise avec une paire clé-valeur de balise spécifique, dans cet exemple, `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"
    }
  }
}
```

Exemple politique : Supprimer les systèmes de fichiers dotés de balises spécifiques

L'exemple de stratégie suivant permet à un utilisateur de supprimer uniquement les systèmes de fichiers marqués avec `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"
            }
        }
    ]
}
```

Utilisation des rôles liés à un service pour Amazon EFS

Amazon Elastic File System utilise un rôle lié à un [service AWS Identity and Access Management](#) (IAM). Un rôle lié à un service Amazon EFS est un type unique de rôle IAM lié directement à Amazon EFS. Le rôle prédéfini lié au service Amazon EFS inclut les autorisations dont le service a besoin pour appeler d'autres personnes en votre Services AWS nom.

Un rôle lié à un service simplifie la configuration d'Amazon EFS, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Amazon EFS définit les autorisations de ses rôles liés à un service et seul Amazon EFS peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer le rôle lié à un service Amazon EFS uniquement après avoir supprimé vos systèmes de fichiers Amazon EFS. Vos ressources Amazon EFS sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Le rôle lié à un service permet à tous les appels d'API d'être visibles. AWS CloudTrail Cela facilite le suivi et la vérification des exigences, car vous pouvez suivre toutes les actions exécutées par Amazon EFS en votre nom. Pour de plus amples informations, veuillez consulter [Entrées de journal pour les rôles liés à un service EFS](#).

Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Autorisations du rôle lié à un service pour Amazon EFS.

Amazon EFS utilise le rôle lié au service nommé `AWSServiceRoleForAmazonElasticFileSystem` pour permettre à Amazon EFS d'appeler et de gérer AWS des ressources pour le compte de vos systèmes de fichiers EFS.

Le rôle `AWSServiceRoleForAmazonElasticFileSystem` lié au service fait confiance à ce qu'`elasticfilesystem.amazonaws.com` assume le rôle.

La stratégie d'autorisations liée au rôle permet à Amazon EFS de réaliser les actions incluses dans la définition de la stratégie JSON :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource": [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
```

```

        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
    ],
    "Resource": [
        "arn:aws:backup:*:*:backup-plan:*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": [
                "backup.amazonaws.com"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
    ],
    "Condition": {
        "StringLike": {
            "iam:PassedToService": "backup.amazonaws.com"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem>DeleteReplicationConfiguration",
        "elasticfilesystem:ReplicationRead",

```

```
        "elasticfilesystem:ReplicationWrite"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

Vous devez configurer manuellement les autorisations IAM AWS KMS lorsque vous créez un nouveau système de fichiers EFS chiffré au repos. Pour en savoir plus, veuillez consulter la section [Chiffrement de données au repos](#).

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section [Autorisations relatives aux rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Amazon EFS

Dans la plupart des cas, il n'est pas nécessaire de créer manuellement un rôle lié à un service. Lorsque vous créez des cibles de montage ou une configuration de réplication pour votre système de fichiers EFS dans l'AWS Management Console AWS CLI AWS API, Amazon EFS crée le rôle lié au service pour vous.

En outre, si vous le supprimez manuellement service-linked-role, puis que vous devez le créer à nouveau, vous pouvez utiliser le même processus pour recréer le rôle dans votre compte. Lorsque vous créez des cibles de montage ou une configuration de réplication pour votre système de fichiers EFS, Amazon EFS crée le rôle lié au service pour vous.

Toutefois, si Amazon EFS ne crée pas le service-linked-role ou si vous avez commencé à utiliser Amazon EFS avant qu'il ne prenne en charge les rôles liés à un service, vous pouvez créer manuellement le rôle lié à un service. Pour obtenir des instructions, consultez la section [Création d'un rôle lié à un service](#) dans le guide de l'utilisateur IAM.

Modification d'un rôle lié à un service pour Amazon EFS

Amazon EFS ne vous autorise pas à modifier le rôle lié à un service `AWSServiceRoleForAmazonElasticFileSystem`. Une fois que vous avez créé un rôle lié

à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, voir [Mettre à jour un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Amazon EFS

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement. Pour de plus amples informations, veuillez consulter [Nettoyez les ressources et protégez votre AWS compte](#).

Note

Si le service Amazon EFS utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSService RoleForAmazonElasticFileSystem service. Pour plus d'informations, consultez [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés aux services Amazon EFS

Amazon EFS prend en charge l'utilisation de rôles liés à un service partout Régions AWS où le service est disponible. Pour plus d'informations, consultez la section [Points AWS de terminaison du service](#) dans le Guide de Références générales AWS l'utilisateur.

Résolution de problèmes pour l'identité et l'accès Amazon Elastic File System

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous utilisez Amazon EFS et IAM.

Rubriques

- [Je ne suis pas autorisé à effectuer une action dans Amazon EFS](#)
- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon EFS](#)

Je ne suis pas autorisé à effectuer une action dans Amazon EFS

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource `my-example-widget` fictive, mais ne dispose pas des autorisations `elasticfilesystem:GetWidget` fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
elasticfilesystem:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource `my-example-widget` à l'aide de l'action `elasticfilesystem:GetWidget`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon EFS.

Certains services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Amazon EFS. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon EFS

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Amazon EFS est compatible avec ces fonctionnalités, veuillez consulter [Comment Amazon Elastic File System fonctionne avec IAM](#).
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section [Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez](#) dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section [Fournir un accès à des ressources Comptes AWS détenues par des tiers](#) dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez [Fournir un accès à des utilisateurs authentifiés en externe \(fédération d'identité\)](#) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers

Vous pouvez utiliser à la fois des stratégies d'identité IAM et des stratégies de ressource pour contrôler l'accès client NFS aux ressources Amazon EFS d'une manière évolutive et optimisée pour les environnements sur le cloud. En utilisant IAM, vous pouvez autoriser les clients à effectuer des actions spécifiques sur un système de fichiers, y compris l'accès racine, en lecture seule et en écriture. Une autorisation « d'autorisation » sur une action dans le cadre d'une stratégie d'identité IAM ou d'une politique de ressources du système de fichiers autorise l'accès à cette action.

L'autorisation n'a pas besoin d'être accordée à la fois dans une politique d'identité et dans une politique de ressources.

Les clients NFS peuvent s'identifier à l'aide d'un rôle IAM lors de la connexion à un système de fichiers EFS. Lorsqu'un client se connecte à un système de fichiers, Amazon EFS évalue la stratégie de ressources IAM du système de fichiers (appelée « stratégie de système de fichiers ») ainsi que les politiques IAM basées sur l'identité afin de déterminer les autorisations d'accès au système de fichiers appropriées à accorder.

Lorsque vous utilisez l'autorisation IAM pour des clients NFS, les connexions client et les décisions d'autorisation IAM sont consignées dans AWS CloudTrail. Pour plus d'informations sur la journalisation des appels d'API Amazon EFS avec CloudTrail, consultez [Journalisation des appels d'API Amazon EFS avec AWS CloudTrail](#).

Important

Vous devez utiliser l'assistant de montage EFS pour monter vos systèmes de fichiers EFS afin d'utiliser l'autorisation IAM pour contrôler l'accès des clients. Pour de plus amples informations, veuillez consulter [Montage avec autorisation IAM](#).

Stratégie de système de fichiers EFS par défaut

La stratégie du système de fichiers EFS par défaut n'utilise pas IAM pour l'authentification et accorde un accès complet à tout client anonyme pouvant se connecter au système de fichiers à l'aide d'une cible de montage. La politique par défaut est en vigueur quand aucune politique de système de fichiers configurée par l'utilisateur n'est en vigueur, y compris au moment de la création du système de fichiers. Chaque fois que la stratégie de système de fichiers par défaut est en vigueur, une opération d'API [DescribeFileSystemPolicy](#) renvoie une réponse `PolicyNotFound`.

Actions EFS pour les clients

Vous pouvez spécifier les actions suivantes pour les clients sur un système de fichiers à l'aide d'une stratégie de système de fichiers.

Action	Description
<code>elasticfilesystem:ClientMount</code>	Fournit un accès en lecture seule à un système de fichiers.

Action	Description
<code>elasticfilesystem:ClientWrite</code>	Fournit les droits d'écriture sur un système de fichiers.
<code>elasticfilesystem:ClientRootAccess</code>	Permet d'utiliser l'utilisateur root lors de l'accès à un système de fichiers.

Clés de condition EFS pour les clients NFS

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Amazon EFS dispose des clés de condition prédéfinies suivantes pour les clients NFS. Aucune autre clé de condition n'est appliquée lors de l'utilisation des contrôles IAM pour sécuriser l'accès aux systèmes de fichiers EFS.

Clé de condition EFS	Description	Opérateur
<code>aws:SecureTransport</code>	Utilisez cette clé pour exiger que les clients utilisent TLS lors de la connexion à un système de fichiers EFS.	Booléen
<code>aws:SourceIp</code>	Utilisez cette clé pour comparer l'adresse IP du demandeur avec celle spécifiée dans la politique. La clé de condition <code>aws:SourceIp</code> ne peut être utilisée que pour les plages d'adresses IP publiques.	Chaîne
<code>elasticfilesystem:AccessPointArn</code>	ARN du point d'accès EFS auquel le client se connecte.	Chaîne
<code>elasticfilesystem:AccessedViaMountTarget</code>	Utilisez cette clé pour empêcher les clients qui n'utilisent pas de cibles de montage de systèmes	Booléen

Clé de condition EFS	Description	Opérateur
	de fichiers d'accéder à un système de fichiers EFS.	

Exemples de stratégie de système de fichiers

Pour consulter des exemples de politiques relatives aux systèmes de fichiers Amazon EFS, consultez [Exemples de politiques basées sur les ressources pour Amazon EFS](#).

Contrôle de l'accès réseau aux systèmes de fichiers EFS pour les clients NFS

Vous pouvez contrôler l'accès par les clients NFS aux systèmes de fichiers à l'aide de stratégies de sécurité de la couche réseau et de systèmes de fichiers EFS. Vous pouvez utiliser les mécanismes de sécurité de la couche réseau disponibles sur Amazon EC2, tels que les règles des groupes de sécurité VPC et le réseau. ACLs Vous pouvez également utiliser AWS IAM pour contrôler l'accès NFS à l'aide d'une politique de système de fichiers EFS et de politiques basées sur l'identité.

Rubriques

- [Utilisation de groupes de sécurité VPC](#)
- [Utilisation des points de terminaison VPC d'interface dans Amazon EFS](#)

Utilisation de groupes de sécurité VPC

Lorsque vous utilisez Amazon EFS, vous spécifiez des groupes de sécurité VPC pour vos EC2 instances et des groupes de sécurité pour les cibles de montage EFS associées au système de fichiers. Les groupes de sécurité font office de pare-feu, et les règles que vous ajoutez définissent le flux de trafic. Dans l'[exercice Getting started](#), vous avez créé un groupe de sécurité lorsque vous avez lancé l'instance EFS. Vous en avez ensuite associé un autre avec la cible de montage EFS (c'est-à-dire, le groupe de sécurité par défaut pour votre VPC par défaut). Cette approche fonctionne pour l'exercice Getting Started. Toutefois, pour un système de production, vous devez configurer des groupes de sécurité dotés d'autorisations minimales pour une utilisation avec Amazon EFS.

Vous pouvez autoriser l'accès entrant et sortant à votre système de fichiers EFS. Pour ce faire, vous ajoutez des règles qui permettent aux instances EFS de se connecter à votre système de fichiers EFS via la cible de montage à l'aide du port NFS (Network File System).

- Chaque EC2 instance qui monte le système de fichiers doit disposer d'un groupe de sécurité doté d'une règle autorisant l'accès sortant à la cible de montage sur le port NFS.
- La cible de montage EFS doit disposer d'un groupe de sécurité doté d'une règle autorisant l'accès entrant depuis chaque EC2 instance sur laquelle vous souhaitez monter le système de fichiers.

Ports source pour travailler avec Amazon EFS

Afin de prendre en charge une large gamme de clients NFS, Amazon EFS autorise les connexions à partir de n'importe quel port source. Si vous avez besoin que seuls des utilisateurs privilégiés puissent accéder à Amazon EFS, nous vous recommandons d'utiliser la règle de pare-feu client suivante. Connectez-vous à votre système de fichiers à l'aide de SSH et exécutez la commande suivante :

```
iptables -I OUTPUT 1 -m owner --uid-owner 1-4294967294 -m tcp -p tcp --dport 2049 -j DROP
```

Cette commande insère une nouvelle règle au début de la chaîne OUTPUT (-I OUTPUT 1). Cette règle empêche tout processus non privilégié et ne dépendant pas du noyau (-m owner --uid-owner 1-4294967294) d'ouvrir une connexion au port NFS (-m tcp -p tcp --dport 2049).

Considérations relatives à la sécurité pour l'accès réseau

Un client NFS version 4.1 (NFSv4.1) ne peut monter un système de fichiers que s'il peut établir une connexion réseau avec le port NFS (port TCP 2049) de l'une des cibles de montage du système de fichiers. De même, un client NFSv4.1 ne peut affirmer un identifiant d'utilisateur et de groupe lors de l'accès à un système de fichiers que s'il peut établir cette connexion réseau.

La possibilité d'établir une telle connexion réseau est régie par une combinaison des éléments suivants :

- Isolement réseau fourni par le VPC des cibles de montage – Les cibles de montage du système de fichiers ne peuvent pas être associées à des adresses IP publiques. Les seules cibles qui peuvent monter les systèmes de fichiers sont les suivantes :
 - EC2 Instances Amazon dans le VPC Amazon local

- EC2 instances connectées VPCs
- Serveurs sur site connectés à un Amazon VPC à l'aide d'AWS Direct Connect ou d'AWS Virtual Private Network (VPN)
- Listes de contrôle d'accès réseau (ACLs) pour les sous-réseaux VPC du client et des cibles de montage, pour l'accès depuis l'extérieur des sous-réseaux de la cible de montage — Pour monter un système de fichiers, le client doit être en mesure d'établir une connexion TCP avec le port NFS d'une cible de montage et de recevoir le trafic de retour.
- Règles des groupes de sécurité VPC du client et des cibles de montage, pour tous les accès — Pour qu'une EC2 instance puisse monter un système de fichiers, les règles de groupe de sécurité suivantes doivent être en vigueur :
 - Le système de fichiers doit avoir une cible de montage dont l'interface réseau comporte un groupe de sécurité avec une règle permettant les connexions entrantes sur le port NFS à partir de l'instance. Vous pouvez activer les connexions entrantes par adresse IP (plage d'adresses CIDR) ou par groupe de sécurité. La source des règles du groupe de sécurité du port NFS entrant sur les interfaces réseau de cible de montage est un élément clé pour le contrôle d'accès des systèmes de fichiers. Les règles entrantes autres que celle du port NFS, et les règles sortantes, ne sont pas utilisées par les interfaces réseau pour les cibles de montage du système de fichier.
 - L'instance de montage doit avoir une interface réseau comportant une règle de groupe de sécurité permettant les connexions sortantes vers le port NFS sur l'une des cibles de montage du système de fichiers. Vous pouvez activer les connexions sortantes par adresse IP (plage d'adresses CIDR) ou par groupe de sécurité.

Pour de plus amples informations, veuillez consulter [Gérer des cibles de Montage](#).

Création de groupes de sécurité

Pour créer des groupes de sécurité pour les EC2 instances et les cibles de montage EFS

Voici les étapes générales que vous allez suivre lors de la création des groupes de sécurité pour Amazon EFS. Pour obtenir des instructions sur la création des groupes de sécurité, consultez la section [Créer un groupe de sécurité](#) dans le guide de l'utilisateur Amazon VPC.

1. Pour vos EC2 instances, créez un groupe de sécurité avec les règles suivantes :
 - Règle entrante qui autorise l'accès entrant qui permet d'utiliser Secure Shell (SSH) depuis n'importe quel hôte. Vous pouvez éventuellement limiter l'adresse Source.

- Règle sortante qui permet à tout le trafic de sortir. Lorsque vous créez un groupe de sécurité, il est créé avec une règle sortante par défaut, vous ne devriez donc pas avoir à en ajouter une.
2. Pour votre cible de montage EFS, créez un groupe de sécurité avec les règles suivantes :
- Règle entrante qui autorise l'accès depuis le groupe de EC2 sécurité. Identifiez le groupe EC2 de sécurité comme source.
 - Règle sortante permettant d'ouvrir la connexion TCP sur tous les ports NFS. Identifiez le groupe EC2 de sécurité comme destination.

Utilisation des points de terminaison VPC d'interface dans Amazon EFS

Pour établir une connexion privée entre votre cloud privé virtuel (VPC) et l'API Amazon EFS, vous pouvez créer un point de terminaison d'un VPC d'interface. Le point de terminaison fournit une connectivité sécurisée à l'API Amazon EFS sans nécessiter une passerelle Internet, une instance NAT ou un réseau privé virtuel (VPN). Pour plus d'informations, consultez la section [Accès à un AWS service à l'aide d'un point de terminaison VPC d'interface](#) dans le guide de l'utilisateur Amazon VPC.

Les points de terminaison VPC d'interface sont alimentés par AWS PrivateLink une fonctionnalité qui permet une communication privée entre les AWS services à l'aide d'adresses IP privées. Pour l'utiliser AWS PrivateLink, créez un point de terminaison VPC d'interface pour Amazon EFS dans votre VPC à l'aide de la console, de l'API ou de la CLI Amazon VPC. Cela crée une interface réseau élastique dans votre sous-réseau avec une adresse IP privée qui sert les demandes d'API Amazon EFS. Vous pouvez également accéder à un point de terminaison VPC depuis des environnements sur site ou depuis une autre VPCs utilisation AWS VPN, AWS Direct Connect ou depuis le peering VPC. Pour en savoir plus, consultez [Connect your VPC to services AWS PrivateLink](#) in the Amazon VPC User Guide.

Création d'un point de terminaison d'interface pour Amazon EFS

Pour créer un point de terminaison d'un VPC d'interface pour Amazon EFS, utilisez l'une des méthodes suivantes :

- **com.amazonaws.*region*.elasticfilesystem** – Crée un point de terminaison pour les opérations d'API Amazon EFS.
- **com.amazonaws.*region*.elasticfilesystem-fips** – Crée un point de terminaison pour l'API Amazon EFS conforme à la [norme Federal Information Processing Standard \(FIPS\) 140-2](#).

Pour obtenir la liste complète des points de terminaison Amazon EFS, consultez la section Points de [terminaison et quotas Amazon Elastic File System](#) dans le. Référence générale d'Amazon Web Services

Pour plus d'informations sur la création d'un point de terminaison d'interface, consultez [Accéder à un AWS service à l'aide d'un point de terminaison VPC d'interface](#) dans le guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour Amazon EFS

Pour contrôler l'accès à l'API Amazon EFS, vous pouvez associer une politique AWS Identity and Access Management (IAM) à votre point de terminaison VPC. La stratégie spécifie les éléments suivants :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez [Contrôle de l'accès aux points de terminaison d'un VPC à l'aide de politiques de point de terminaison](#) dans le Guide de l'utilisateur Amazon VPC.

L'exemple suivant montre une stratégie de point de terminaison d'un VPC qui refuse à tout le monde l'autorisation de créer un système de fichiers EFS via le point de terminaison. L'exemple de politique accorde également à tout le monde l'autorisation d'effectuer toutes les autres actions.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "elasticfilesystem:CreateFileSystem",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

```
}
```

Utilisateurs, groupes et autorisations au niveau du système de fichiers réseau (NFS)

Après la création d'un système de fichiers, par défaut, seul l'utilisateur racine (UID 0) dispose d'autorisations de lecture-écriture-exécution. Pour que d'autres utilisateurs puissent modifier le système de fichiers, l'utilisateur racine doit leur accorder explicitement l'accès. Vous pouvez utiliser des points d'accès pour automatiser la création de répertoires accessibles en écriture à partir d'un utilisateur non racine. Pour de plus amples informations, veuillez consulter [Utilisation des points d'accès](#).

Un mode de style Unix est associé aux objets du système de fichiers EFS. La valeur de ce mode définit les autorisations permettant d'effectuer des actions au niveau de cet objet. Les utilisateurs familiers avec les systèmes de style UNIX comprendront facilement comment Amazon EFS se comporte quant à ces autorisations.

En outre, sur les systèmes de type Unix, les utilisateurs et les groupes sont mappés à des identificateurs numériques, lesquels sont utilisés par Amazon EFS pour représenter la propriété de fichier. Pour Amazon EFS, les objets du système de fichiers (c'est-à-dire les fichiers, les répertoires, etc.) appartiennent à un seul propriétaire et à un seul groupe. Amazon EFS utilise le numérique mappé IDs pour vérifier les autorisations lorsqu'un utilisateur tente d'accéder à un objet du système de fichiers.

Note

Le protocole NFS prend en charge un maximum de 16 groupes IDs (GIDs) par utilisateur et tous les groupes supplémentaires GIDs sont tronqués à partir des demandes des clients NFS. Pour de plus amples informations, veuillez consulter [Accès refusé aux fichiers autorisés sur le système de fichiers NFS](#).

Vous trouverez ci-dessous des exemples d'autorisations et une discussion sur les considérations relatives aux autorisations de NFS pour Amazon EFS.

Rubriques

- [Autorisations sur les fichiers et les répertoires](#)

- [Exemples de cas d'utilisation et d'autorisations du système de fichiers EFS](#)
- [Autorisations d'identification d'utilisateur et de groupe pour les fichiers et les répertoires d'un système de fichiers](#)
- [Aucun écrasement racine](#)
- [Mise en cache des autorisations](#)
- [Modification de la propriété d'un objet du système de fichiers](#)
- [Points d'accès EFS](#)

Autorisations sur les fichiers et les répertoires

Les fichiers et les répertoires d'un système de fichiers EFS prennent en charge les autorisations de lecture, d'écriture et d'exécution standard de style UNIX basées sur l'identifiant d'utilisateur et de groupe affirmé par le client NFSv4 .1 de montage, sauf si un point d'accès EFS est remplacé par un point d'accès EFS. Pour de plus amples informations, veuillez consulter [Utilisateurs, groupes et autorisations au niveau du système de fichiers réseau \(NFS\)](#).

Note

Par défaut, cette couche de contrôle d'accès dépend de la confiance accordée au client NFSv4 .1 pour ce qui est de l'affirmation de l'identifiant de l'utilisateur et du groupe. Vous pouvez utiliser des politiques basées sur les ressources AWS Identity and Access Management (IAM) et des politiques d'identité pour autoriser les clients NFS et fournir des autorisations d'accès en lecture seule, en écriture et en root. Vous pouvez utiliser des points d'accès EFS pour remplacer les informations d'identité d'utilisateur et de groupe du système d'exploitation fournies par le client NFS. Pour plus d'informations, consultez [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#) et [Création de points d'accès](#).

À titre d'exemple d'autorisations de lecture, d'écriture et d'exécution pour les fichiers et les répertoires, Alice peut avoir des autorisations lui permettant de lire et d'écrire dans tout fichier de son répertoire personnel sur un système de fichiers, `/alice`. Toutefois, dans cet exemple, Alice n'est pas autorisée à lire ni à écrire dans les fichiers du répertoire personnel de Mark sur le même système de fichiers, `/mark`. Alice et Mark sont tous deux autorisés à lire, mais pas à écrire, sur les fichiers du répertoire partagé `/share`.

Exemples de cas d'utilisation et d'autorisations du système de fichiers EFS

Après avoir créé un système de fichiers EFS et monté des cibles pour le système de fichiers dans votre VPC, vous pouvez monter le système de fichiers distant localement sur votre instance Amazon EC2 . La commande `mount` permet de monter un répertoire sur le système de fichiers. Toutefois, lorsque vous créez le système de fichiers pour la première fois, un seul répertoire racine se trouve à l'emplacement `/`. L'utilisateur racine et le groupe racine sont propriétaires du répertoire monté.

La commande `mount` suivante permet de monter le répertoire racine d'un système de fichiers Amazon EFS, identifié par le nom DNS de système de fichiers, dans le répertoire local `/efs-mount-point`.

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

Le mode d'autorisations initial autorise :

- des autorisations `read-write-execute` sur le propriétaire racine
- des autorisations `read-execute` sur le groupe racine
- des autorisations `read-execute` sur les autres

Seul l'utilisateur racine peut modifier ce répertoire. L'utilisateur racine peut aussi accorder des autorisations à d'autres utilisateurs pour l'écriture dans ce répertoire, par exemple :

- Créer des sous-répertoires par utilisateur accessibles en écriture. Pour step-by-step obtenir des instructions, voir [Tutoriel : Création de sous-répertoires accessibles en écriture par utilisateur](#).
- Autorisez les utilisateurs à écrire à la racine du système de fichiers EFS. Un utilisateur avec des privilèges racine peut accorder à d'autres utilisateurs l'accès au système de fichiers.
 - Pour attribuer la propriété du système de fichiers EFS à un utilisateur et à un groupe non root, procédez comme suit :

```
$ sudo chown user:group /EFSroot
```

- Pour remplacer les autorisations du système de fichiers par des autorisations moins restrictives, utilisez la commande suivante :

```
$ sudo chmod 777 /EFSroot
```

Cette commande accorde des read-write-execute privilèges à tous les utilisateurs sur toutes les EC2 instances sur lesquelles le système de fichiers est monté.

Autorisations d'identification d'utilisateur et de groupe pour les fichiers et les répertoires d'un système de fichiers

Les fichiers et les répertoires d'un système de fichiers EFS prennent en charge les autorisations de lecture, d'écriture et d'exécution standard de style UNIX en fonction de l'ID utilisateur et du groupe. IDs Lorsqu'un client NFS monte un système de fichiers EFS sans utiliser de point d'accès, l'ID utilisateur et l'ID de groupe fournis par le client sont approuvés. Vous pouvez utiliser les points d'accès EFS pour remplacer l'ID utilisateur et le groupe IDs utilisés par le client NFS. Lorsque des utilisateurs tentent d'accéder à des fichiers et à des répertoires, Amazon EFS contrôle leur utilisateur IDs et leur groupe IDs pour vérifier que chaque utilisateur est autorisé à accéder aux objets. Amazon EFS les utilise également IDs pour indiquer le propriétaire et le propriétaire du groupe pour les nouveaux fichiers et répertoires créés par l'utilisateur. Amazon EFS n'examine pas les noms des utilisateurs ou des groupes, il utilise uniquement les identifiants numériques.

Note

Lorsque vous créez un utilisateur sur une EC2 instance, vous pouvez attribuer n'importe quel ID utilisateur numérique (UID) ou ID de groupe (GID) à l'utilisateur. Les utilisateurs numériques IDs sont définis dans le `/etc/passwd` fichier sur les systèmes Linux. Le groupe numérique IDs se trouve dans le `/etc/group` fichier. Ces fichiers définissent les mappages entre les noms et IDs. En dehors de l' EC2 instance, Amazon EFS n'effectue aucune authentification pour ces derniers IDs, y compris l'ID racine de 0.

Si un utilisateur accède à un système de fichiers EFS à partir de deux EC2 instances différentes, selon que l'UID de l'utilisateur est identique ou différent sur ces instances, vous constatez un comportement différent, comme suit :

- Si les utilisateurs IDs sont identiques sur les deux EC2 instances, Amazon EFS considère qu'ils indiquent le même utilisateur, quelle que soit l' EC2 instance utilisée. L'expérience utilisateur lors de l'accès au système de fichiers est la même dans les deux EC2 instances.

- Si l'utilisateur IDs n'est pas le même sur les deux EC2 instances, Amazon EFS considère qu'il s'agit d'utilisateurs différents. L'expérience utilisateur n'est pas la même lorsqu'il accède au système de fichiers EFS à partir des deux EC2 instances différentes.
- Si deux utilisateurs différents sur des EC2 instances différentes partagent un même identifiant, Amazon EFS les considère comme étant le même utilisateur.

Vous pouvez envisager de gérer les mappages d'ID utilisateur de manière cohérente entre EC2 les instances. Les utilisateurs peuvent vérifier leur ID numérique à l'aide de la commande `id`.

```
$ id

uid=502(joe) gid=502(joe) groups=502(joe)
```

Désactivation de l'outil de mappage d'ID

Les utilitaires NFS du système d'exploitation incluent un démon appelé ID Mapper qui gère le mappage entre les noms d'utilisateur et IDs. Dans Amazon Linux, ce démon est appelé `rpc.idmapd` et sur Ubuntu il est appelé `idmapd`. Il traduit l'utilisateur et IDs le groupe en noms, et vice versa. Toutefois, Amazon EFS ne traite que des données numériques. IDs Nous vous recommandons de désactiver ce processus sur vos EC2 instances. Sur Amazon Linux, l'outil de mappage d'ID est généralement désactivé. Si tel est le cas, ne l'activez pas. Pour désactiver l'outil de mappage d'ID, utilisez la commande illustrée ci-dessous.

```
$ service rpcidmapd status
$ sudo service rpcidmapd stop
```

Aucun écrasement racine

Par défaut, l'écrasement root est désactivé sur les systèmes de fichiers EFS. Amazon EFS se comporte comme un serveur NFS Linux avec `no_root_squash`. Si un ID d'utilisateur ou de groupe est 0, Amazon EFS traite cet utilisateur en tant qu'utilisateur root, et il omet les vérifications d'autorisations (en autorisant l'accès à tous les objets de système de fichiers et leur modification). L'écrasement root peut être activé sur une connexion client lorsque la politique d'identité ou de ressource AWS Identity and Access Management (AWS IAM) n'autorise pas l'accès à `ClientRootAccess`. Lorsque l'écrasement racine est activé, l'utilisateur racine est converti en utilisateur disposant d'autorisations limitées sur le serveur NFS.

Pour de plus amples informations, veuillez consulter [Utilisation de l'IAM pour contrôler l'accès aux systèmes de fichiers](#).

Activer l'écrasement des racines à l'aide de l'autorisation IAM pour les clients NFS

Vous pouvez configurer Amazon EFS pour empêcher l'accès root à votre système de fichiers EFS pour tous les AWS principaux, à l'exception d'un seul poste de gestion. Pour ce faire, configurez l'autorisation AWS Identity and Access Management (IAM) pour les clients NFS (Network File System).

Pour ce faire, vous devez configurer deux stratégies d'autorisation IAM comme suit :

- Créez une stratégie de système de fichiers EFS qui autorise explicitement l'accès en lecture et en écriture au système de fichiers et qui refuse implicitement l'accès racine.
- Attribuez une identité IAM à la station EC2 de gestion Amazon qui nécessite un accès root au système de fichiers à l'aide d'un profil d' EC2 instance. Pour plus d'informations sur les profils d' EC2 instance Amazon, consultez la section [Utiliser les profils d'instance](#) dans le Guide de AWS Identity and Access Management l'utilisateur.
- Attribuez la politique AmazonElasticFileSystemClientFullAccess AWS gérée au rôle IAM de la station de travail de gestion. Pour plus d'informations sur les politiques AWS gérées pour Amazon EFS, consultez [Gestion des identités et des accès pour Amazon EFS](#).

Pour activer l'écrasement racine à l'aide de l'autorisation IAM pour les clients NFS, procédez comme suit :

Pour empêcher l'accès de la racine au système de fichiers

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Choisissez File Systems (Systèmes de fichiers).
3. Choisissez le système de fichiers sur lequel vous souhaitez activer l'écrasement root.
4. Sur la page de détails du système de fichiers, choisissez Stratégie du système de fichiers, puis Modifier. La page File system policy (Stratégie du système de fichiers) s'affiche.
5. Choisissez Empêcher l'accès root par défaut* dans les options de politique. L'objet JSON de politique apparaît dans l'éditeur de stratégie.
6. Choisissez Save (Enregistrer) pour enregistrer la stratégie de système de fichiers.

Les clients non anonymes peuvent obtenir un accès racine au système de fichiers via une stratégie basée sur l'identité. Lorsque vous associez la stratégie gérée `AmazonElasticFileSystemClientFullAccess` au rôle de la station de travail, IAM accorde l'accès racine à la station de travail en fonction de sa stratégie d'identité.

Pour activer l'accès racine à partir de la station de travail de gestion

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Créez un rôle pour Amazon EC2 appelé `EFS-client-root-access`. IAM crée un profil d'instance portant le même nom que le EC2 rôle que vous avez créé.
3. Assignez la politique AWS gérée `AmazonElasticFileSystemClientFullAccess` au EC2 rôle que vous avez créé. Le contenu de cette stratégie est présenté ci-dessous.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource": "*"
    }
  ]
}
```

4. Attachez le profil d'instance à l' EC2 instance que vous utilisez comme poste de travail de gestion, comme décrit ci-dessous. Pour plus d'informations, consultez [Attacher un rôle IAM à une instance](#) dans le Guide de l' EC2 utilisateur Amazon pour les instances Linux.
 - a. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
 - b. Dans le panneau de navigation, choisissez Instances.
 - c. Choisissez l'instance. Pour Actions, choisissez Instance Settings (Paramètres d'instance), puis Attach/Replace IAM role (Attacher/Remplacer le rôle IAM).
 - d. Sélectionnez le rôle IAM que vous avez créé lors de la première étape, `EFS-client-root-access`, puis choisissez Apply (Appliquer).

5. Installez l'assistant de montage EFS sur la station de travail de gestion. Pour plus d'informations sur l'assistant de montage EFS et le `amazon-efs-utils` package, consultez [Installation du client Amazon EFS](#)
6. Montez le système de fichiers EFS sur la station de travail de gestion à l'aide de la commande suivante avec l'option `iam mount`.

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

Vous pouvez configurer l' EC2 instance Amazon pour monter automatiquement le système de fichiers avec l'autorisation IAM. Pour en savoir plus sur le montage d'un système de fichiers EFS avec autorisation IAM, consultez [Montage avec autorisation IAM](#).

Mise en cache des autorisations

Amazon EFS met en cache les autorisations de fichiers pendant une courte période. Par conséquent, un utilisateur dont l'accès a été récemment révoqué peut encore accéder à cet objet pendant une brève période.

Modification de la propriété d'un objet du système de fichiers

Amazon EFS applique l'attribut `chown_restricted` POSIX. Cela signifie que seul l'utilisateur racine peut modifier le propriétaire d'un objet du système de fichiers. L'utilisateur racine ou propriétaire peut modifier le groupe propriétaire d'un objet du système de fichiers. Cependant, à moins que l'utilisateur soit de type racine, le groupe ne peut être remplacé que par un groupe dont l'utilisateur propriétaire est un membre.

Points d'accès EFS

Un point d'accès applique un utilisateur, un groupe et un chemin d'accès du système de fichiers pour système d'exploitation à toute demande de système de fichiers effectuée à l'aide du point d'accès. L'utilisateur et le groupe du système d'exploitation du point d'accès remplacent toutes les informations d'identité fournies par le client NFS. Le chemin d'accès du système de fichiers est exposé au client en tant que répertoire racine du point d'accès. Cette approche garantit que chaque application utilise toujours l'identité correcte du système d'exploitation et le bon répertoire lors de l'accès à des ensembles de données basés sur des fichiers partagés. Les applications utilisant le point d'accès peuvent uniquement accéder aux données dans leur propre répertoire et en dessous. Pour plus d'informations sur les points d'accès, consultez [Utilisation des points d'accès](#).

Utilisation des points d'accès

Les points d'accès EFS sont des points d'entrée spécifiques à une application dans un système de fichiers EFS qui facilitent la gestion de l'accès des applications aux ensembles de données partagés. Les points d'accès peuvent appliquer de manière forcée une identité d'utilisateur, y compris les groupes POSIX de l'utilisateur, pour toutes les demandes de système de fichiers effectuées via le point d'accès. Les points d'accès peuvent également appliquer de manière forcée un répertoire racine différent pour le système de fichiers afin que les clients puissent uniquement accéder aux données stockées dans le répertoire spécifié ou dans les sous-répertoires.

Vous pouvez utiliser des politiques AWS Identity and Access Management (IAM) pour garantir que des applications spécifiques utilisent un point d'accès spécifique. En combinant des politiques IAM avec des points d'accès, vous pouvez facilement fournir un accès sécurisé à des ensembles de données spécifiques pour vos applications.

Note

Vous devez créer au moins une cible de montage sur votre système de fichiers EFS pour utiliser les points d'accès.

Vous pouvez créer des points d'accès pour un système de fichiers EFS existant à l'aide de AWS Management Console, the AWS Command Line Interface (AWS CLI) et de l'API Amazon EFS. Un système de fichiers EFS peut avoir un [maximum de 10 000 points d'accès](#). Vous ne pouvez pas modifier un point d'accès une fois qu'il a été créé.

Pour step-by-step les procédures de création d'un point d'accès, voir [Création de points d'accès](#).

Vous utilisez l'assistant de montage EFS lors du montage d'un système de fichiers à l'aide d'un point d'accès. Dans la commande mount, vous devez inclure l'ID du système de fichiers, l'ID du point d'accès et l'option mount `tls`, comme illustré dans l'exemple suivant.

```
$ mount -t efs -o tls,iam,accesspoint=fsap-abcdef0123456789a fs-  
abc0123def456789a: /localmountpoint
```

Pour plus d'informations sur le montage de systèmes de fichiers à l'aide d'un point d'accès, veuillez consulter [Montage avec points d'accès EFS](#).

Rubriques

- [Application forcée d'une identité utilisateur à l'aide d'un point d'accès](#)
- [Application forcée d'un répertoire racine avec un point d'accès](#)
- [Utilisation des points d'accès dans les stratégies IAM](#)

Application forcée d'une identité utilisateur à l'aide d'un point d'accès

Vous pouvez utiliser un point d'accès pour appliquer de manière forcée les informations d'utilisateur et de groupe pour toutes les demandes de système de fichiers effectuées via le point d'accès. Pour activer cette fonction, vous devez spécifier l'identité du système d'exploitation à appliquer de manière forcée lors de la création du point d'accès.

Dans le cadre de ce document, vous fournissez ce qui suit :

- ID utilisateur : ID d'utilisateur POSIX numérique de l'utilisateur.
- ID de groupe : ID de groupe POSIX numérique de l'utilisateur.
- Groupe secondaire IDs : liste facultative de groupes secondaires IDs.

Lorsque le contrôle des utilisateurs est activé, Amazon EFS remplace l'utilisateur et le groupe du client NFS IDs par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers. L'application forcée par l'utilisateur a également l'impact suivant :

- Le propriétaire et le groupe des nouveaux fichiers et répertoires sont définis sur l'ID utilisateur et l'ID de groupe du point d'accès.
- L'EFS prend en compte l'ID utilisateur, l'ID de groupe et le groupe secondaire IDs du point d'accès lors de l'évaluation des autorisations du système de fichiers. EFS ignore ceux du client NFS. IDs

Important

L'application forcée d'une identité d'utilisateur est soumise à l'autorisation IAM `ClientRootAccess`.

Par exemple, dans certains cas, vous pouvez configurer l'ID utilisateur du point d'accès, l'ID du groupe ou les deux pour qu'ils soient à la racine (c'est-à-dire définir l'UID, le GID ou les deux sur 0). Dans ce cas, vous devez accorder l'autorisation IAM `ClientRootAccess` au client NFS.

Application forcée d'un répertoire racine avec un point d'accès

Vous pouvez utiliser un point d'accès pour remplacer le répertoire racine d'un système de fichiers. Lors de l'application forcée d'un répertoire racine, le client NFS lié au point d'accès utilise le répertoire racine configuré sur le point d'accès au lieu du répertoire racine du système de fichiers.

Vous activez cette fonction en définissant l'attribut de point d'accès `Path` lors de la création d'un point d'accès. L'attribut `Path` est le chemin d'accès complet du répertoire racine du système de fichiers pour toutes les demandes de système de fichiers effectuées via ce point d'accès. Le chemin complet ne peut pas dépasser 100 caractères. Il peut inclure jusqu'à quatre sous-répertoires.

Lorsque vous spécifiez un répertoire racine sur un point d'accès, il devient le répertoire racine du système de fichiers pour le client NFS qui monte le point d'accès. Par exemple, supposons que le répertoire racine de votre point d'accès soit `/data`. Dans ce cas, le montage `fs-12345678:/` à l'aide du point d'accès a le même effet que le montage `fs-12345678:/data` sans l'utilisation du point d'accès.

Lorsque vous spécifiez un répertoire racine dans votre point d'accès, assurez-vous que les autorisations d'annuaire sont configurées pour permettre à l'utilisateur du point d'accès de monter correctement le système de fichiers. Plus précisément, assurez-vous que le bit d'exécution est défini pour l'utilisateur ou le groupe du point d'accès, ou pour tout le monde. Par exemple, une valeur d'autorisation d'annuaire de 755 permet au propriétaire de l'utilisateur d'annuaire de répertorier des fichiers, de créer des fichiers et de monter, et à tous les autres utilisateurs de lister des fichiers et de les monter.

Création du répertoire racine d'un point d'accès

Si aucun chemin d'accès au répertoire racine n'existe pour un point d'accès sur le système de fichiers, Amazon EFS crée automatiquement ce répertoire racine avec la propriété et les autorisations configurables. Amazon EFS ne créera pas le répertoire racine si vous ne spécifiez pas la propriété et les autorisations du répertoire lors de sa création. Cette approche permet de provisionner l'accès au système de fichiers pour un utilisateur ou une application spécifique sans monter votre système de fichiers à partir d'un hôte Linux. Pour créer un répertoire racine, vous devez configurer la propriété et les autorisations du répertoire racine à l'aide des attributs suivants lors de la création d'un point d'accès :

- `OwnerUid` : ID utilisateur POSIX numérique à utiliser en tant que propriétaire du répertoire racine.
- `OwnerGid` : ID de groupe POSIX numérique à utiliser en tant que groupe propriétaire du répertoire racine.

- **Autorisations** : mode Unix du répertoire. Une configuration commune est 755. Assurez-vous que le bit d'exécution est défini pour l'utilisateur du point d'accès afin qu'il puisse être monté. Cette configuration donne au propriétaire du répertoire l'autorisation d'entrer, de répertorier et d'écrire de nouveaux fichiers dans le répertoire. Elle donne à tous les autres utilisateurs l'autorisation d'entrer et de répertorier des fichiers. Pour plus d'informations sur l'utilisation des modes de fichier et de répertoire Unix, veuillez consulter [Utilisateurs, groupes et autorisations au niveau du système de fichiers réseau \(NFS\)](#).

Amazon EFS crée un répertoire racine de point d'accès uniquement si le nom `OwnerId`, le `OwnGid` et les autorisations sont spécifiés pour le répertoire. Si vous ne fournissez pas ces informations, Amazon EFS ne crée pas le répertoire racine. Si le répertoire racine n'existe pas, les tentatives de montage au moyen du point d'accès échoueront.

Lorsque vous montez un système de fichiers avec un point d'accès, le répertoire racine du point d'accès est créé s'il n'existe pas déjà, à condition que le répertoire racine `OwnerId` et les autorisations aient été spécifiés lors de la création du point d'accès. Si le répertoire racine du point d'accès existe déjà au moment du montage, les autorisations existantes ne seront pas écrasées par le point d'accès. Si vous supprimez le répertoire racine, EFS le recréera lorsque le système de fichiers sera monté de nouveau à l'aide du point d'accès.

Note

Amazon EFS ne créera pas le répertoire racine si vous ne spécifiez pas la propriété et les autorisations du répertoire racine du point d'accès. Toutes les tentatives de montage du point d'accès échoueront.

Modèle de sécurité pour les répertoires racine d'un point d'accès

Lorsqu'un remplacement de répertoire racine est en vigueur, Amazon EFS se comporte comme un serveur NFS Linux avec l'option `no_subtree_check` activée.

Dans le protocole NFS, les serveurs génèrent des descripteurs de fichier qui sont utilisés par les clients comme références uniques lors de l'accès aux fichiers. EFS génère en toute sécurité des descripteurs de fichier imprévisibles et spécifiques à un système de fichiers EFS. Lorsqu'un remplacement du répertoire racine est en place, Amazon EFS ne divulgue pas les descripteurs de fichiers situés en dehors du répertoire racine spécifié. Cependant, dans certains cas, un utilisateur peut obtenir un descripteur de fichier pour un fichier en dehors de son point d'accès en utilisant un

out-of-band mécanisme. Par exemple, cela est envisageable s'ils ont accès à un deuxième point d'accès. Dans ce cas, ils peuvent effectuer des opérations de lecture et d'écriture sur le fichier.

La propriété des fichiers et les autorisations d'accès sont toujours appliquées pour l'accès aux fichiers dans et hors du répertoire racine du point d'accès d'un utilisateur.

Utilisation des points d'accès dans les stratégies IAM

Vous pouvez utiliser une stratégie IAM pour appliquer de manière forcée l'accès d'un client NFS spécifique, identifié par son rôle IAM, à un point d'accès particulier. Pour ce faire, utilisez la clé de condition IAM `elasticfilesystem:AccessPointArn`. `AccessPointArn` est l'ARN (Amazon Resource Name) du point d'accès avec lequel le système de fichiers est monté.

Voici un exemple de stratégie de système de fichiers qui permet au rôle IAM `app1` d'accéder au système de fichiers à l'aide du point d'accès `fsap-01234567`. Cette stratégie permet également à `app2` d'utiliser le système de fichiers via le point d'accès `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"
        }
      }
    ]
  }
}
```

Blocage de l'accès public aux systèmes de fichiers EFS

La fonctionnalité de blocage de l'accès public d'Amazon EFS fournit des paramètres qui vous aident à gérer l'accès public aux systèmes de fichiers EFS. Par défaut, les nouveaux systèmes de fichiers EFS n'autorisent pas l'accès public. En revanche, vous pouvez modifier les stratégies du système de fichiers pour autoriser l'accès public.

Important

L'activation du blocage de l'accès public permet de protéger vos ressources en empêchant l'accès public d'être accordé par le biais des politiques de ressources directement associées au système de fichiers. Outre l'activation du blocage de l'accès public, examinez attentivement les politiques suivantes pour vous assurer qu'elles n'accordent pas d'accès public :

- Politiques basées sur l'identité associées aux AWS principaux associés (par exemple, rôles IAM)
- Politiques basées sur les AWS ressources associées (par exemple, clés AWS Key Management Service (KMS))

Rubriques

- [Blocage de l'accès public avec AWS Transfer Family](#)
- [La signification du mot « public »](#)

Blocage de l'accès public avec AWS Transfer Family

Lorsque vous utilisez Amazon EFS avec AWS Transfer Family, les demandes d'accès au système de fichiers reçues d'un serveur Transfer Family appartenant à un compte différent de celui du système de fichiers sont bloquées si le système de fichiers autorise l'accès public. Amazon EFS évalue les politiques IAM du système de fichiers, et si la politique est publique, il bloque la demande. Pour autoriser AWS Transfer Family l'accès à votre système de fichiers, mettez à jour la politique de votre système de fichiers afin qu'elle ne soit pas considérée comme publique.

Note

L'utilisation de Transfer Family avec Amazon EFS est désactivée par défaut pour Compte AWS les systèmes de fichiers EFS dotés de politiques autorisant l'accès public créées avant le 6 janvier 2021. Pour activer l'utilisation de Transfer Family pour accéder à votre système de fichiers, contactez le AWS Support.

La signification du mot « public »

Pour évaluer si un système de fichiers autorise l'accès public, Amazon EFS part du principe que la stratégie du système de fichiers est publique. Puis, il évalue la stratégie du système de fichiers pour déterminer si elle est qualifiée comme non publique. Pour être considérée comme non publique, une stratégie de système de fichiers doit uniquement accorder l'accès aux valeurs fixes (valeurs ne contenant aucun caractère générique) d'un ou de plusieurs des éléments suivants :

- Un ensemble de routages interdomaines sans classe (CIDRs), utilisant `aws:SourceIp` Pour plus d'informations sur le CIDR, consultez [RFC 4632](#) le site Web de l'éditeur RFC.
- Un AWS principal, un utilisateur, un rôle ou un principal de service (par exemple, `aws:PrincipalOrgID`)
- `aws:SourceArn`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:SourceOwner`
- `aws:SourceAccount`
- `elasticfilesystem:AccessedViaMountTarget`
- `aws:userid`, outside the pattern `"AROLEID:*`

Conformément à ces règles, l'exemple de stratégie suivant est considéré comme public.

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

Vous pouvez rendre cette stratégie de système de fichiers non publique en utilisant la clé de condition `elasticfilesystem:AccessedViaMountTarget` définie sur `true`. Vous pouvez utiliser `elasticfilesystem:AccessedViaMountTarget` pour autoriser les actions EFS spécifiées aux clients accédant au système de fichiers EFS à l'aide d'une cible de montage du système de fichiers. La stratégie non publique suivante utilise la clé de condition `elasticfilesystem:AccessedViaMountTarget` définie sur `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"
      }
    }
  }
]
```

Pour de plus amples informations sur l'utilisation des clés de condition Amazon EFS, consultez la section [Clés de condition EFS pour les clients NFS](#). Pour plus d'informations sur la création de stratégies de système de fichiers, consultez [Création de politiques de système de fichiers](#).

Validation de conformité pour Amazon EFS

Pour savoir si un [programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- [Conformité et gouvernance de la sécurité](#) : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- [Référence des services éligibles HIPAA](#) : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de <https://aws.amazon.com/compliance/resources/> de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- [AWS Guides de conformité destinés aux clients](#) — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans

de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).

- [Évaluation des ressources à l'aide des règles](#) du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- [AWS Security Hub](#)— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez [Référence des contrôles Security Hub](#).
- [Amazon GuardDuty](#) — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- [AWS Audit Manager](#)— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Amazon EFS

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité (AZs). Régions AWS fournissent plusieurs réseaux physiquement séparés et isolés AZs, connectés par un réseau à faible latence, à haut débit et hautement redondant. Vous pouvez ainsi concevoir et exploiter des applications et des bases de données qui basculent automatiquement entre les zones sans interruption. AZs AZs sont plus hautement disponibles, tolérants aux pannes et évolutifs que les infrastructures traditionnelles de centres de données uniques ou multiples.

Les systèmes de fichiers Amazon EFS sont résilients face à une ou plusieurs défaillances de zone de disponibilité au sein d'une Région AWS. Les cibles de montage sont elles-mêmes conçues pour être hautement disponibles. Lorsque vous concevez pour une haute disponibilité et un basculement vers une autre solution AZs, gardez à l'esprit que, même si les adresses IP et le DNS de vos cibles de montage dans chaque zone de disponibilité sont statiques, il s'agit de composants redondants soutenus par de multiples ressources. Pour de plus amples informations, veuillez consulter [Comment Amazon EFS fonctionne avec Amazon EC2](#).

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Isolation du réseau pour Amazon EFS

En tant que service géré, Amazon Elastic File System est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section [Sécurité du AWS cloud](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon EFS via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser [AWS Security Token Service](#) (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Ils peuvent être APIs appelés depuis n'importe quel emplacement réseau, mais Amazon EFS prend en charge les politiques d'accès basées sur les ressources, qui peuvent inclure des restrictions basées sur l'adresse IP source. Vous pouvez également utiliser les politiques Amazon EFS pour contrôler l'accès à partir de points de terminaison Amazon Virtual Private Cloud (Amazon VPC) spécifiques ou spécifiques. VPCs En fait, cela isole l'accès réseau à une ressource Amazon EFS donnée uniquement du VPC spécifique au sein AWS du réseau.

Quotas Amazon EFS

Vous trouverez ci-dessous les informations sur les quotas lors de l'utilisation d'Amazon EFS.

Rubriques

- [Les quotas Amazon EFS que vous pouvez augmenter](#)
- [Les quotas de ressources Amazon EFS que vous ne pouvez pas Modifier](#)
- [Quotas pour les clients NFS](#)
- [Quotas pour les systèmes de fichiers Amazon EFS](#)
- [Fonctionnalités NFSv4 4.0 et 4.1 non prises en charge](#)
- [Considérations supplémentaires](#)
- [Résolution des erreurs de fonctionnement des fichiers liées aux quotas](#)

Les quotas Amazon EFS que vous pouvez augmenter

Service Quotas est un AWS service qui vous permet de gérer vos quotas, ou limites, à partir d'un seul endroit. Dans la [console Service Quotas](#), vous pouvez consulter les valeurs limites d'Amazon EFS et demander une augmentation du quota pour le nombre de systèmes de fichiers EFS dans un Région AWS et pour les IOPS en lecture pour les données fréquemment consultées.

Vous pouvez aussi demander une augmentation des quotas Amazon EFS suivants en contactant l'assistance AWS . Pour en savoir plus, veuillez consulter la section [Demande d'augmentation de quota](#). L'équipe du service Amazon EFS examine chaque demande individuellement.

- Nombre de systèmes de fichiers pour chaque compte client.
- Nombre de points d'accès pour chaque système de fichiers.
- Nombre maximal d'IOPS en lecture par système de fichiers grâce au débit élastique. Lorsque les IOPS en lecture pour les systèmes de fichiers fréquemment utilisés sont augmentées, les IOPS en lecture pour les systèmes de fichiers rarement utilisés et les IOPS en écriture sont également augmentées.
- Débit élastique par système de fichiers régional pour tous les clients connectés dans un Région AWS.
- Débit provisionné par système de fichiers régional pour tous les clients connectés dans un. Région AWS

Le tableau suivant répertorie les quotas de ressources par défaut généraux que vous pouvez demander à modifier.

Ressource	Quota par défaut
Nombre de systèmes de fichiers pour chaque compte client dans un Région AWS	1 000
Nombre de points d'accès pour chaque système de fichiers	10 000
Nombre maximal d'IOPS par système de fichiers grâce au débit élastique	Données rarement consultées lues : 90 000
	Données fréquemment consultées lues : 250 000
	Écrire : 50 000
Vous pouvez demander une augmentation jusqu'à 10 fois le quota par défaut d'IOPS de lecture pour les données fréquemment consultées. L'augmentation des IOPS de lecture pour les données fréquemment consultée s entraîne également une augmentation des IOPS de lecture pour les données rarement consultées et des IOPS d'écriture.	

Le tableau suivant répertorie les quotas de débit élastiques par système de fichiers pour tous les clients connectés dans chaque Région AWS système de fichiers.

Systèmes de fichiers régionaux : débit élastique total par défaut par système de fichiers pour tous les clients connectés de chaque système de fichiers Région AWS

Région AWS	Débit de lecture maximal	Débit d'écriture maximal (débit mesuré)
Région US East (Ohio)	60 gibioctets par seconde () GiBps	5 GiBps
Région USA Est (Virginie du Nord)		
Région USA Ouest (Oregon)		
Asia Pacific (Mumbai) Region		
Région Asie-Pacifique (Séoul)		
Région Asie-Pacifique (Singapour)		
Région Asie-Pacifique (Sydney)		
Asia Pacific (Tokyo) Region		
Europe (Frankfurt) Region		
Région Europe (Irlande)		
Région Europe (London)		
Tous les autres Régions AWS	20 GiBps	1 GiBps

Le tableau suivant répertorie les quotas de débit alloués par système de fichiers pour tous les clients connectés de chaque système de fichiers. Région AWS

Systèmes de fichiers régionaux — Débit total provisionné par défaut par système de fichiers pour tous les clients connectés de chaque système de fichiers Région AWS

Région AWS	Débit de lecture maximal	Débit d'écriture maximal (débit mesuré)
Région US East (Ohio)	10 GiBps	3,33 GiBps
Région USA Est (Virginie du Nord)		
Région USA Ouest (Oregon)		
Région Europe (Irlande)		
Tous les autres Régions AWS	3 GiBps	1 GiBps

Demande d'augmentation de quota

Pour demander une augmentation de ces quotas via AWS Support, procédez comme suit. L'équipe Amazon EFS examine chaque demande d'augmentation de quota.

Pour demander une augmentation de quota via AWS Support

1. Ouvrez la page [AWS Support Centre](#) et connectez-vous si nécessaire. Ensuite, choisissez Create Case (Créer une demande).
2. Sous Create case (Créer une demande), choisissez Service Limit Increase (Augmentation de limite de service).
3. Pour Limit Type (Type de limite), choisissez le type de limite à augmenter. Remplissez les champs nécessaires du formulaire, puis choisissez votre méthode de contact préférée.

Les quotas de ressources Amazon EFS que vous ne pouvez pas Modifier

Les quotas de plusieurs ressources Amazon EFS ne peuvent pas être Modifiés, notamment :

- Quotas pour les ressources générales, telles que le nombre de connexions pour chaque système de fichiers.
- Quotas de débit élastiques et provisionnés par système de fichiers One Zone pour tous les clients connectés d'un. Région AWS
- Quotas de débit élevés par système de fichiers régional ou à zone unique pour tous les clients connectés dans un. Région AWS

Le tableau suivant répertorie les quotas de ressources généraux qui ne peuvent pas être modifiés.

Quotas de ressources généraux qui ne peuvent pas être Modifiés

Ressource	Quota
Nombre de connexions pour chaque système de fichiers	25 000
Nombre de cibles de Montage pour chaque système de fichiers d'une Zone de disponibilité	1
Nombre de cibles de Montage pour chaque cloud privé virtuel (VPC)	1 400
Nombre de groupes de sécurité pour chaque cible de Montage	5
Nombre de balises pour chaque système de fichiers	50
Nombre de VPCs pour chaque système de fichiers	1

 Note

Les clients peuvent également se connecter à des cibles de Montage qui se trouvent dans un compte ou un VPC différent de celui du système de fichiers. Pour de plus amples informations, veuillez consulter [Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC](#).

Le tableau suivant répertorie les limites de débit élastiques et provisionnées par défaut totales par système de fichiers pour tous les clients connectés de chaque système de fichiers. Région AWS

Systèmes de fichiers à zone unique : débit élastique et provisionné total par défaut par système de fichiers pour tous les clients connectés de chaque système de fichiers Région AWS

Région AWS	Débit de lecture maximal	Débit d'écriture maximal (débit mesuré)
Tout Régions AWS	3 GiBps	1 GiBps

Le tableau suivant répertorie les limites de débit totales de Bursting par système de fichiers pour tous les clients connectés de chaque système de fichiers. Région AWS

Systèmes de fichiers régionaux et à zone unique : débit total en rafale par système de fichiers pour tous les clients connectés de chaque système de fichiers Région AWS

Région AWS	Débit de lecture maximal	Débit d'écriture maximal
Région US East (Ohio)	5 GiBps	3 GiBps
Région USA Est (Virginie du Nord)		
Région USA Ouest (Oregon)		
Région Asie-Pacifique (Sydney)		
Région Europe (Irlande)		
Tous les autres Régions AWS	3 GiBps	1 GiBps

Quotas pour les clients NFS

Les quotas suivants s'appliquent aux clients NFS, en supposant qu'il s'agit d'un client Linux NFSv4 8.1 :

- Le débit de lecture et d'écriture combiné maximal est de 1 500 mégaoctets par seconde (MiBps) pour les systèmes de fichiers utilisant le débit élastique et montés à l'aide de la version 2.0 ou ultérieure du client Amazon EFS (amazon-efs-utils version) ou du pilote Amazon EFS CSI (. aws-efs-csi-driver Le débit maximal pour tous les autres systèmes de fichiers est de 500 MiBps. Pour

plus d'informations sur les performances, consultez [Récapitulatif des performances](#). Le débit du client NFS représente le nombre total d'octets envoyés et reçus, avec une taille minimale de demande NFS de 4 ko (après application d'un taux de comptage de 1/3 pour les demandes de lecture).

- Jusqu'à 65 536 utilisateurs actifs pour chaque client peuvent avoir des fichiers ouverts en même temps.
- Jusqu'à 65 536 fichiers s'ouvrent simultanément sur l'instance. La création d'une liste de contenu du répertoire n'est pas comptabilisée comme une ouverture de fichier.
- Chaque support unique sur le client peut acquérir jusqu'à 65 536 verrous par connexion.
- Lorsque vous vous connectez à , les clients NFS situés sur site ou dans une autre Région AWS peuvent observer un débit plus faible que lors de la connexion à EFS à partir de la même Région AWS. Cet effet est dû à une latence réseau accrue. Une latence réseau égale ou inférieure à 1 ms est nécessaire pour atteindre un débit maximal par client. Utilisez le service de migration de DataSync données lors de la migration de grands ensembles de données depuis des serveurs NFS locaux vers EFS.
- Le protocole NFS prend en charge un maximum de 16 groupes IDs (GIDs) par utilisateur et tous les groupes supplémentaires GIDs sont tronqués à partir des demandes des clients NFS. Pour de plus amples informations, veuillez consulter [Accès refusé aux fichiers autorisés sur le système de fichiers NFS](#).
- Utilisation d'Amazon EFS avec Microsoft Windows n'est pas prise en charge.

Quotas pour les systèmes de fichiers Amazon EFS

Les quotas suivants sont spécifiques aux systèmes de fichiers Amazon EFS.

Ressource	Quota
Longueur du nom de fichier, en octets	255
Longueur du lien symbolique (symlink), en octets	4 080
Nombre de liens directs vers un fichier	177
Taille maximum d'un seul fichier	52 673 613 135 872 octets (47,9 TiB)
Nombre de niveaux pour la profondeur du répertoire	1 000

Ressource	Quota
Nombre de verrous sur un même fichier pour l'ensemble des instances et des utilisateurs	512
Limite de caractères pour chaque politique de système de fichiers	20 000
*Nombre d'opérations de fichier par seconde pour le mode General Purpose	250 000

*Pour plus d'informations sur le nombre d'opérations de fichier par seconde pour le mode usage général, consultez [Récapitulatif des performances](#).

Fonctionnalités NFSv4 4.0 et 4.1 non prises en charge

Bien qu'Amazon EFS ne NFSv2 prenne pas en charge les versions NFSv4 .1 et NFSv4 .0, à l'exception des fonctionnalités suivantes : NFSv3

- pNFS
- Attributs étendus
- Délégation client ou rappels de tout type
 - L'opération OPEN retourne toujours OPEN_DELEGATE_NONE comme type de délégation.
 - L'opération OPEN retourne NFSERR_NOTSUPP pour CLAIM_DELEGATE_CUR et les types de demande CLAIM_DELEGATE_PREV.
- Verrouillage obligatoire

Tous les verrous dans Amazon EFS sont consultatifs, ce qui signifie que les opérations READ et WRITE ne recherchent pas les verrous en conflit avant l'exécution de l'opération.

- Refus du partage

NFS prend en charge le concept de refus de partage. Le refus de partage est principalement utilisé par les clients Windows pour que les utilisateurs refusent à d'autres l'accès à un fichier particulier qui a été ouvert. Amazon EFS ne prend pas en charge cela et renvoie l'erreur NFS NFS4ERR_NOTSUPP pour toutes les commandes OPEN spécifiant une valeur de refus de

partage autre que `OPEN4_SHARE_DENY_NONE`. Les clients NFS Linux utilisent uniquement `OPEN4_SHARE_DENY_NONE`.

- Listes de contrôle d'accès (ACLs)
- Amazon EFS ne met pas à jour l'attribut `time_access` lors des lectures de fichiers. Amazon EFS met à jour `time_access` lors des événements suivants :
 - Lorsqu'un fichier est créé (un inode est créé).
 - Lorsqu'un client NFS effectue un appel `setattr` explicite.
 - Lors d'une écriture sur l'inode causé par, par exemple, les Modifications de taille de fichier ou les Modifications de métadonnées de fichier.
 - Tout attribut inode est mis à jour.
- Espaces de noms
- Cache de réponse permanent
- Sécurité basée sur Kerberos
- NFSv4.1. Conservation des données
- SetUID sur les répertoires
- Types de fichiers non pris en charge lors de l'utilisation de l'opération `CREATE` : unités de blocs (`NF4BLK`), unités de caractères (`NF4CHR`), répertoire d'attributs (`NF4ATTRDIR`) et attribut nommé (`NF4NAMEDATTR`).
- Attributs non pris en charge : `FATTR4_ARCHIVE`, `FATTR4_FILES_AVAIL`, `FATTR4_FILES_FREE`, `FATTR4_FILES_TOTAL`, `FATTR4_FS_LOCATIONS`, `_MIMETYPE`, `_QUOTA_AVAIL_HARD`, `_QUOTA_AVAIL_SOFT`, `_QUOTA_USED`, `_TIME_BACKUP` et `_ACL`.
`FATTR4 FATTR4 FATTR4 FATTR4 FATTR4 FATTR4`

Une tentative de définition de ces attributs entraîne une erreur `NFS4ERR_ATTRNOTSUPP` qui est renvoyée au client.

Considérations supplémentaires

En outre, notez les éléments suivants :

- Pour obtenir une liste des emplacements Régions AWS dans lesquels vous pouvez créer des systèmes de fichiers Amazon EFS, consultez le [guide de Références générales AWS l'utilisateur](#).
- Amazon EFS ne prend pas en charge l'option de Montage `nconnect`.

- Vous pouvez Monter un système de fichiers à partir de serveurs de centre de données sur site à l'aide de AWS Direct Connect et VPN. Pour de plus amples informations, veuillez consulter [Tutoriel : Montage avec des clients locaux](#).

Résolution des erreurs de fonctionnement des fichiers liées aux quotas

Lorsque vous accédez aux systèmes de fichiers EFS, certaines limites s'appliquent aux fichiers du système de fichiers. Un dépassement de ces limites entraîne des erreurs d'opérations sur les fichiers. Pour plus d'informations sur les limites basées sur les fichiers dans Amazon EFS, consultez [Quotas Amazon EFS](#).

Vous trouverez ci-après certaines erreurs courantes d'opérations sur les fichiers et les limites associées à chaque erreur.

Rubriques

- [Échec de la commande avec l'erreur « Quota de disque dépassé »](#)
- [Échec de la commande avec l'erreur « Erreur d'E/S »](#)
- [Échec de la commande avec l'erreur « Le nom de fichier est trop long »](#)
- [Échec de la commande avec l'erreur « Fichier introuvable »](#)
- [Échec de la commande avec l'erreur « Trop de liens »](#)
- [Échec de la commande avec l'erreur « Fichier trop volumineux »](#)

Échec de la commande avec l'erreur « Quota de disque dépassé »

Amazon EFS ne prend pas en charge actuellement les quotas de disque utilisateur. Cette erreur peut se produire si les limites suivantes ont été dépassées :

- Jusqu'à 65 536 utilisateurs actifs peuvent ouvrir des fichiers en même temps. Un compte utilisateur connecté plusieurs fois est comptabilisé comme un seul utilisateur actif.
- Jusqu'à 65 536 fichiers peuvent être ouverts simultanément pour une instance. La création d'une liste de contenu du répertoire n'est pas comptabilisée comme une ouverture de fichier.
- Chaque support unique sur le client peut acquérir jusqu'à 65 536 verrous par connexion.

Action à exécuter

Si vous rencontrez ce problème, vous pouvez le résoudre en identifiant quelles limites parmi les susmentionnées vous dépassez, puis en apportant les modifications nécessaires pour respecter cette limite. Pour de plus amples informations, veuillez consulter [Quotas pour les clients NFS](#).

Échec de la commande avec l'erreur « Erreur d'E/S »

Cette erreur se produit pour l'une des raisons suivantes :

- Plus de 65 536 comptes utilisateurs actifs pour chaque instance ont des fichiers ouverts en même temps.

Action à exécuter

Si vous rencontrez ce problème, vous pouvez le résoudre en respectant les limites prises en charge pour les fichiers ouverts sur vos instances. Pour ce faire, réduisez le nombre d'utilisateurs actifs ayant des fichiers de votre système de fichiers Amazon EFS ouverts simultanément sur vos instances.

- La AWS KMS clé chiffrant votre système de fichiers a été supprimée.

Action à exécuter

Si vous rencontrez ce problème, vous ne pouvez plus déchiffrer les données qui ont été chiffrées sous cette clé, ce qui signifie que les données deviennent irrécupérables.

Échec de la commande avec l'erreur « Le nom de fichier est trop long »

Cette erreur se produit lorsque la taille d'un nom de fichier est trop importante ou que son lien symbolique (symlink) est trop long. Les noms de fichiers ont les limites suivantes :

- Un nom peut compter jusqu'à 255 octets.
- Un symlink peut compter jusqu'à 4 080 octets.

Action à exécuter

Si vous rencontrez ce problème, vous pouvez le résoudre en réduisant la taille du nom de fichier ou la longueur du symlink, afin de respecter les limites prises en charge.

Échec de la commande avec l'erreur « Fichier introuvable »

Cette erreur se produit car certaines anciennes versions 32 bits d'Oracle E-Business Suite utilisent des interfaces d'E/S de fichiers 32 bits, et EFS utilise des numéros d'inode 64 bits. ``stat ()`` et ``readdir ()`` sont des appels système qui peuvent échouer.

Action à exécuter

Si vous rencontrez cette erreur, vous pouvez la résoudre à l'aide de l'option de démarrage `nfs.enable_ino64=0` kernel. Cette option compresse les numéros d'inode EFS 64 bits en 32 bits. Les options de démarrage du noyau sont gérées différemment pour les différentes distributions Linux. Sur Amazon Linux, activez cette option en ajoutant `nfs.enable_ino64=0 kernel` à la variable `GRUB_CMDLINE_LINUX_DEFAULT` dans `/etc/default/grub`. Veuillez consulter votre distribution pour obtenir une documentation spécifique sur la façon d'activer les options de démarrage du noyau.

Échec de la commande avec l'erreur « Trop de liens »

Cette erreur se produit lorsqu'il y a trop de liens physiques vers un fichier. Vous pouvez avoir jusqu'à 177 liens physiques dans un fichier.

Action à exécuter

Si vous rencontrez ce problème, vous pouvez le résoudre en réduisant le nombre de liens physiques dans un fichier afin de respecter à la limite prise en charge.

Échec de la commande avec l'erreur « Fichier trop volumineux »

Cette erreur se produit lorsqu'un fichier est trop volumineux. Un fichier peut atteindre la taille de 47.9 673 613 135 872 octets (TiB).

Action à exécuter

Si vous rencontrez ce problème, vous pouvez le résoudre en réduisant la taille du fichier afin de respecter la limite prise en charge.

API Amazon EFS

L'API Amazon EFS est un protocole réseau basé sur [HTTP \(RFC 2616\)](#). Pour chaque appel d'API, vous envoyez une requête HTTP au point de terminaison d'API Amazon EFS spécifique à la région pour savoir Région AWS où vous souhaitez gérer les systèmes de fichiers. L'API utilise des documents JSON (RFC 4627) pour les corps de requête/réponse HTTP.

L'API Amazon EFS est un modèle RPC. Dans ce modèle, il existe un ensemble fixe d'opérations et la syntaxe de chaque opération est connue des clients sans aucune interaction préalable. Dans la section suivante, vous pouvez trouver une description de chaque opération d'API à l'aide d'une notation RPC abstraite. Chacune a un nom d'opération qui n'apparaît pas dans le transfert. Pour chaque opération, la rubrique spécifie le mapping d'éléments de requête HTTP.

L'opération Amazon EFS spécifique à laquelle est mappée une requête donnée est déterminée par une combinaison de la méthode de la demande (GET, PUT, POST ou DELETE) et de la correspondance de Request-URI avec l'un des différents modèles. Si l'opération est PUT ou POST, Amazon EFS extrait les arguments d'appel du segment de chemin Request-URI, les paramètres de requête, ainsi que l'objet JSON dans le corps de la requête.

Note

Bien que les noms des opérations `CreateFileSystem`, tels que, n'apparaissent pas sur le fil, ils ont une signification dans les politiques AWS Identity and Access Management (IAM). Pour de plus amples informations, veuillez consulter [Gestion des identités et des accès pour Amazon EFS](#).

Le nom de l'opération est également utilisé pour nommer les commandes dans les outils de ligne de commande et les éléments du AWS SDK. APIs Par exemple, il existe une AWS CLI commande nommée `create-file-system` qui correspond à l'`CreateFileSystem` opération.

Le nom de l'opération apparaît également dans AWS CloudTrail les journaux des appels d'API Amazon EFS.

Points de terminaison d'API

Un point de terminaison est une URL qui sert de point d'entrée à un service AWS Web. Amazon EFS prend en charge les types de terminaux suivants :

- IPv4 points de terminaison
- Points de terminaison à double pile (à IPv4 la fois IPv6)
- [Points de terminaison FIPS](#)

Lorsque vous faites une demande, vous pouvez spécifier le point de terminaison à utiliser. Si vous ne spécifiez aucun point de IPv4 terminaison, celui-ci est utilisé par défaut. Pour utiliser un autre type de point de terminaison, vous devez le spécifier dans votre demande. Pour obtenir un exemple de la façon de procéder, consultez [Spécification des points de terminaison](#). Pour un tableau des points de terminaison disponibles, consultez la section Points de [terminaison et quotas Amazon EFS](#).

IPv4 points de terminaison

IPv4 les terminaux ne prennent en charge que IPv4 le trafic. IPv4 les points de terminaison sont disponibles pour toutes les régions. Le format du IPv4 point de terminaison dépend de la région.

- Pour les IPv4 terminaux situés dans les régions AWS commerciales, le format `elasticfilesystem.region.amazonaws.com`.

Par exemple, si vous le spécifiez `elasticfilesystem.us-west-2.amazonaws.com` comme point de terminaison, nous dirigeons votre demande vers le point de terminaison de la région USA Ouest (Oregon) (us-west-2).

- Pour les IPv4 points de terminaison situés dans les régions de Chine, le format `elasticfilesystem.region.amazonaws.com.cn`.

Par exemple, le point de terminaison de l'API Amazon EFS pour la région de Chine (Pékin) `elasticfilesystem.cn-north-1.amazonaws.com.cn`.

Points de terminaison à double pile (IPv4 et IPv6)

Les terminaux à double pile prennent en charge à la fois le trafic IPv4 et IPv6 le trafic. Lorsque vous envoyez une demande à un point de terminaison à double pile, l'URL du point de terminaison correspond à une IPv4 adresse IPv6 ou à une adresse, selon le protocole utilisé par votre réseau et votre client. Le format du point de terminaison à double pile dépend de la région.

- Pour les points de terminaison à double pile dans les régions AWS commerciales, le format est. `efs.aws-region.api.aws`

Par exemple, le point de terminaison à double pile pour la région USA Ouest (Oregon) (us-west-2) est `efs.eu-west-2.api.aws`

- Pour les points de terminaison à double pile dans les régions de Chine, le format est `efs.region.api.amazonaws.com.cn`

Par exemple, le point de terminaison à double pile pour la région de Chine (Pékin) est `efs.cn-north-1.api.amazonaws.com.cn`.

Spécification des points de terminaison

Les exemples suivants montrent comment spécifier un point de terminaison pour la région USA Ouest (Californie du Nord) (us-west-1) à l'aide du pour Amazon EFS. AWS CLI

IPv4

```
aws efs get-rest-apis --region us-west-1 --endpoint-url https://elasticfilesystem.us-west-1.amazonaws.com
```

Double pile

```
aws efs get-rest-apis --region us-west-1 --endpoint-url https://efs.us-west-1.api.aws
```

Version de l'API

La version de l'API utilisée pour un appel est identifiée par le premier segment de chemin de l'URI de la demande, et sa forme est une date ISO 8601. Pour obtenir un exemple, consultez [CreateFileSystem](#).

La documentation décrit l'API version 2015-02-01.

Rubriques en relation

Les sections suivantes fournissent des descriptions d'opérations d'API, indiquent comment créer une signature pour l'authentification de la requête et comment accorder des autorisations pour ces opérations d'API à l'aide de stratégies IAM.

- [Gestion des identités et des accès pour Amazon EFS](#)

- [Actions](#)
- [Types de données](#)

Utilisation du débit de demandes d'API de requête pour Amazon EFS

Les demandes d'API Amazon EFS sont limitées pour chaque Compte AWS région afin d'améliorer les performances du service. Tous les appels d'API Amazon EFS effectués ensemble, qu'ils proviennent d'une application, de la AWS CLI console Amazon EFS ou de la console Amazon EFS, ne doivent pas dépasser le taux de demandes d'API maximal autorisé. Le taux maximal de demandes d'API peut varier d'un pays à l'autre Régions AWS. Les demandes d'API effectuées sont attribuées au sous-jacent Compte AWS.

Si une demande d'API dépasse le taux de demandes d'API pour sa catégorie, la demande renvoie le code d'erreur `ThrottlingException`. Pour éviter cette erreur, assurez-vous que votre application n'effectue pas de nouvelles tentatives de demandes d'API à un taux élevé. Vous pouvez le faire en utilisant l'interrogation avec soin et en utilisant les tentatives d'interruption exponentielle.

Interrogation

Votre application peut avoir besoin d'appeler une opération d'API de façon répétée pour vérifier une mise à jour du statut. Avant de démarrer l'interrogation, indiquez la durée potentielle de la demande. Lorsque vous commencez l'interrogation, utilisez un intervalle de veille approprié entre les demandes successives. Pour obtenir de meilleurs résultats, utilisez un intervalle de veille croissant.

Nouvelles tentatives ou traitement par lots

Votre application peut avoir besoin de relancer une demande d'API après un échec ou de traiter plusieurs ressources (par exemple, l'ensemble de vos systèmes de fichiers Amazon EFS). Pour réduire le taux de demandes d'API, utilisez un intervalle de veille approprié entre les demandes successives. Pour obtenir de meilleurs résultats, utilisez un intervalle de veille croissant ou variable.

Calcul de l'intervalle de veille

Lorsque vous devez interroger ou relancer une demande d'API, nous vous recommandons d'utiliser un algorithme d'interruption exponentielle pour calculer l'intervalle de sommeil entre les appels d'API. L'idée sous-jacente consiste à utiliser des temps d'attente progressivement plus longs entre

les tentatives en cas de réponses d'erreur consécutives. Pour plus d'informations et des exemples d'implémentation de cet algorithme, consultez la section [Comportement de la nouvelle tentative](#) dans le Référence générale d'Amazon Web Services.

Actions

Les actions suivantes sont prises en charge :

- [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

Crée un point d'accès EFS. Un point d'accès est une vue spécifique à l'application dans un système de fichiers EFS qui applique un utilisateur et un groupe de système d'exploitation, ainsi qu'un chemin d'accès au système de fichiers, à toute demande de système de fichiers effectuée via le point d'accès. L'utilisateur et le groupe du système d'exploitation remplacent toutes les informations d'identité fournies par le client NFS. Le chemin d'accès du système de fichiers est exposé en tant que répertoire racine du point d'accès. Les applications qui utilisent le point d'accès ne peuvent accéder qu'aux données de leur propre répertoire et de leurs éventuels sous-répertoires. Un système de fichiers peut avoir un maximum de 10 000 points d'accès, sauf si vous demandez une augmentation. Pour plus d'informations, veuillez consulter la rubrique [Montage d'un système de fichiers à l'aide de points d'accès EFS](#).

Note

Si plusieurs demandes de création de points d'accès sur le même système de fichiers sont envoyées en succession rapide et que le système de fichiers est proche de la limite des points d'accès, il est possible que la réponse à ces demandes soit limitée. Cela permet de garantir que le système de fichiers ne dépasse pas le quota de points d'accès indiqué.

Cette opération exige des autorisations pour l'action `elasticfilesystem:CreateAccessPoint`.

Les points d'accès peuvent être balisés lors de leur création. Si les balises sont spécifiées dans l'action de création d'action, IAM effectue une autorisation supplémentaire sur l'action `elasticfilesystem:TagResource` pour vérifier si les utilisateurs sont autorisés à créer des balises. Par conséquent, vous devez octroyer des autorisations explicites d'utiliser l'action `elasticfilesystem:TagResource`. Pour plus d'informations, consultez [Octroi d'autorisations pour baliser les ressources lors de la création](#).

Syntaxe de la demande

```
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"
    }
  ]
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

ClientToken

Chaîne de 64 caractères ASCII maximum utilisée par Amazon EFS pour garantir une création idempotente.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : .+

Obligatoire : oui

FileSystemId

ID du système de fichiers EFS auquel le point d'accès donne un accès.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

PosixUser

L'utilisateur et le groupe du système d'exploitation appliqués à toutes les demandes de système de fichiers effectuées via le point d'accès.

Type : objet [PosixUser](#)

Obligatoire : non

RootDirectory

Détermine le répertoire du système de fichiers EFS que le point d'accès expose en tant que répertoire racine de votre système de fichiers aux clients NFS utilisant le point d'accès. Les clients utilisant le point d'accès peuvent uniquement accéder au répertoire racine et en dessous. Si le `RootDirectory > Path` spécifié n'existe pas, Amazon EFS le crée et applique les paramètres `CreationInfo` lorsqu'un client se connecte à un point d'accès. Lorsque vous spécifiez un `RootDirectory`, vous devez fournir le `Path`, et le `CreationInfo`.

Amazon EFS crée un répertoire racine uniquement si vous avez fourni le `CreationInfo : OwnUid`, le `OwnGid` et les autorisations pour le répertoire. Si vous ne fournissez pas ces informations, Amazon EFS ne crée pas le répertoire racine. Si le répertoire racine n'existe pas, les tentatives de Montage au Moyen du point d'accès échoueront.

Type : objet [RootDirectory](#)

Obligatoire : non

Tags

Crée des balises associées au point d'accès. Chaque balise est une paire clé-valeur, chaque clé doit être unique. Pour plus d'informations, consultez la section [AWS Ressources relatives au balisage](#) dans le Guide de référence AWS général.

Type : tableau d'objets [Tag](#)

Obligatoire : non

Syntaxe de la réponse

```
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"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AccessPointArn](#)

Le Amazon Resource Name (ARN) unique associé au point d'accès.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}$`

[AccessPointId](#)

L'ID du point d'accès, attribué par Amazon EFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

[ClientToken](#)

Chaîne opaque spécifiée dans la demande pour garantir la création idempotente.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `.+`

[FileSystemId](#)

ID du système de fichiers EFS auquel le point d'accès s'applique.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[LifeCycleState](#)

Identifie la phase du cycle de vie du point d'accès.

Type : String

Valeurs valides : `creating | available | updating | deleting | deleted | error`

Name

Nom de ce point d'accès. Il s'agit de la valeur de la balise Name.

Type : String

OwnerId

Identifie Compte AWS le propriétaire de la ressource du point d'accès.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : $^(\backslash d\{12\}) | (\backslash d\{4\} - \backslash d\{4\} - \backslash d\{4\})\$$

PosixUser

L'identité POSIX complète, y compris l'ID utilisateur, l'ID de groupe et le groupe secondaire IDs sur le point d'accès utilisé pour toutes les opérations sur les fichiers par les clients NFS utilisant le point d'accès.

Type : objet [PosixUser](#)

RootDirectory

Répertoire du système de fichiers Amazon EFS que le point d'accès expose en tant que répertoire racine aux clients NFS utilisant le point d'accès.

Type : objet [RootDirectory](#)

Tags

Les balises associées au point d'accès, présentées sous la forme d'un tableau d'objets Tag.

Type : tableau d'objets [Tag](#)

Erreurs

AccessPointAlreadyExists

Renvoyé si le point d'accès que vous essayez de créer existe déjà, avec le jeton de création que vous avez fourni dans la demande.

Code d'état HTTP : 409

AccessPointLimitExceeded

Renvoyé si le Compte AWS nombre maximum de points d'accès autorisés par système de fichiers a déjà été créé. Pour en savoir plus, consultez <https://docs.aws.amazon.com/efs/latest/ug/limits.html#limits-efs-resources-per-account-per-region>.

Code d'état HTTP : 403

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la FileSystemId valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifecycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

ThrottlingException

Renvoyé lorsque l'action CreateAccessPoint API est appelée trop rapidement et que le nombre de points d'accès sur le système de fichiers approche de la [limite de 120](#).

Code d'état HTTP : 429

Voir aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateFileSystem

Crée un nouveau système de fichiers vide. L'opération exige un jeton de création dans la demande qui est utilisé par Amazon EFS pour garantir la création idempotente (appeler l'opération avec le même jeton de création n'a aucun effet). S'il n'existe pas actuellement de système de fichiers appartenant à l'appelant Compte AWS avec le jeton de création spécifié, cette opération effectue les opérations suivantes :

- Crée un nouveau système de fichiers vide. Le système de fichiers possède un ID attribué par Amazon EFS ainsi qu'un état du cycle de vie initial `creating`.
- Retourne avec la description du système de fichiers créé.

Sinon, cette opération retourne une erreur `FileSystemAlreadyExists` avec l'ID du système de fichiers existant.

Note

Pour les cas d'utilisation de base, vous pouvez utiliser un UUID généré de façon aléatoire pour le jeton de création.

L'opération idempotente vous permet de relancer un appel `CreateFileSystem` sans risque de créer un système de fichiers supplémentaire. Cela peut se produire lorsqu'un appel initial échoue sans que vous puissiez savoir si un système de fichiers a été créé ou non. Par exemple, un délai d'attente au niveau du transport ou la réinitialisation de votre connexion. Tant que vous utilisez le même jeton de création, si l'appel initial a réussi à créer un système de fichiers, le client peut découvrir de son existence à partir de l'erreur `FileSystemAlreadyExists`.

Pour plus d'informations, consultez [Création d'un système de fichiers](#) dans le Guide de l'utilisateur Amazon EFS.

Note

L'appel `CreateFileSystem` se termine, tandis que l'état du cycle de vie du système de fichiers est toujours au statut `creating`. Vous pouvez vérifier le statut de création du système de fichiers en appelant l'opération [DescribeFileSystems](#) qui retourne l'état du système de fichiers, entre autres.

Cette opération accepte également un paramètre `PerformanceMode` facultatif que vous choisissez pour votre système de fichiers. Nous le recommandons `generalPurpose` `PerformanceMode` pour tous les systèmes de fichiers. Le `maxIO` mode est un type de performance de génération précédente conçu pour les charges de travail hautement parallélisées qui peuvent tolérer des latences plus élevées que le mode. `generalPurpose` `MaxIO` le mode n'est pas pris en charge pour les systèmes de fichiers `One Zone` ou les systèmes de fichiers qui utilisent le débit élastique.

Il ne `PerformanceMode` peut pas être modifié une fois le système de fichiers créé. Pour plus d'informations, consultez [Amazon EFS : modes de performances](#).

Vous pouvez définir le mode de débit du système de fichiers à l'aide du paramètre `ThroughputMode`.

Une fois le système de fichiers entièrement créé, Amazon EFS définit son état du un cycle de vie `available`, après quoi vous pouvez créer une ou plusieurs cibles de Montage pour le système de fichiers de votre VPC. Pour de plus amples informations, veuillez consulter [CreateMountTarget](#). Vous montez votre système de fichiers Amazon EFS sur une EC2 instance de votre VPC à l'aide de la cible de montage. Pour plus d'informations, consultez [Fonctionnement d'Amazon EFS](#).

Cette opération exige des autorisations pour l'action `elasticfilesystem:CreateFileSystem`.

Les systèmes de fichiers peuvent être étiquetés lors de leur création. Si les balises sont spécifiées dans l'action de création d'action, IAM effectue une autorisation supplémentaire sur l'action `elasticfilesystem:TagResource` pour vérifier si les utilisateurs sont autorisés à créer des balises. Par conséquent, vous devez octroyer des autorisations explicites d'utiliser l'action `elasticfilesystem:TagResource`. Pour plus d'informations, consultez [Octroi d'autorisations pour baliser les ressources lors de la création](#).

Syntaxe de la demande

```
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"  
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[AvailabilityZoneName](#)

Pour les systèmes de fichiers One Zone, spécifiez la zone de AWS disponibilité dans laquelle créer le système de fichiers. Utilisez le format `us-east-1a` pour spécifier la Zone de disponibilité. Pour plus d'informations sur les systèmes de fichiers One Zone, consultez la section [Types de systèmes de fichiers EFS](#) dans le guide de l'utilisateur Amazon EFS.

Note

Les systèmes de fichiers One Zone ne sont pas disponibles dans toutes les zones de disponibilité dans Régions AWS lesquelles Amazon EFS est disponible.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : .+

Obligatoire : non

[Backup](#)

Spécifie si les sauvegardes automatiques sont activées sur le système de fichiers que vous créez. Définissez la valeur sur `true` pour activer les sauvegardes automatiques. Si vous créez

un système de fichiers Zone unique, les sauvegardes automatiques sont activées par défaut. Pour plus d'informations, consultez [Sauvegardes automatiques](#) dans le Guide de l'utilisateur Amazon EFS.

La valeur par défaut est `false`. Toutefois, si vous spécifiez un `AvailabilityZoneName`, la valeur par défaut est `true`.

 Note

AWS Backup n'est pas disponible dans tous les Régions AWS pays où Amazon EFS est disponible.

Type : booléen

Obligatoire : non

CreationToken

Chaîne de maximum 64 caractères ASCII. Amazon EFS l'utilise pour garantir la création idempotente.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `.+`

Obligatoire : oui

Encrypted

Une valeur booléenne qui, si elle est vraie, crée un système de fichiers chiffré. Lorsque vous créez un système de fichiers chiffré, vous avez la possibilité de spécifier une AWS Key Management Service clé existante (clé KMS). Si vous ne spécifiez pas de clé KMS, la clé KMS par défaut pour Amazon EFS, `/aws/elasticfilesystem`, est utilisée pour protéger le système de fichiers chiffré.

Type : booléen

Obligatoire : non

KmsKeyId

L'ID de la clé KMS que vous souhaitez utiliser pour protéger le système de fichiers crypté. Ce paramètre est obligatoire uniquement si vous souhaitez utiliser une clé KMS personnalisée. Si ce paramètre n'est pas spécifié, la clé KMS par défaut pour Amazon EFS est utilisée. Vous pouvez spécifier un ID de clé KMS en utilisant les formats suivants :

- ID de clé - Identifiant unique de la clé, par exemple `1234abcd-12ab-34cd-56ef-1234567890ab`.
- ARN - Amazon Resource Name (ARN) pour la clé, par exemple `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- Alias de clé - Un nom d'affichage précédemment créé pour une clé, par exemple `alias/projectKey1`.
- ARN d'alias de clé - ARN pour un alias de clé, par exemple `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`.

Si vous l'utilisez `KmsKeyId`, vous devez définir le paramètre `Encrypted` sur [CreateFileSystemtrue](#).

Important

EFS n'accepte que les clés KMS symétriques. Vous ne pouvez pas utiliser de clés KMS asymétriques avec les systèmes de fichiers Amazon EFS.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^([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/_-]+))))$`

Obligatoire : non

PerformanceMode

Mode de performances du système de fichiers. Nous recommandons le mode `performanceGeneralPurpose` pour tous les systèmes de fichiers. Les systèmes de fichiers utilisant le mode de performance `maxIO` peuvent évoluer vers des niveaux plus élevés de débit cumulé et

d'opérations par seconde avec comme contrepartie des latences légèrement plus élevées pour la plupart des opérations de fichier. Le mode de performances ne peut pas être Modifié une fois que le système de fichiers a été créé. Le mode maxIO n'est pas pris en charge sur les systèmes de fichiers utilisant des classes de stockage Zone unique.

 Important

En raison des latences par opération plus élevées avec Max E/S, nous recommandons d'utiliser le mode de performance Usage général pour tous les systèmes de fichiers.

La valeur par défaut est `generalPurpose`.

Type : String

Valeurs valides : `generalPurpose` | `maxIO`

Obligatoire : non

[ProvisionedThroughputInMibps](#)

Débit, mesuré en mébiotets par seconde (MiBps), que vous souhaitez allouer au système de fichiers que vous créez. Obligatoire si `ThroughputMode` est défini sur `provisioned`. Les valeurs valides sont comprises entre 1 et 3414 MiBps, la limite supérieure dépendant de la région. Pour augmenter cette limite, contactez Support. Pour plus d'informations, consultez [Quotas Amazon EFS que vous pouvez augmenter](#) dans le Guide de l'utilisateur Amazon EFS.

Type : double

Plage valide : valeur minimum de 1,0.

Obligatoire : non

[Tags](#)

Utilisez cette valeur pour créer une ou plusieurs balises associées au système de fichiers. Chaque balise est une paire clé-valeur définie par l'utilisateur. Nommez votre système de fichiers au moment de la création en incluant une paire clé-valeur `"Key": "Name", "Value": "{value}"`. Chaque clé doit être unique. Pour plus d'informations, consultez la section [AWS Ressources relatives au balisage](#) dans le Guide de référence AWS général.

Type : tableau d'objets [Tag](#)

Obligatoire : non

[ThroughputMode](#)

Spécifie le mode de débit du système de fichiers. Il peut s'agir du mode `bursting`, `provisioned` ou `elastic`. Si vous définissez `ThroughputMode` sur `provisioned`, vous devez également définir une valeur pour `ProvisionedThroughputInMibps`. Après avoir créé le système de fichiers, vous pouvez réduire son débit en mode Débit alloué ou passer d'un mode de débit à l'autre, avec certaines restrictions de temps. Pour de plus amples informations, consultez [Spécification du débit avec le mode alloué](#) dans le Guide de l'utilisateur Amazon EFS.

La valeur par défaut est `bursting`.

Type : String

Valeurs valides : `bursting` | `provisioned` | `elastic`

Obligatoire : non

Syntaxe de la réponse

```
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"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

AvailabilityZoneId

Identifiant unique et cohérent de la Zone de disponibilité dans laquelle se trouve le système de fichiers, valide uniquement pour les systèmes de fichiers Zone unique. Par exemple, use1-az1 il s'agit d'un identifiant de zone de disponibilité pour le Région AWS us-east-1, qui possède le même emplacement dans chaque cas. Compte AWS

Type : String

AvailabilityZoneName

Décrit la zone de AWS disponibilité dans laquelle se trouve le système de fichiers et n'est valide que pour les systèmes de fichiers One Zone. Pour de plus amples informations, consultez [Utilisation de classes de stockage EFS](#) dans le Guide de l'utilisateur Amazon EFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : .+

CreationTime

Heure de création du système de fichiers, en secondes (depuis 1970-01-01T 00:00:00 Z).

Type : Timestamp

CreationToken

Chaîne opaque spécifiée dans la demande.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : . +

Encrypted

Valeur booléenne qui, si la valeur est true, indique que le système de fichiers est chiffré.

Type : booléen

FileSystemArn

Le nom de ressource Amazon Resource Name (ARN) pour le système de fichiers EFS, au format `arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id`. Exemple avec des exemples de données : `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Type : String

FileSystemId

ID du système de fichiers, attribué par Amazon EFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

FileSystemProtection

Décrit la protection du système de fichiers.

Type : objet [FileSystemProtectionDescription](#)

[KmsKeyId](#)

Identifiant AWS KMS key utilisé pour protéger le système de fichiers chiffré.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^([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](#)

Phase du cycle de vie du système de fichiers.

Type : String

Valeurs valides : `creating | available | updating | deleting | deleted | error`

[Name](#)

Vous pouvez ajouter des balises à un système de fichiers, y compris une balise Name. Pour de plus amples informations, veuillez consulter [CreateFileSystem](#). Si le système de fichiers possède une balise Name, Amazon EFS renvoie la valeur dans ce champ.

Type : String

Contraintes de longueur : longueur maximale de 256.

Modèle : `^([\p{L}\p{Z}\p{N}_./=+\-@]*)$`

[NumberOfMountTargets](#)

Le nombre actuel de cibles de Montage du système de fichiers. Pour de plus amples informations, veuillez consulter [CreateMountTarget](#).

Type : entier

Plage valide : Valeur minimum de 0.

OwnerId

Celui Compte AWS qui a créé le système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : `^\d{12})|(\d{4}-\d{4}-\d{4})$`

PerformanceMode

Mode de performances du système de fichiers.

Type : String

Valeurs valides : `generalPurpose` | `maxIO`

ProvisionedThroughputInMibps

Quantité de débit allouée, mesurée en MiBps, pour le système de fichiers. Valable pour les systèmes de fichiers utilisant `ThroughputMode` défini sur `provisioned`.

Type : double

Plage valide : Valeur minimum de 1,0.

SizeInBytes

La dernière taille mesurée connue (en octets) des données stockées dans le système de fichiers, dans son champ `Value`, et l'heure à laquelle cette taille a été déterminée dans son champ `Timestamp`. La valeur `Timestamp` est le nombre entier de secondes écoulées depuis 1970-01-01T 00:00:00 Z. La valeur `SizeInBytes` ne représente pas la taille d'un instantané cohérent du système de fichiers, mais elle est finalement cohérente lorsqu'aucune écriture n'est effectuée dans le système de fichiers. Cela signifie que `SizeInBytes` représente la taille réelle uniquement si le système de fichiers n'est pas Modifié pendant une période supérieure à deux heures. Dans le cas contraire, la valeur ne correspond pas exactement à la taille du système de fichiers à un Moment donné.

Type : objet [FileSystemSize](#)

Tags

Tags associés au système de fichiers, présentés sous forme de tableau des objets Tag.

Type : tableau d'objets [Tag](#)

[ThroughputMode](#)

Affiche le mode de débit du système de fichiers. Pour plus d'informations, consultez les [Modes de débit](#) dans le Guide de l'utilisateur Amazon EFS.

Type : String

Valeurs valides : `bursting` | `provisioned` | `elastic`

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemAlreadyExists

Renvoyé si le système de fichiers que vous essayez de créer existe déjà, avec le jeton de création que vous avez fourni.

Code d'état HTTP : 409

FileSystemLimitExceeded

Renvoie si le nombre maximum de systèmes de fichiers autorisés par compte Compte AWS a déjà été créé.

Code d'état HTTP : 403

InsufficientThroughputCapacity

Renvoyé si la capacité est insuffisante pour fournir un débit supplémentaire. Cette valeur peut être renvoyée lorsque vous essayez de créer un système de fichiers en mode débit alloué, lorsque vous essayez d'augmenter le débit alloué d'un système de fichiers existant ou lorsque vous essayez de faire passer un système de fichiers existant du mode débit en rafale au mode débit alloué. Réessayez ultérieurement.

HTTP Status Code: 503

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

ThroughputLimitExceeded

Renvoie si le mode de débit ou la quantité de débit alloué ne peuvent pas être Modifiés car la limite de débit de 1024 Mbits/s a été atteinte.

Code d'état HTTP : 400

UnsupportedAvailabilityZone

Renvoyé si la fonctionnalité Amazon EFS demandée n'est pas disponible dans la Zone de disponibilité spécifiée.

Code d'état HTTP : 400

Exemples

Créez d'un système de fichiers EFS

L'exemple suivant envoie une requête POST pour créer un système de fichiers dans la région us-west-2 avec les sauvegardes automatiques activées. La demande est spécifiée `myFileSystem1` comme jeton de création pour l'idempotencie.

Exemple de demande

```
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"
    }
]
```

Exemple de réponse

```
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"
}
```

Créer un système de fichiers EFS chiffré avec disponibilité de Zone unique

L'exemple suivant envoie une requête POST pour créer un système de fichiers dans la région us-west-2 avec les sauvegardes automatiques activées. Le système de fichiers disposera d'un espace de stockage Zone unique dans la zone de us-west-2b disponibilité .

Exemple de demande

```
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"
    }
  ]
}
```

Exemple de réponse

```
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"  
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateMountTarget

Crée une cible de montage pour un système de fichiers. Vous pouvez ensuite monter le système de fichiers sur des EC2 instances à l'aide de la cible de montage. Pour plus d'informations sur les cibles de montage, consultez [la section Gestion des cibles de montage](#).

Pour créer une cible de montage pour un système de fichiers EFS, l'état du cycle de vie du système de fichiers doit être `available`. Pour de plus amples informations, veuillez consulter [DescribeFileSystems](#).

Après avoir créé la cible de montage, Amazon EFS renvoie une réponse qui inclut une `MountTargetId` et une adresse IP (`IpAddress` ou `Ipv6Address`). Vous utilisez cette adresse IP lors du montage du système de fichiers dans une EC2 instance. Vous pouvez également utiliser le nom DNS de la cible de montage lors du montage du système de fichiers. L'EC2 instance sur laquelle vous montez le système de fichiers à l'aide de la cible de montage peut convertir le nom DNS de la cible de montage en adresse IP. Pour plus d'informations, consultez [Comment fonctionne Amazon EFS](#).

Notez que vous pouvez créer des cibles de montage pour un système de fichiers dans un seul VPC, et qu'il ne peut y avoir qu'une seule cible de montage par Zone de disponibilité. Pour plus d'informations, consultez la section [Création de cibles de montage](#).

Si la demande répond aux exigences, Amazon EFS procède comme suit :

- Il crée une cible de montage dans le sous-réseau spécifié.
- Crée une nouvelle interface réseau dans le sous-réseau avec les éléments suivants :
 - Description Mount target `fsmt-id` for file system `fs-id` où se `fsmt-id` trouve l'ID de la cible de montage, et où `fs-id` est le `FileSystemId`.
 - `requesterManaged` propriété de l'interface réseau définie sur `true` et `requesterId` valeur définie sur EFS.

Chaque cible de montage possède une interface EC2 réseau gérée par le demandeur correspondante. Une fois l'interface réseau créée, Amazon EFS définit le `NetworkInterfaceId` champ de la description de la cible de montage sur l'ID de l'interface réseau et son adresse IP sur son adresse. En cas d'échec de la création de l'interface réseau, l'opération `CreateMountTarget` entière échoue.

 Note

L'appel `CreateMountTarget` se termine seulement après la création de l'interface réseau, mais tant que l'état de la cible de montage est `creating`, vous pouvez vérifier le statut de création de la cible de montage en appelant l'opération [DescribeMountTargets](#), ce qui retourne l'état de la cible de montage, entre autres.

Cette opération exige des autorisations pour l'action suivante sur le système de fichiers :

- `elasticfilesystem:CreateMountTarget`

Cette opération nécessite également des autorisations pour les EC2 actions Amazon suivantes :

- `ec2:DescribeSubnets`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`

Syntaxe de la demande

```
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"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

FileSystemId

ID du système de fichiers pour lequel créer la cible de montage.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

IpAddress

Si la cible `IpAddressType` de montage est IPv4 (`IPV4_ONLY` ou `DUAL_STACK`), spécifiez l'IPv4 adresse à utiliser. Si vous ne spécifiez pas `IpAddress`, Amazon EFS sélectionne une adresse IP non utilisée dans le sous-réseau spécifié pour `SubnetId`.

Type : String

Contraintes de longueur : longueur minimale de 7. Longueur maximale de 15.

Modèle : `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Obligatoire : non

IpAddressType

Type d'adresse IP de la cible de montage. Les valeurs possibles sont `IPV4_ONLY` (IPv4 adresses uniquement), `IPV6_ONLY` (IPv6 adresses uniquement) et `DUAL_STACK` (double pile, à la fois IPv4 et IPv6 adresses). Si vous ne spécifiez pas `IpAddressType`, alors `IPV4_ONLY` est utilisé.

Note

Le `IpAddressType` doit correspondre au type d'adresse IP du sous-réseau. En outre, le `IpAddressType` paramètre remplace la valeur définie comme adresse IP par défaut pour le sous-réseau du VPC. Par exemple, si le `IpAddressType` is `IPV4_ONLY` et le `AssignIpv6AddressOnCreation` is `true`, ils IPv4 sont utilisés pour la cible de montage. Pour plus d'informations, consultez [Modifier les attributs d'adressage IP de votre sous-réseau](#).

Type : String

Valeurs valides : IPV4_ONLY | IPV6_ONLY | DUAL_STACK

Obligatoire : non

Ipv6Address

Si la cible `IPAddressType` de montage est IPv6 (`IPV6_ONLY` ou `DUAL_STACK`), spécifiez l'IPv6 adresse à utiliser. Si vous ne spécifiez pas de `Ipv6Address`, Amazon EFS sélectionne une adresse IP non utilisée dans le sous-réseau spécifié pour `SubnetId`.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 39

Obligatoire : non

SecurityGroups

Groupe de sécurité VPC IDs, du format. `sg-xxxxxxx` Ils doivent être destinés au même VPC que le sous-réseau spécifié. Le nombre maximum de groupes de sécurité dépend du quota du compte. Pour plus d'informations, consultez [Amazon VPC Quotas](#) dans le guide de l'utilisateur Amazon VPC (voir le tableau des groupes de sécurité). Si vous ne spécifiez aucun groupe de sécurité, Amazon EFS utilise le groupe de sécurité par défaut pour le VPC du sous-réseau.

Type : tableau de chaînes

Membres du tableau : nombre maximum de 100 éléments.

Contraintes de longueur : longueur minimale de 11. Longueur maximale de 43.

Modèle : `^sg-[0-9a-f]{8,40}`

Obligatoire : non

SubnetId

ID du sous-réseau dans lequel ajouter la cible de montage. Pour les systèmes de fichiers Zone unique, utilisez le sous-réseau associé à la Zone de disponibilité du système de fichiers. Le type de sous-réseau doit être le même que le `IpAddressType`.

Type : String

Contraintes de longueur : longueur minimale de 15. Longueur maximale de 47.

Modèle : ^subnet-[0-9a-f]{8,40}\$

Obligatoire : oui

Syntaxe de la réponse

```
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"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AvailabilityZoneId

Identifiant unique et cohérent de la Zone de disponibilité dans laquelle réside la cible de montage. Par exemple, use1-az1 il s'agit d'un ID AZ pour la région us-east-1 et il a le même emplacement dans chaque région. Compte AWS

Type : String

AvailabilityZoneName

Nom de la Zone de disponibilité dans laquelle se trouve la cible de montage. Les zones de disponibilité sont associées indépendamment aux noms de chacune d'entre elles Compte AWS.

Par exemple, il se Compte AWS peut que votre zone us-east-1a de disponibilité ne soit pas la même que celle us-east-1a d'une autre Compte AWS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : .+

FileSystemId

L'ID du système de fichiers pour lequel la cible de montage est destinée.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

IpAddress

IPv4 Adresse de la cible de montage.

Type : String

Contraintes de longueur : longueur minimale de 7. Longueur maximale de 15.

Modèle : `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Ipv6Address

IPv6 Adresse de la cible de montage.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 39

LifeCycleState

État du cycle de vie de la cible de montage.

Type : String

Valeurs valides : creating | available | updating | deleting | deleted | error

MountTargetId

ID de cible de montage attribué par le système.

Type : String

Contraintes de longueur : longueur minimale de 13. Longueur maximale de 45.

Modèle : ^fsmt-[0-9a-f]{8,40}\$

NetworkInterfaceId

ID de l'interface réseau créée par Amazon EFS lors de la création de la cible de montage.

Type : String

OwnerId

Compte AWS ID propriétaire de la ressource.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : ^(\d{12})|(\d{4}-\d{4}-\d{4})\$

SubnetId

ID du sous-réseau de la cible de montage.

Type : String

Contraintes de longueur : longueur minimale de 15. Longueur maximale de 47.

Modèle : ^subnet-[0-9a-f]{8,40}\$

VpcId

ID du cloud privé virtuel (VPC) dans lequel la cible de montage est configurée.

Type : String

Erreurs

AvailabilityZonesMismatch

Renvoie si la zone de disponibilité spécifiée pour la cible de montage est différente de la zone de disponibilité du système de fichiers. Pour plus d'informations, reportez-vous à la section [Redondance du stockage régional et à une zone](#).

Code d'état HTTP : 400

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifecycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

IpAddressInUse

Renvoyé si la demande a spécifié une adresse IP (`IpAddress` ou `Ipv6Address`) déjà utilisée dans le sous-réseau.

Code d'état HTTP : 409

MountTargetConflict

Renvoie si la cible de montage enfreint l'une des restrictions spécifiées en fonction des cibles de montage existantes du système de fichiers.

Code d'état HTTP : 409

NetworkInterfaceLimitExceeded

Le compte appelant a atteint la limite d'interfaces réseau élastiques pour le compte en question Région AWS. Supprimez certaines interfaces réseau ou demandez que le quota de comptes soit augmenté. Pour plus d'informations, consultez les [Quotas Amazon VPC](#) dans le Guide de l'utilisateur Amazon VPC (consultez l'entrée Interfaces réseau par région dans le tableau des interfaces réseau).

Code d'état HTTP : 409

NoFreeAddressesInSubnet

Non renvoyé `IpAddress` ou `Ipv6Address` a été fourni dans la demande et il n'y a aucune adresse IP libre dans le sous-réseau spécifié.

Code d'état HTTP : 409

SecurityGroupLimitExceeded

Renvoyé si le nombre `SecurityGroups` spécifié dans la demande est supérieur à la limite, qui est basée sur le quota du compte. Supprimez certains groupes de sécurité ou demandez que le quota de comptes soit augmenté. Pour plus d'informations, consultez [Amazon VPC Quotas](#) dans le guide de l'utilisateur Amazon VPC (voir le tableau des groupes de sécurité).

Code d'état HTTP : 400

SecurityGroupNotFound

Renvoyé si l'un des groupes de sécurité spécifiés n'existe pas dans le cloud privé virtuel (VPC) du sous-réseau.

Code d'état HTTP : 400

SubnetNotFound

Renvoyé s'il n'y a aucun sous-réseau dont l'ID est `SubnetId` fourni dans la demande.

Code d'état HTTP : 400

UnsupportedAvailabilityZone

Renvoyé si la fonctionnalité Amazon EFS demandée n'est pas disponible dans la Zone de disponibilité spécifiée.

Code d'état HTTP : 400

Exemples

Création d'une cible de montage à une IPv4 adresse disponible sur un sous-réseau

La demande suivante spécifie uniquement le système de fichiers et le sous-réseau de la cible de montage. La cible est créée à une IPv4 adresse disponible sur le sous-réseau spécifié, avec le groupe de sécurité par défaut associé au VPC.

Exemple de demande

```
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"}
```

Exemple de réponse

```
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"
}
```

Création d'une cible de montage à une IPv4 adresse spécifique

La demande suivante indique le système de fichiers, le sous-réseau, le groupe de sécurité et l'IPv4adresse à utiliser pour la cible de montage.

Exemple de demande

```
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"
  ]
}
```

Exemple de réponse

```
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"
}
```

Création d'une cible de montage à une IPv6 adresse spécifique

La demande suivante indique le système de fichiers, le sous-réseau, le groupe de sécurité et l'IPv6adresse à utiliser pour la cible de montage.

Exemple de demande

```
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"
  ]
}
```

Exemple de réponse

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Type: application/json
Content-Length: 252

{
  "OwnerId": "251839141158",
  "MountTargetId": "fsmnt-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"
}
```


Création d'une cible de montage à une IPv4 adresse disponible sur un sous-réseau à double pile

La demande suivante spécifie le système de fichiers, le sous-réseau et le type d'adresse de la cible de montage. La cible est créée à une IPv4 adresse disponible sur le sous-réseau à double pile spécifié, le groupe de sécurité par défaut étant associé au VPC.

Exemple de demande

```
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"}
```

Exemple de réponse

```
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"
}
```

Créez une cible de montage sur des adresses IPv4 et des IPv6 adresses spécifiques sur un sous-réseau à double pile

La demande suivante indique le système de fichiers, le sous-réseau, le groupe de sécurité, l'IPv4 adresse et l'IPv6 adresse de la cible de montage. La cible est créée aux IPv6 adresses IPv4 et adresses spécifiées sur un sous-réseau à double pile.

Exemple de demande

```
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"
  ]
}
```

Exemple de réponse

```
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"  
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateReplicationConfiguration

Crée une configuration de réplication vers un système de fichiers EFS nouveau ou existant. Pour plus d'informations, consultez la [Réplication Amazon EFS](#) dans le Guide de l'utilisateur Amazon EFS. La configuration de la réplication spécifie les éléments suivants :

- Système de fichiers source : système de fichiers EFS que vous souhaitez répliquer.
- Système de fichiers de destination : système de fichiers de destination vers lequel le système de fichiers source est répliqué. Il ne peut y avoir qu'un seul système de fichiers de destination dans une configuration de réplication.

Note

Un système de fichiers ne peut faire partie que d'une seule configuration de réplication.

Les paramètres de destination pour la configuration de réplication varient selon que vous effectuez une réplication vers un nouveau système de fichiers ou vers un système de fichiers existant, et si vous effectuez une réplication entre plusieurs systèmes. Comptes AWS Pour plus d'informations, consultez [DestinationToCreate](#).

Cette opération exige des autorisations pour l'action `elasticfilesystem:CreateReplicationConfiguration`. En outre, d'autres autorisations sont requises en fonction de la manière dont vous répliquez les systèmes de fichiers. Pour plus d'informations, consultez la section [Autorisations requises pour la réplication](#) dans le guide de l'utilisateur Amazon EFS.

Syntaxe de la demande

```
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"  
  }  
]  
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

SourceFileSystemId

Spécifie le système de fichiers Amazon EFS que vous souhaitez répliquer. Ce système de fichiers ne peut pas déjà être un système de fichiers source ou de destination dans une autre configuration de réplication.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Destinations

Un tableau d'objets de configuration de destination. Un seul objet de configuration de destination est pris en charge.

Type : tableau d'objets [DestinationToCreate](#)

Obligatoire : oui

Syntaxe de la réponse

```
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"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Décrit le moment où la configuration de réplication a été créée.

Type : Timestamp

Destinations

Tableau d'objets de destination. Un seul objet de destination est pris en charge.

Type : tableau d'objets [Destination](#)

OriginalSourceFileSystemArn

Amazon Resource Name (ARN) du système de fichiers EFS source d'origine dans la configuration de réplication.

Type : String

SourceFileSystemArn

Amazon Resource Name (ARN) du système de fichiers source actuel dans la configuration de réplication.

Type : String

SourceFileSystemId

ID du système de fichiers Amazon EFS source qui est répliqué.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

SourceFileSystemOwnerId

ID du système de fichiers source Compte AWS dans lequel réside le système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

SourceFileSystemRegion

Le système de fichiers EFS source Région AWS dans lequel se trouve le système de fichiers EFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

ConflictException

Renvoie si le système de fichiers source d'une réplication est chiffré mais que le système de fichiers de destination n'est pas chiffré.

Code d'état HTTP : 409

FileSystemLimitExceeded

Renvoyé si le nombre maximum de systèmes de fichiers autorisés par compte Compte AWS a déjà été créé.

Code d'état HTTP : 403

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifeCycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InsufficientThroughputCapacity

Renvoyé si la capacité est insuffisante pour fournir un débit supplémentaire. Cette valeur peut être renvoyée lorsque vous essayez de créer un système de fichiers en mode débit alloué, lorsque vous essayez d'augmenter le débit alloué d'un système de fichiers existant ou lorsque vous essayez de faire passer un système de fichiers existant du mode débit en rafale au mode débit alloué. Réessayez ultérieurement.

HTTP Status Code: 503

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

ReplicationNotFound

Renvoyé si le système de fichiers spécifié ne possède pas de configuration de réplication.

Code d'état HTTP : 404

ThroughputLimitExceeded

Renvoie si le mode de débit ou la quantité de débit alloué ne peuvent pas être modifiés car la limite de débit de 1024 Mbits/s a été atteinte.

Code d'état HTTP : 400

UnsupportedAvailabilityZone

Renvoyé si la fonctionnalité Amazon EFS demandée n'est pas disponible dans la Zone de disponibilité spécifiée.

Code d'état HTTP : 400

ValidationException

Renvoyé si le AWS Backup service n'est pas disponible dans le Région AWS pays dans lequel la demande a été faite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateTags

Note

OBSOLÈTE - CreateTags est obsolète et n'est pas maintenu. Pour créer des balises pour les ressources EFS, utilisez l'action API [TagResource](#).

Crée ou remplace des balises associées à un système de fichiers. Chaque balise est une paire clés-valeurs. Si une clé de balise spécifiée dans la demande existe déjà dans le système de fichiers, cette opération remplace sa valeur par la valeur fournie dans la demande. Si vous ajoutez la balise Name à votre système de fichiers, Amazon EFS la renvoie en réponse à l'opération [DescribeFileSystems](#).

Cette opération nécessite une autorisation pour l'action `elasticfilesystem:CreateTags`.

Syntaxe de la demande

```
POST /2015-02-01/create-tags/FileSystemId HTTP/1.1
Content-type: application/json

{
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[FileSystemId](#)

L'ID du système de fichiers dont vous souhaitez modifier les balises (chaîne). Cette opération modifie uniquement les balises, pas le système de fichiers.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[Tags](#)

Un tableau des objets `Tag` à ajouter. Chaque objet `Tag` est une paire clé-valeur.

Type : tableau d'objets [Tag](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteAccessPoint

Supprime le point d'accès spécifié. Une fois la suppression terminée, les nouveaux clients ne peuvent plus se connecter aux points d'accès. Les clients connectés au point d'accès au moment de la suppression continueront de fonctionner jusqu'à ce qu'ils mettent fin à leur connexion.

Cette opération exige des autorisations pour l'action `elasticfilesystem:DeleteAccessPoint`.

Syntaxe de la demande

```
DELETE /2015-02-01/access-points/AccessPointId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

AccessPointId

ID du point d'accès à supprimer.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

AccessPointNotFound

Renvoyé si la AccessPointId valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

BadRequest

Renvoyé si la demande est mal formulée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteFileSystem

Supprime un système de fichiers, ce qui coupe définitivement l'accès à son contenu. Au retour, le système de fichiers n'existe plus et vous ne pouvez accéder à aucun contenu du système de fichiers supprimé.

Vous devez supprimer manuellement les cibles de montage associées à un système de fichiers avant de pouvoir supprimer un système de fichiers EFS. Cette étape est exécutée pour vous lorsque vous utilisez la AWS console pour supprimer un système de fichiers.

Note

Vous ne pouvez pas supprimer un système de fichiers faisant partie d'une configuration de réplication EFS. Vous devez d'abord supprimer la configuration de réplication.

Vous ne pouvez pas supprimer un système de fichiers qui est en cours d'utilisation. En d'autres termes, si le système de fichiers possède des cibles de montage, vous devez d'abord les supprimer. Pour plus d'informations, consultez [DescribeMountTargets](#) et [DeleteMountTarget](#).

Note

L'appel DeleteFileSystem est renvoyé alors que l'état du système de fichiers est toujours deleting. Vous pouvez vérifier l'état de suppression du système de fichiers en appelant l'opération [DescribeFileSystems](#), qui renvoie la liste des systèmes de fichiers de votre compte. Si vous transmettez un ID de système de fichiers ou un jeton de création pour le système de fichiers supprimé, le [DescribeFileSystems](#) retourne une erreur 404 FileSystemNotFound.

Cette opération exige des autorisations pour l'action `elasticfilesystem:DeleteFileSystem`.

Syntaxe de la demande

```
DELETE /2015-02-01/file-systems/FileSystemId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

FileSystemId

ID du système de fichiers que vous souhaitez supprimer.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemInUse

Renvoie si un système de fichiers possède des cibles de montage.

Code d'état HTTP : 409

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

Exemples

Supprimer un système de fichiers

L'exemple suivant envoie une demande DELETE au point de terminaison `file-systems` (`elasticfilesystem.us-west-2.amazonaws.com/2015-02-01/file-systems/fs-01234567`) pour supprimer un système de fichiers dont l'ID est `fs-01234567`.

Exemple de demande

```
DELETE /2015-02-01/file-systems/fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T233021Z
Authorization: <...>
```

Exemple de réponse

```
HTTP/1.1 204 No Content
x-amzn-RequestId: a2d125b3-7ebd-4d6a-ab3d-5548630bff33
Content-Length: 0
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteFileSystemPolicy

Supprime le `FileSystemPolicy` pour le système de fichiers spécifié. La valeur par défaut `FileSystemPolicy` entre en vigueur une fois que la politique existante est supprimée. Pour plus d'informations sur la politique de système de fichiers par défaut, consultez [Utilisation de politiques basées sur les ressources avec EFS](#).

Cette opération exige des autorisations pour l'action `elasticfilesystem:DeleteFileSystemPolicy`.

Syntaxe de la demande

```
DELETE /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

FileSystemId

Spécifie le système de fichiers EFS pour lequel vous souhaitez supprimer le `FileSystemPolicy`.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifecycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteMountTarget

Supprime la cible de montage spécifiée.

Cette opération interrompt de force tous les montages du système de fichiers en utilisant la cible de montage qui est supprimée, ce qui peut perturber les instances ou les applications qui utilisent ces montages. Pour éviter que les applications ne soient interrompues brusquement, vous pouvez envisager de démonter tous les supports de la cible de montage, si possible. L'opération supprime également l'interface réseau associée. Les écritures non validées peuvent être perdues, mais le fait de casser une cible de montage à l'aide de cette opération ne corrompt pas le système de fichiers lui-même. Le système de fichiers que vous avez créé est conservé. Vous pouvez monter une EC2 instance dans votre VPC en utilisant une autre cible de montage.

Cette opération exige des autorisations pour l'action suivante sur le système de fichiers :

- `elasticfilesystem>DeleteMountTarget`

Note

L'appel `DeleteMountTarget` est renvoyé alors que l'état de la cible de montage est toujours `actifdeleting`. Vous pouvez vérifier la suppression de la cible de montage en appelant l'opération [DescribeMountTargets](#), qui renvoie une liste des descriptions des cibles de montage pour le système de fichiers donné.

L'opération nécessite également des autorisations pour l' EC2 action Amazon suivante sur l'interface réseau de la cible de montage :

- `ec2>DeleteNetworkInterface`

Syntaxe de la demande

```
DELETE /2015-02-01/mount-targets/MountTargetId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MountTargetId

ID de la cible de montage à supprimer (chaîne).

Contraintes de longueur : longueur minimale de 13. Longueur maximale de 45.

Modèle : `^fsmt-[0-9a-f]{8,40}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

DependencyTimeout

Le délai imparti pour répondre à la demande a expiré et le client doit réessayer l'appel.

Code d'état HTTP : 504

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

MountTargetNotFound

Renvoyé s'il n'y a aucune cible de montage avec l'identifiant spécifié dans celui de l'appelant Compte AWS.

Code d'état HTTP : 404

Exemples

Supprimer la cible de montage d'un système de fichiers

L'exemple suivant envoie une demande DELETE pour supprimer une cible de montage spécifique.

Exemple de demande

```
DELETE /2015-02-01/mount-targets/fsmt-9a13661e HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T232908Z
Authorization: <...>
```

Exemple de réponse

```
HTTP/1.1 204 No Content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)

- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteReplicationConfiguration

Supprimer une configuration de réplication La suppression d'une configuration de réplication met fin au processus de réplication. Après la suppression d'une configuration de réplication, le système de fichiers de destination devient `Writeable` et sa protection contre le remplacement de la réplication est réactivée. Pour plus d'informations, consultez [Supprimer une configuration de réplication](#).

Cette opération exige des autorisations pour l'action `elasticfilesystem:DeleteReplicationConfiguration`.

Syntaxe de la demande

```
DELETE /2015-02-01/file-systems/SourceFileSystemId/replication-configuration?
deletionMode=DeletionMode HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

DeletionMode

Lors de la réplication croisée Comptes AWS ou croisée Régions AWS, Amazon EFS supprime la configuration de réplication à la fois du compte source et de destination ou de la région (ALL_CONFIGURATIONS) par défaut. Si un problème de configuration ou d'autorisation empêche Amazon EFS de supprimer la configuration de réplication des deux côtés, vous pouvez utiliser ce LOCAL_CONFIGURATION_ONLY mode pour supprimer la configuration de réplication uniquement du côté local (le compte ou la région à partir duquel la suppression est effectuée).

Note

Utilisez ce LOCAL_CONFIGURATION_ONLY mode uniquement dans le cas où Amazon EFS ne parvient pas à supprimer la configuration de réplication à la fois dans le compte ou la région source et de destination. La suppression de la configuration locale rend la configuration de l'autre compte ou de l'autre région irrécupérable. En outre, n'utilisez pas ce mode pour la réplication entre le même compte et la même région, car cela entraîne une erreur d'exception. `BadRequest`

Valeurs valides : ALL_CONFIGURATIONS | LOCAL_CONFIGURATION_ONLY

SourceFileSystemId

ID du système de fichiers source dans la configuration de réplication.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

ReplicationNotFound

Renvoyé si le système de fichiers spécifié ne possède pas de configuration de réplication.

Code d'état HTTP : 404

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteTags

Note

OBSOLÈTE - DeleteTags est obsolète et n'est pas maintenu. Pour supprimer les balises des ressources EFS, utilisez l'action API [UntagResource](#).

Supprime les balises spécifiées à partir d'un système de fichiers. Si la demande DeleteTags inclut une clé de balise qui n'existe pas, Amazon EFS l'ignore et ne provoque aucune erreur. Pour plus d'informations sur les balises et les restrictions associées, consultez la section [Restrictions relatives aux balises](#) dans le guide de AWS Billing and Cost Management l'utilisateur.

Cette opération exige des autorisations pour l'action `elasticfilesystem:DeleteTags`.

Syntaxe de la demande

```
POST /2015-02-01/delete-tags/FileSystemId HTTP/1.1
Content-type: application/json

{
  "TagKeys": [ "string" ]
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[FileSystemId](#)

L'ID du système de fichiers dont vous souhaitez supprimer les balises (chaîne).

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

TagKeys

Une liste de clés d'étiquette à supprimer.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : `^(?![aA]{1}[wW]{1}[sS]{1}:)([\\p{L}\\p{Z}\\p{N}_.: /+=\\-@]+)$`

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeAccessPoints

Renvoie la description d'un point d'accès Amazon EFS spécifique si `AccessPointId` est fourni. Si vous fournissez un `EFS FileSystemId`, il renvoie les descriptions de tous les points d'accès pour ce système de fichiers. Vous pouvez fournir un `AccessPointId` ou un `FileSystemId` dans la demande, mais pas les deux.

Cette opération exige des autorisations pour l'action `elasticfilesystem:DescribeAccessPoints`.

Syntaxe de la demande

```
GET /2015-02-01/access-points?  
AccessPointId=AccessPointId&FileSystemId=FileSystemId&MaxResults=MaxResults&NextToken=NextToken  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

AccessPointId

(Facultatif) Spécifie un point d'accès EFS à décrire dans la réponse ; il s'exclut mutuellement avec `FileSystemId`.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

FileSystemId

(Facultatif) Si vous fournissez un `FileSystemId`, EFS renvoie tous les points d'accès à ce système de fichiers ; ils s'excluent mutuellement avec `AccessPointId`.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

MaxResults

(Facultatif) Lorsque vous récupérez tous les points d'accès d'un système de fichiers, vous pouvez éventuellement spécifier le paramètre `MaxItems` pour limiter le nombre d'objets renvoyés dans une réponse. La valeur par défaut est 100.

Plage valide : valeur minimum de 1.

NextToken

`NextToken` est présent si la charge utile de la réponse est paginée. Vous pouvez utiliser `NextMarker` pour une demande ultérieure pour obtenir la page suivante de descriptions de points d'accès.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
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"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AccessPoints](#)

Un ensemble de descriptions de points d'accès.

Type : tableau d'objets [AccessPointDescription](#)

[NextToken](#)

Présent s'il y a plus de points d'accès que ceux renvoyés dans la réponse. Vous pouvez utiliser le NextMarker dans la requête suivante pour récupérer les descriptions supplémentaires.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

Erreurs

AccessPointNotFound

Renvoyé si la `AccessPointId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

BadRequest

Renvoyé si la demande est mal formulée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)

- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeAccountPreferences

Renvoie les paramètres des préférences du compte pour le compte Compte AWS associé à l'utilisateur qui fait la demande, dans la version actuelle Région AWS.

Syntaxe de la demande

```
GET /2015-02-01/account-preferences HTTP/1.1
Content-type: application/json
```

```
{
  "MaxResults": number,
  "NextToken": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

MaxResults

(Facultatif) Lorsque vous récupérez les préférences du compte, vous pouvez éventuellement spécifier le paramètre `MaxItems` pour limiter le nombre d'objets renvoyés dans une réponse. La valeur par défaut est 100.

Type : entier

Plage valide : Valeur minimum de 1.

Obligatoire : non

NextToken

(Facultatif) Vous pouvez utiliser `NextToken` dans une requête ultérieure pour récupérer la page suivante de préférences Compte AWS des points d'accès si la charge utile de la réponse a été paginée.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "ResourceIdPreference": {
    "ResourceIdType": "string",
    "Resources": [ "string" ]
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

Présent s'il y a plus d'enregistrements que ceux renvoyés dans la réponse. Vous pouvez utiliser NextToken dans la requête suivante pour récupérer les descriptions supplémentaires.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

[ResourceIdPreference](#)

Décrit le paramètre de préférence d'ID de ressource Compte AWS associé à l'utilisateur qui fait la demande, dans la version actuelle Région AWS.

Type : objet [ResourceIdPreference](#)

Erreurs

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeBackupPolicy

Renvoie la politique de sauvegarde pour le système de fichiers EFS spécifié.

Syntaxe de la demande

```
GET /2015-02-01/file-systems/FileSystemId/backup-policy HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

FileSystemId

Spécifie le système de fichiers EFS pour lequel récupérer le BackupPolicy.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPolicy": {
    "Status": "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPolicy](#)

Décrit la politique de sauvegarde du système de fichiers, en indiquant si les sauvegardes automatiques sont activées ou désactivées.

Type : objet [BackupPolicy](#)

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

PolicyNotFound

Renvoyé si `no_backup` est spécifié pour un système de fichiers EFS à zone unique.

Code d'état HTTP : 404

ValidationException

Renvoyé si le AWS Backup service n'est pas disponible dans la Région AWS dans laquelle la demande a été faite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeFileSystemPolicy

Renvoie le `FileSystemPolicy` pour le système de fichiers EFS spécifié.

Cette opération exige des autorisations pour l'action `elasticfilesystem:DescribeFileSystemPolicy`.

Syntaxe de la demande

```
GET /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[FileSystemId](#)

Spécifie le système de fichiers EFS pour lequel récupérer le `FileSystemPolicy`.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "FileSystemId": "string",
  "Policy": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

FileSystemId

Spécifie le système de fichiers EFS auquel s'applique `FileSystemPolicy`.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Policy

Le JSON formaté `FileSystemPolicy` pour le système de fichiers EFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 20000.

Modèle : `[\s\S]+`

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

PolicyNotFound

Renvoyé si aucun backup est spécifié pour un système de fichiers EFS à zone unique.

Code d'état HTTP : 404

Exemples

exemple

Cet exemple illustre une utilisation de `DescribeFileSystemPolicy`.

Exemple de demande

```
GET /2015-02-01/file-systems/fs-01234567/policy HTTP/1.1
```

Exemple de réponse

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

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeFileSystems

Renvoie la description d'un système de fichiers Amazon EFS spécifique si le système de fichiers `CreationToken` ou le `FileSystemId` est fourni. Dans le cas contraire, il renvoie des descriptions de tous les systèmes de fichiers appartenant Compte AWS à Région AWS l'appelant dans le terminal que vous appelez.

Lorsque vous récupérez toutes les descriptions des systèmes de fichiers, vous pouvez éventuellement spécifier le paramètre `MaxItems` pour limiter le nombre de descriptions dans une réponse. Ce nombre est automatiquement fixé à 100. S'il reste d'autres descriptions de systèmes de fichiers `NextMarker`, Amazon EFS renvoie un jeton opaque dans la réponse. Dans ce cas, vous devez envoyer une demande suivante avec le paramètre de demande `Marker` défini sur la valeur de `NextMarker`.

Pour récupérer la liste des descriptions de votre système de fichiers, cette opération est utilisée dans un processus itératif, dans lequel elle `DescribeFileSystems` est d'abord appelée sans le `Marker`, puis l'opération continue à l'appeler avec le paramètre `Marker` défini sur la valeur de `NextMarker` de la réponse précédente jusqu'à ce que la réponse n'a pas de `NextMarker`.

L'ordre des systèmes de fichiers renvoyés en réponse à un `DescribeFileSystems` appel et l'ordre des systèmes de fichiers renvoyés dans les réponses d'une itération à appels multiples ne sont pas spécifiés.

Cette opération exige des autorisations pour l'action `elasticfilesystem:DescribeFileSystems`.

Syntaxe de la demande

```
GET /2015-02-01/file-systems?  
CreationToken=CreationToken&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

CreationToken

(Facultatif) Limite la liste au système de fichiers avec ce jeton de création (chaîne). Vous spécifiez un jeton de création lorsque vous créez un système de fichiers Amazon EFS.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : .+

[FileSystemId](#)

(Facultatif) ID du système de fichiers dont vous souhaitez récupérer la description (chaîne).

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[Marker](#)

(Facultatif) Un jeton de pagination opaque renvoyé par une opération `DescribeFileSystems` précédente (chaîne). Le cas échéant, indique de continuer la liste à partir de laquelle l'appel de retour s'était arrêté.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : .+

[MaxItems](#)

(Facultatif) Spécifie le nombre maximum de systèmes de fichiers à renvoyer dans la réponse (entier). Ce nombre est automatiquement fixé à 100. La réponse est paginée à 100 par page si vous avez plus de 100 systèmes de fichiers.

Plage valide : valeur minimum de 1.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
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"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[FileSystems](#)

Tableau de descriptions de systèmes de fichiers.

Type : tableau d'objets [FileSystemDescription](#)

[Marker](#)

Présent s'il est fourni par l'appelant dans la demande (chaîne).

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

[NextMarker](#)

Présent s'il y a plus de systèmes de fichiers que ceux renvoyés dans la réponse (String). Vous pouvez utiliser `NextMarker` dans la requête suivante pour récupérer les descriptions.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

Exemples

Extrait une liste de 10 systèmes de fichiers

L'exemple suivant envoie une requête GET au file-systems point de terminaison (`elasticfilesystem.us-west-2.amazonaws.com/2015-02-01/file-systems`). La demande spécifie un paramètre de requête `MaxItems` pour limiter le nombre de descriptions de systèmes de fichiers à 10.

Exemple de demande

```
GET /2015-02-01/file-systems?MaxItems=10 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T191208Z
Authorization: <...>
```

Exemple de réponse

```
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
      }
    }
  ]
}
```

```
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeLifecycleConfiguration

Renvoie l'`LifecycleConfiguration` objet actuel pour le système de fichiers EFS spécifié. La gestion du cycle de vie utilise l'objet `LifecycleConfiguration` pour identifier le moment où il convient de déplacer des fichiers entre les classes de stockage. Pour un système de fichiers sans objet `LifecycleConfiguration`, l'appel renvoie un tableau vide dans la réponse.

Cette opération exige des autorisations pour l'opération `elasticfilesystem:DescribeLifecycleConfiguration`.

Syntaxe de la demande

```
GET /2015-02-01/file-systems/FileSystemId/lifecycle-configuration HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

FileSystemId

L'ID du système de fichiers dont vous souhaitez récupérer l'objet `LifecycleConfiguration` (String).

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
```

```
"LifecyclePolicies": [  
  {  
    "TransitionToArchive": "string",  
    "TransitionToIA": "string",  
    "TransitionToPrimaryStorageClass": "string"  
  }  
]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LifecyclePolicies

Un ensemble de politiques de gestion du cycle de vie. EFS prend en charge au maximum une politique par système de fichiers.

Type : tableau d'objets [LifecyclePolicy](#)

Membres du tableau : nombre maximum de 3 éléments.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la FileSystemId valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

Exemples

Récupérer la configuration du cycle de vie d'un système de fichiers

La requête suivante récupère l'objet LifecycleConfiguration pour le système de fichiers spécifié.

Exemple de demande

```
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: <...>
```

Exemple de réponse

```
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"
    }
  ]
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeMountTargets

Renvoie les descriptions de toutes les cibles de montage actuelles, ou une cible de montage spécifique, pour un système de fichiers. Lorsque vous demandez toutes les cibles de montage actuelles, l'ordre des cibles de montage renvoyées dans la réponse n'est pas spécifié.

Cette opération nécessite des autorisations pour l'action `elasticfilesystem:DescribeMountTargets`, soit sur l'ID du système de fichiers que vous spécifiez dans `FileSystemId`, soit sur le système de fichiers de la cible de montage dans laquelle vous spécifiez dans `MountTargetId`.

La commande CLI correspondante est `describe-mount-targets`.

Syntaxe de la demande

```
GET /2015-02-01/mount-targets?  
AccessPointId=AccessPointId&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems&MountTargetId=MountTargetId  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

AccessPointId

(Facultatif) L'ID du point d'accès dont vous souhaitez répertorier les cibles de montage. Il doit être inclus dans votre demande si un `FileSystemId` ou `MountTargetId` n'est pas inclus dans votre demande. Accepte un ID de point d'accès ou un ARN en entrée.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

FileSystemId

(Facultatif) ID du système de fichiers dont vous souhaitez répertorier les cibles de montage (chaîne). Il doit être inclus dans votre demande si un `AccessPointId` ou `MountTargetId` n'est pas inclus. Accepte un ID de système de fichiers ou un ARN en entrée.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Marker

(Facultatif) Un jeton de pagination opaque renvoyé par une opération `DescribeMountTargets` précédente (chaîne). S'il est présent, il indique de continuer la liste à partir de l'endroit où le précédent appel de retour s'est arrêté.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : `.+`

MaxItems

(Facultatif) Nombre maximum de cibles de montage à renvoyer dans la réponse. Actuellement, ce nombre est automatiquement défini sur 10 et les autres valeurs sont ignorées. La réponse est paginée à 100 par page si vous avez plus de 100 cibles de montage.

Plage valide : valeur minimum de 1.

MountTargetId

(Facultatif) ID de la cible de montage que vous souhaitez faire décrire (chaîne). Il doit être inclus dans votre demande si `FileSystemId` n'est pas inclus. Accepte un ID de cible de montage ou un ARN en entrée.

Contraintes de longueur : longueur minimale de 13. Longueur maximale de 45.

Modèle : `^fsmt-[0-9a-f]{8,40}$`

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
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"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[Marker](#)

Si la demande inclut le Marker, la réponse renvoie cette valeur dans ce champ.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : .+

[MountTargets](#)

Renvoie les cibles de montage du système de fichiers sous forme de tableau d'objets MountTargetDescription.

Type : tableau d'objets [MountTargetDescription](#)

[NextMarker](#)

Si une valeur est présente, il y a plus de cibles de montages à renvoyer. Dans une demande ultérieure, vous pouvez fournir Marker dans votre demande pour récupérer le prochain ensemble de cibles de montage.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

Erreurs

AccessPointNotFound

Renvoyé si la `AccessPointId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

BadRequest

Renvoyé si la demande est mal formulée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

MountTargetNotFound

Renvoyé s'il n'y a aucune cible de montage avec l'identifiant spécifié dans celui de l'appelant Compte AWS.

Code d'état HTTP : 404

Exemples

Récupère les descriptions des cibles de montage créées pour un système de fichiers

La requête suivante récupère les descriptions des cibles de montage créées pour le système de fichiers spécifié.

Exemple de demande

```
GET /2015-02-01/mount-targets?FileSystemId=fs-01234567 HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140622T191252Z
Authorization: <...>
```

Exemple de réponse

```
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"
    }
  ]
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)

- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeMountTargetSecurityGroups

Renvoie les groupes de sécurité actuellement en vigueur pour une cible de montage. Cette opération nécessite que l'interface réseau de la cible de montage ait été créée et que l'état du cycle de vie de la cible de montage n'est pas `deleted`.

Cette opération nécessite des autorisations pour les actions suivantes :

- action `elasticfilesystem:DescribeMountTargetSecurityGroups` sur le système de fichiers de la cible de montage.
- action `ec2:DescribeNetworkInterfaceAttribute` sur l'interface réseau de la cible de montage.

Syntaxe de la demande

```
GET /2015-02-01/mount-targets/MountTargetId/security-groups HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MountTargetId

ID de la cible de montage dont vous souhaitez modifier les groupes de sécurité.

Contraintes de longueur : longueur minimale de 13. Longueur maximale de 45.

Modèle : `^fsmt-[0-9a-f]{8,40}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json
```

```
{  
  "SecurityGroups": [ "string" ]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[SecurityGroups](#)

Tableau de groupes de sécurité.

Type : tableau de chaînes

Membres du tableau : nombre maximum de 100 éléments.

Contraintes de longueur : longueur minimale de 11. Longueur maximale de 43.

Modèle : `^sg-[0-9a-f]{8,40}`

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

IncorrectMountTargetState

Renvoyé si l'état de la cible de montage n'est pas correct pour l'opération.

Code d'état HTTP : 409

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

MountTargetNotFound

Renvoyé s'il n'y a aucune cible de montage avec l'identifiant spécifié dans celui de l'appelant Compte AWS.

Code d'état HTTP : 404

Exemples

Récupérer les groupes de sécurité en vigueur pour un système de fichiers.

L'exemple suivant retrouve les groupes de sécurité en vigueur pour l'interface réseau associée à une cible de montage.

Exemple de demande

```
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: <...>
```

Exemple de réponse

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-Length: 57

{
  "SecurityGroups" : [
    "sg-188d9f74"
  ]
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)

- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeReplicationConfigurations

Récupère la configuration de réplication pour un système de fichiers spécifique. Si aucun système de fichiers n'est spécifié, toutes les configurations de réplication pour le Compte AWS in an Région AWS sont récupérées.

Syntaxe de la demande

```
GET /2015-02-01/file-systems/replication-configurations?  
FileSystemId=FileSystemId&MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[FileSystemId](#)

Vous pouvez récupérer la configuration de réplication pour un système de fichiers spécifique en fournissant son ID de système de fichiers. Pour la réplication entre comptes et entre régions, un compte peut uniquement décrire la configuration de réplication d'un système de fichiers dans sa propre région.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[MaxResults](#)

(Facultatif) Pour limiter le nombre d'objets renvoyés dans une réponse, vous pouvez spécifier le paramètre `MaxItems`. La valeur par défaut est 100.

Plage valide : valeur minimum de 1.

[NextToken](#)

`NextToken` est présent si la charge utile de la réponse est paginée. Vous pouvez utiliser `NextToken` dans une requête ultérieure pour récupérer la page de sortie suivante.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : `.+`

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
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"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

Vous pouvez utiliser NextToken dans la requête suivante pour récupérer les descriptions supplémentaires.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

Replications

Ensemble de configurations de réplication renvoyé.

Type : tableau d'objets [ReplicationConfigurationDescription](#)

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la FileSystemId valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

ReplicationNotFound

Renvoyé si le système de fichiers spécifié ne possède pas de configuration de réplication.

Code d'état HTTP : 404

ValidationException

Renvoyé si le AWS Backup service n'est pas disponible dans le Région AWS pays dans lequel la demande a été faite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeTags

Note

OBSOLÈTE - L'action `DescribeTags` est obsolète et n'est pas maintenue. Pour afficher les balises associées aux ressources EFS, utilisez l'action `ListTagsForResource` API.

Renvoie les balises associées à un système de fichiers. L'ordre des balises renvoyées dans la réponse à un appel `DescribeTags` et l'ordre des balises renvoyées dans les réponses d'une itération à appels multiples (lors de l'utilisation de la pagination) ne sont pas spécifiés.

Cette opération exige des autorisations pour l'action `elasticfilesystem:DescribeTags`.

Syntaxe de la demande

```
GET /2015-02-01/tags/FileSystemId?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

FileSystemId

ID du système de fichiers dont vous voulez récupérer le jeu de balises.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Marker

(Facultatif) Un jeton de pagination opaque renvoyé par une opération `DescribeTags` précédente (chaîne). S'il est présent, il indique de continuer la liste à partir de l'endroit où l'appel précédent s'est arrêté.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

[MaxItems](#)

(Facultatif) Nombre maximum de balises de système de fichiers à renvoyer dans la réponse. Actuellement, ce nombre est automatiquement défini sur 100 et les autres valeurs sont ignorées. La réponse est paginée à 100 par page si vous avez plus de 100 balises.

Plage valide : valeur minimum de 1.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "Marker": "string",
  "NextMarker": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[Marker](#)

Si la demande inclut un Marker, la réponse renvoie cette valeur dans ce champ.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

[NextMarker](#)

Si une valeur est présente, il y a d'autres balises à renvoyer. Dans une demande ultérieure, vous pouvez fournir la valeur de `NextMarker` comme valeur du paramètre `Marker` dans votre prochaine demande pour récupérer le prochain ensemble de balises.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

[Tags](#)

Tags associés au système de fichiers, présentés sous forme de tableau des objets `Tag`.

Type : tableau d'objets [Tag](#)

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

Exemples

Récupérer toutes les balises associées à un système de fichiers

La requête suivante récupère les balises (paires clé-valeur) associées au système de fichiers spécifié.

Exemple de demande

```
GET /2015-02-01/tags/fs-01234567/ HTTP/1.1
Host: elasticfilesystem.us-west-2.amazonaws.com
x-amz-date: 20140620T215404Z
Authorization: <...>
```

Exemple de réponse

```
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"
    }
  ]
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListTagsForResource

Répertorie toutes les balises d'une ressource EFS de haut niveau. Vous devez fournir l'ID de la ressource dont vous souhaitez récupérer les balises.

Cette opération exige des autorisations pour l'action `elasticfilesystem:DescribeAccessPoints`.

Syntaxe de la demande

```
GET /2015-02-01/resource-tags/ResourceId?MaxResults=MaxResults&NextToken=NextToken
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

(Facultatif) Spécifie le nombre maximum d'objets de balises à renvoyer dans la réponse. La valeur par défaut est 100.

Plage valide : valeur minimum de 1.

NextToken

(Facultatif) Vous pouvez utiliser `NextToken` dans une requête ultérieure pour récupérer la page suivante de descriptions des points d'accès si la charge utile de la réponse a été paginée.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : . +

ResourceId

Spécifie la ressource EFS dont vous souhaitez récupérer des balises. Vous pouvez récupérer des balises pour les systèmes de fichiers EFS et les points d'accès à l'aide de ce point de terminaison d'API.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(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})$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

NextToken est présent si la charge utile de la réponse est paginée. Vous pouvez utiliser NextToken pour une demande ultérieure pour obtenir la page suivante de descriptions de points d'accès.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : .+

Tags

Tableau des balises de ressource EFS spécifiée.

Type : tableau d'objets [Tag](#)

Erreurs

AccessPointNotFound

Renvoyé si la AccessPointId valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

BadRequest

Renvoyé si la demande est mal formulée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la FileSystemId valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ModifyMountTargetSecurityGroups

Modifie l'ensemble de groupes de sécurité en vigueur pour une cible de montage.

Lorsque vous créez une cible de montage, Amazon EFS crée également une interface réseau. Pour de plus amples informations, veuillez consulter [CreateMountTarget](#). Cette opération remplace les groupes de sécurité en vigueur pour l'interface réseau associée à une cible de montage avec les SecurityGroups fournis dans la demande. Cette opération nécessite que l'interface réseau de la cible de montage ait été créée et que l'état du cycle de vie de la cible de montage ne soit pas deleted.

L'opération nécessite des autorisations pour les actions suivantes :

- Action elasticfilesystem:ModifyMountTargetSecurityGroups sur le système de fichiers de la cible de montage.
- action ec2:ModifyNetworkInterfaceAttribute sur l'interface réseau de la cible de montage.

Syntaxe de la demande

```
PUT /2015-02-01/mount-targets/MountTargetId/security-groups HTTP/1.1
Content-type: application/json

{
  "SecurityGroups": [ "string" ]
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MountTargetId](#)

ID de la cible de montage dont vous souhaitez modifier les groupes de sécurité.

Contraintes de longueur : longueur minimale de 13. Longueur maximale de 45.

Modèle : ^fsmt-[0-9a-f]{8,40}\$

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[SecurityGroups](#)

Un ensemble de groupes de sécurité VPC. IDs

Type : tableau de chaînes

Membres du tableau : nombre maximum de 100 éléments.

Contraintes de longueur : longueur minimale de 11. Longueur maximale de 43.

Modèle : `^sg-[0-9a-f]{8,40}`

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

IncorrectMountTargetState

Renvoyé si l'état de la cible de montage n'est pas correct pour l'opération.

Code d'état HTTP : 409

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

MountTargetNotFound

Renvoyé s'il n'y a aucune cible de montage avec l'identifiant spécifié dans celui de l'appelant Compte AWS.

Code d'état HTTP : 404

SecurityGroupLimitExceeded

Renvoyé si le nombre SecurityGroups spécifié dans la demande est supérieur à la limite, qui est basée sur le quota du compte. Supprimez certains groupes de sécurité ou demandez que le quota de comptes soit augmenté. Pour plus d'informations, consultez [Amazon VPC Quotas](#) dans le guide de l'utilisateur Amazon VPC (voir le tableau des groupes de sécurité).

Code d'état HTTP : 400

SecurityGroupNotFound

Renvoyé si l'un des groupes de sécurité spécifiés n'existe pas dans le cloud privé virtuel (VPC) du sous-réseau.

Code d'état HTTP : 400

Exemples

Remplacer les groupes de sécurité d'une cible de montage

L'exemple suivant remplace les groupes de sécurité en vigueur pour l'interface réseau associée à une cible de montage.

Exemple de demande

```
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"  
]  
}
```

Exemple de réponse

```
HTTP/1.1 204 No Content  
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutAccountPreferences

Utilisez cette opération pour définir la préférence du compte actuel Région AWS afin d'utiliser une ressource longue de 17 caractères (63 bits) ou courte de 8 caractères (32 bits) IDs pour le nouveau système de fichiers EFS et de monter les ressources cibles. Toutes les ressources existantes ne IDs sont pas affectées par les modifications que vous apportez. Vous pouvez définir la préférence d'identification pendant la période d'inscription lorsque l'EFS passe à une ressource IDs longue. Pour plus d'informations, consultez [la section Gestion des ressources Amazon EFS IDs](#).

Note

À partir d'octobre 2021, vous recevrez un message d'erreur si vous essayez de définir les préférences du compte pour utiliser l'identifiant de ressource au format court à 8 caractères. Contactez le AWS support si vous recevez un message d'erreur et devez utiliser l'abréviation IDs pour « système de fichiers » et « ressources cibles » de montage.

Syntaxe de la demande

```
PUT /2015-02-01/account-preferences HTTP/1.1
Content-type: application/json
```

```
{
  "ResourceIdType": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[ResourceIdType](#)

Spécifie la préférence d'ID de ressource EFS à définir pour l'utilisateur Compte AWS, dans la Région AWS version actuelle, soit LONG_ID (17 caractères), soit SHORT_ID (8 caractères).

Note

À partir d'octobre 2021, vous recevrez un message d'erreur lorsque vous aurez défini la préférence du compte sur SHORT_ID. Contactez le AWS support si vous recevez un message d'erreur et devez utiliser l'abréviation IDs pour « système de fichiers » et « ressources cibles » de montage.

Type : String

Valeurs valides : LONG_ID | SHORT_ID

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "ResourceIdPreference": {
    "ResourceIdType": "string",
    "Resources": [ "string" ]
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ResourceIdPreference

Décrit le type de ressource et son identifiant préféré pour celui de l'utilisateur Compte AWS, dans la version actuelle Région AWS.

Type : objet [ResourceIdPreference](#)

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutBackupPolicy

Met à jour la politique de sauvegarde du système de fichiers. Utilisez cette action pour démarrer ou arrêter les sauvegardes automatiques du système de fichiers.

Syntaxe de la demande

```
PUT /2015-02-01/file-systems/FileSystemId/backup-policy HTTP/1.1
Content-type: application/json
```

```
{
  "BackupPolicy": {
    "Status": "string"
  }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[FileSystemId](#)

Spécifie le système de fichiers EFS pour lequel mettre à jour la politique de sauvegarde.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[BackupPolicy](#)

Politique de sauvegarde incluse dans la demande PutBackupPolicy.

Type : objet [BackupPolicy](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPolicy": {
    "Status": "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPolicy](#)

Décrit la politique de sauvegarde du système de fichiers, en indiquant si les sauvegardes automatiques sont activées ou désactivées.

Type : objet [BackupPolicy](#)

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifecycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

ValidationException

Renvoyé si le AWS Backup service n'est pas disponible dans la Région AWS dans laquelle la demande a été faite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutFileSystemPolicy

Applique un `FileSystemPolicy` Amazon EFS à un système de fichiers Amazon EFS. Une politique de système de fichiers est une politique basée sur les ressources IAM et peut contenir plusieurs déclarations de politique. Un système de fichiers possède toujours exactement une politique de système de fichiers, qui peut être la stratégie par défaut ou une politique explicite définie ou mise à jour à l'aide de cette opération d'API. Les politiques du système de fichiers EFS sont limitées à 20 000 caractères. Lorsqu'une politique explicite est définie, elle remplace la stratégie par défaut. Pour plus d'informations sur la politique de système de fichiers par défaut, consultez la section [Politique de système de fichiers EFS par défaut](#).

Note

Les politiques du système de fichiers EFS sont limitées à 20 000 caractères.

Cette opération exige des autorisations pour l'action `elasticfilesystem:PutFileSystemPolicy`.

Syntaxe de la demande

```
PUT /2015-02-01/file-systems/FileSystemId/policy HTTP/1.1
Content-type: application/json
```

```
{
  "BypassPolicyLockoutSafetyCheck": boolean,
  "Policy": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[FileSystemId](#)

ID du système de fichiers EFS pour lequel vous créez ou mettez à jour `FileSystemPolicy`.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[BypassPolicyLockoutSafetyCheck](#)

(Facultatif) Une valeur booléenne qui indique s'il faut ignorer ou non le contrôle de sécurité du verrouillage `FileSystemPolicy`. Le contrôle de sécurité du verrouillage détermine si la politique de la demande verrouillera ou empêchera le principal IAM qui émet la demande d'effectuer de futures demandes `PutFileSystemPolicy` sur ce système de fichiers. Définissez `BypassPolicyLockoutSafetyCheck` sur `True` uniquement lorsque vous avez l'intention d'empêcher le principal IAM à l'origine de la demande d'effectuer d'autres demandes `PutFileSystemPolicy` sur ce système de fichiers. La valeur par défaut est `False`.

Type : booléen

Obligatoire : non

[Policy](#)

La `FileSystemPolicy` que vous créez. Accepte une définition de politique au format JSON. Les politiques du système de fichiers EFS sont limitées à 20 000 caractères. Pour en savoir plus sur les éléments qui constituent une politique de système de fichiers, consultez la section [Politiques basées sur les ressources dans Amazon EFS](#).

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 20000.

Modèle : `[\s\S]+`

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
```

```
"FileSystemId": "string",  
"Policy": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[FileSystemId](#)

Spécifie le système de fichiers EFS auquel s'applique `FileSystemPolicy`.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[Policy](#)

Le JSON formaté `FileSystemPolicy` pour le système de fichiers EFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 20000.

Modèle : `[\s\S]+`

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifecycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

InvalidPolicyException

Renvoyé si le `FileSystemPolicy` est mal formé ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant. Renvoyé en cas d'erreur liée au contrôle de sécurité lié à la politique de verrouillage.

Code d'état HTTP : 400

Exemples

Création d'un EFS `FileSystemPolicy`

La demande suivante crée un système `FileSystemPolicy` qui permet à tous les AWS principaux de monter le système de fichiers EFS spécifié avec des autorisations de lecture et d'écriture.

Exemple de demande

```
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": ["*"]
      }
    }
  ],
```

```
    }  
  ]  
}
```

Exemple de réponse

```
{  
  "Version": "2012-10-17",  
  "Id": "1",  
  "Statement": [  
    {  
      "Sid": "efs-statement-abcdef01-1111-bbbb-2222-111122224444",  
      "Effect": "Allow",  
      "Action": [  
        "elasticfilesystem:ClientMount",  
        "elasticfilesystem:ClientWrite"  
      ],  
      "Principal": {  
        "AWS": ["*"]  
      },  
      "Resource": "arn:aws:elasticfilesystem:us-east-1:1111222233334444:file-  
system/fs-01234567"  
    }  
  ]  
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutLifecycleConfiguration

Utilisez cette action pour gérer le stockage de votre système de fichiers. Le LifecycleConfiguration se compose d'un ou de plusieurs objets LifecyclePolicy qui définissent les éléments suivants :

- **TransitionToIA**— Quand déplacer des fichiers dans le système de fichiers depuis le stockage principal (classe de stockage standard) vers le stockage à accès peu fréquent (IA).
- **TransitionToArchive**— Quand déplacer les fichiers du système de fichiers depuis leur classe de stockage actuelle (stockage IA ou standard) vers le stockage d'archives.

Les systèmes de fichiers ne peuvent pas passer au stockage d'archives avant de passer au stockage IA. Par conséquent, TransitionToArchive il ne doit pas être défini ou doit être postérieur à TransitionTo IA.

Note

La classe de stockage Archive n'est disponible que pour les systèmes de fichiers qui utilisent le mode débit élastique et le mode de performance General Purpose.

- **TransitionToPrimaryStorageClass**— S'il faut replacer les fichiers du système de fichiers vers le stockage principal (classe de stockage standard) après leur accès dans le stockage IA ou dans le stockage des archives.

Pour plus d'informations, consultez [Gestion du stockage du système de fichiers](#).

Chaque système de fichiers Amazon EFS prend en charge une configuration de cycle de vie, qui s'applique à tous les fichiers du système de fichiers. Si un LifecycleConfiguration objet existe déjà pour le système de fichiers spécifié, un appel PutLifecycleConfiguration modifie la configuration existante. Un appel PutLifecycleConfiguration avec un tableau LifecyclePolicies vide dans le corps de la requête supprime tout tableau existant LifecycleConfiguration. Dans la demande, précisez ce qui suit :

- ID du système de fichiers pour lequel vous activez, désactivez ou modifiez la gestion du cycle de vie.

- Un tableau `LifecyclePolicies` d'objets `LifecyclePolicy` qui définit le moment où les fichiers doivent être déplacés vers le stockage IA, vers le stockage d'archives et vers le stockage principal.

Note

Amazon EFS exige que chaque objet `LifecyclePolicy` n'ait qu'une seule transition. Le tableau `LifecyclePolicies` doit donc être structuré avec des objets `LifecyclePolicy` distincts. Pour plus d'informations, veuillez consulter les exemples de demandes dans la section suivante.

Cette opération exige des autorisations pour l'opération `elasticfilesystem:PutLifecycleConfiguration`.

Pour appliquer un `LifecycleConfiguration` objet à un système de fichiers chiffré, vous devez disposer des mêmes AWS Key Management Service autorisations que lorsque vous avez créé le système de fichiers chiffré.

Syntaxe de la demande

```
PUT /2015-02-01/file-systems/FileSystemId/lifecycle-configuration HTTP/1.1
Content-type: application/json
```

```
{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "string",
      "TransitionToIA": "string",
      "TransitionToPrimaryStorageClass": "string"
    }
  ]
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

FileSystemId

ID du système de fichiers pour lequel créer l'objet `LifecycleConfiguration` (chaîne).

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[LifecyclePolicies](#)

Tableau d'objets `LifecyclePolicy` qui définissent l'objet `LifecycleConfiguration` du système de fichiers. Un `LifecycleConfiguration` objet fournit à la gestion du cycle de vie les informations suivantes :

- **TransitionToIA**— Quand déplacer des fichiers dans le système de fichiers depuis le stockage principal (classe de stockage standard) vers le stockage à accès peu fréquent (IA).
- **TransitionToArchive**— Quand déplacer les fichiers du système de fichiers depuis leur classe de stockage actuelle (stockage IA ou standard) vers le stockage d'archives.

Les systèmes de fichiers ne peuvent pas passer au stockage d'archives avant de passer au stockage IA. Par conséquent, `TransitionToArchive` il ne doit pas être défini ou doit être postérieur à `TransitionTo IA`.

Note

La classe de stockage Archive n'est disponible que pour les systèmes de fichiers qui utilisent le mode débit élastique et le mode de performance General Purpose.

- **TransitionToPrimaryStorageClass**— S'il faut remplacer les fichiers du système de fichiers vers le stockage principal (classe de stockage standard) après leur accès dans le stockage IA ou dans le stockage des archives.

Note

Lorsque vous utilisez la commande `put-lifecycle-configuration` CLI ou l'action `PutLifecycleConfiguration` API, Amazon EFS exige que chaque `LifecyclePolicy` objet n'ait qu'une seule transition. Cela signifie que dans un

corps de demande, LifecyclePolicies doit être structuré comme un tableau d'objets LifecyclePolicy, un objet pour chaque transition de stockage. Pour plus d'informations, veuillez consulter les exemples de demandes dans la section suivante.

Type : tableau d'objets [LifecyclePolicy](#)

Membres du tableau : nombre maximum de 3 éléments.

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "string",
      "TransitionToIA": "string",
      "TransitionToPrimaryStorageClass": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[LifecyclePolicies](#)

Un ensemble de politiques de gestion du cycle de vie. EFS prend en charge au maximum une politique par système de fichiers.

Type : tableau d'objets [LifecyclePolicy](#)

Membres du tableau : nombre maximum de 3 éléments.

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifeCycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

Exemples

Créer une configuration de cycle de vie

L'exemple suivant crée un objet `LifecyclePolicy` à l'aide de l'action `PutLifecycleConfiguration`. Cet exemple crée une politique de cycle de vie qui demande à EFS d'effectuer les opérations suivantes :

- Déplacez tous les fichiers du système de fichiers auxquels vous n'avez pas accédé dans le stockage Standard au cours des 30 derniers jours vers le stockage IA.
- Déplacez tous les fichiers du système de fichiers auxquels vous n'avez pas accédé dans le stockage standard au cours des 90 derniers jours vers le stockage d'archives.
- S'il faut replacer les fichiers vers le stockage principal (standard) après leur accès dans le stockage IA ou dans le stockage d'archives. La classe de stockage Archive n'est disponible que pour les

systèmes de fichiers qui utilisent le mode débit élastique et le mode de performance General Purpose.

Pour plus d'informations, consultez les sections [Classes de stockage EFS](#) et [Gestion du stockage des systèmes de fichiers](#).

Exemple de demande

```
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"
    }
  ]
}
```

Exemple de réponse

```
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"
}
]
```

Exemple de demande put-lifecycle-configuration CLI

Cet exemple illustre une utilisation de PutLifecycleConfiguration.

Exemple de demande

```
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
```

Exemple de réponse

```
{
  "LifecyclePolicies": [
    {
      "TransitionToArchive": "AFTER_90_DAYS"
    },
    {
      "TransitionToIA": "AFTER_30_DAYS"
    },
    {
      "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
    }
  ]
}
```

Désactiver la gestion du cycle de vie ()

L'exemple suivant désactive la gestion du cycle de vie pour le système de fichiers spécifié.

Exemple de demande

```
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": [ ]
}
```

Exemple de réponse

```
HTTP/1.1 200 OK
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
Content-type: application/json
Content-Length: 86

{
  "LifecyclePolicies": [ ]
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

TagResource

Crée une balise pour une ressource EFS. Vous pouvez créer des balises pour les systèmes de fichiers EFS et les points d'accès à l'aide de cette opération d'API.

Cette opération exige des autorisations pour l'action `elasticfilesystem:TagResource`.

Syntaxe de la demande

```
POST /2015-02-01/resource-tags/ResourceId HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ResourceId

L'ID indiquant la ressource EFS pour laquelle vous souhaitez créer une balise.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(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})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Tags

Un tableau des objets `Tag` à ajouter. Chaque objet `Tag` est une paire clé-valeur.

Type : tableau d'objets [Tag](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

AccessPointNotFound

Renvoyé si la `AccessPointId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

BadRequest

Renvoyé si la demande est mal formulée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

Exemples

Créer des balises sur un système de fichiers

La requête suivante crée trois balises ("key1", "key2", et "key3") sur le système de fichiers spécifié.

Exemple de demande

```
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"
    }
  ]
}
```

Exemple de réponse

```
HTTP/1.1 204 no content
x-amzn-RequestId: 01234567-89ab-cdef-0123-456789abcdef
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UntagResource

Supprime les identifications d'une ressource EFS Vous pouvez supprimer des balises des systèmes de fichiers EFS et des points d'accès à l'aide de cette opération d'API.

Cette opération exige des autorisations pour l'action `elasticfilesystem:UntagResource`.

Syntaxe de la demande

```
DELETE /2015-02-01/resource-tags/ResourceId?tagKeys=TagKeys HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ResourceId](#)

Détermine la ressource EFS dont vous souhaitez supprimer les balises.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(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})$`

Obligatoire : oui

[TagKeys](#)

Les clés des paires de balises clé-valeur que vous souhaitez supprimer de la ressource EFS spécifiée.

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : `^(?![aA]{1}[wW]{1}[sS]{1}:)([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]+)$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

AccessPointNotFound

Renvoyé si la `AccessPointId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

BadRequest

Renvoyé si la demande est mal formulée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateFileSystem

Met à jour le mode de débit ou la quantité de débit alloué d'un système de fichiers existant.

Syntaxe de la demande

```
PUT /2015-02-01/file-systems/FileSystemId HTTP/1.1
Content-type: application/json

{
  "ProvisionedThroughputInMibps": number,
  "ThroughputMode": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

FileSystemId

L'ID du système de fichiers que vous souhaitez mettre à jour.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

ProvisionedThroughputInMibps

(Facultatif) Le débit, mesuré en mégaoctets par seconde (MiBps), que vous souhaitez configurer pour le système de fichiers que vous créez. Obligatoire si `ThroughputMode` est défini sur `provisioned`. Les valeurs valides sont comprises entre 1 et 3414 MiBps, la limite supérieure dépendant de la région. Pour augmenter cette limite, contactez Support. Pour plus d'informations, consultez [Quotas Amazon EFS que vous pouvez augmenter](#) dans le Guide de l'utilisateur Amazon EFS.

Type : double

Plage valide : valeur minimum de 1,0.

Obligatoire : non

ThroughputMode

(Facultatif) Met à jour le mode de débit du système de fichiers. Si vous ne mettez pas à jour votre mode de débit, vous n'avez pas besoin de fournir cette valeur dans votre demande. Si vous changez ThroughputMode en provisioned, vous devez également définir une valeur pour ProvisionedThroughputInMibps.

Type : String

Valeurs valides : bursting | provisioned | elastic

Obligatoire : non

Syntaxe de la réponse

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"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 202.

Les données suivantes sont renvoyées au format JSON par le service.

AvailabilityZoneId

Identifiant unique et cohérent de la Zone de disponibilité dans laquelle se trouve le système de fichiers, valide uniquement pour les systèmes de fichiers Zone unique. Par exemple, use1-az1 il s'agit d'un identifiant de zone de disponibilité pour le Région AWS us-east-1, qui possède le même emplacement dans chaque cas. Compte AWS

Type : String

AvailabilityZoneName

Décrit la zone de AWS disponibilité dans laquelle se trouve le système de fichiers et n'est valide que pour les systèmes de fichiers One Zone. Pour de plus amples informations, consultez [Utilisation de classes de stockage EFS](#) dans le Guide de l'utilisateur Amazon EFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : . +

CreationTime

Heure de création du système de fichiers, en secondes (depuis 1970-01-01T 00:00:00 Z).

Type : Timestamp

[CreationToken](#)

Chaîne opaque spécifiée dans la demande.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : .+

[Encrypted](#)

Valeur booléenne qui, si la valeur est true, indique que le système de fichiers est chiffré.

Type : booléen

[FileSystemArn](#)

Le nom de ressource Amazon Resource Name (ARN) pour le système de fichiers EFS, au format `arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id`. Exemple avec des exemples de données : `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Type : String

[FileSystemId](#)

ID du système de fichiers, attribué par Amazon EFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

[FileSystemProtection](#)

Décrit la protection du système de fichiers.

Type : objet [FileSystemProtectionDescription](#)

[KmsKeyId](#)

Identifiant AWS KMS key utilisé pour protéger le système de fichiers chiffré.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^([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

Phase du cycle de vie du système de fichiers.

Type : String

Valeurs valides : `creating | available | updating | deleting | deleted | error`

Name

Vous pouvez ajouter des balises à un système de fichiers, y compris une balise Name. Pour de plus amples informations, veuillez consulter [CreateFileSystem](#). Si le système de fichiers possède une balise Name, Amazon EFS renvoie la valeur dans ce champ.

Type : String

Contraintes de longueur : longueur maximale de 256.

Modèle : `^([\p{L}\p{Z}\p{N}_.: /+=\ -@]*)$`

NumberOfMountTargets

Le nombre actuel de cibles de Montage du système de fichiers. Pour de plus amples informations, veuillez consulter [CreateMountTarget](#).

Type : entier

Plage valide : Valeur minimum de 0.

OwnerId

Celui Compte AWS qui a créé le système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

[PerformanceMode](#)

Mode de performances du système de fichiers.

Type : String

Valeurs valides : `generalPurpose` | `maxIO`

[ProvisionedThroughputInMibps](#)

Quantité de débit allouée, mesurée en MiBps, pour le système de fichiers. Valable pour les systèmes de fichiers utilisant `ThroughputMode` défini sur `provisioned`.

Type : double

Plage valide : Valeur minimum de 1,0.

[SizeInBytes](#)

La dernière taille mesurée connue (en octets) des données stockées dans le système de fichiers, dans son champ `Value`, et l'heure à laquelle cette taille a été déterminée dans son champ `Timestamp`. La valeur `Timestamp` est le nombre entier de secondes écoulées depuis 1970-01-01T 00:00:00 Z. La valeur `SizeInBytes` ne représente pas la taille d'un instantané cohérent du système de fichiers, mais elle est finalement cohérente lorsqu'aucune écriture n'est effectuée dans le système de fichiers. Cela signifie que `SizeInBytes` représente la taille réelle uniquement si le système de fichiers n'est pas `Modifié` pendant une période supérieure à deux heures. Dans le cas contraire, la valeur ne correspond pas exactement à la taille du système de fichiers à un Moment donné.

Type : objet [FileSystemSize](#)

[Tags](#)

Tags associés au système de fichiers, présentés sous forme de tableau des objets `Tag`.

Type : tableau d'objets [Tag](#)

[ThroughputMode](#)

Affiche le mode de débit du système de fichiers. Pour plus d'informations, consultez les [Modes de débit](#) dans le Guide de l'utilisateur Amazon EFS.

Type : String

Valeurs valides : `bursting` | `provisioned` | `elastic`

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifecycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InsufficientThroughputCapacity

Renvoyé si la capacité est insuffisante pour fournir un débit supplémentaire. Cette valeur peut être renvoyée lorsque vous essayez de créer un système de fichiers en mode débit alloué, lorsque vous essayez d'augmenter le débit alloué d'un système de fichiers existant ou lorsque vous essayez de faire passer un système de fichiers existant du mode débit en rafale au mode débit alloué. Réessayez ultérieurement.

HTTP Status Code: 503

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

ThroughputLimitExceeded

Renvoie si le mode de débit ou la quantité de débit alloué ne peuvent pas être Modifiés car la limite de débit de 1024 Mbits/s a été atteinte.

Code d'état HTTP : 400

TooManyRequests

Renvoyé si vous n'attendez pas au moins 24 heures avant de modifier le mode de débit ou de diminuer la valeur du débit alloué.

Code d'état HTTP : 429

Voir aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateFileSystemProtection

Met à jour la protection sur le système de fichiers.

Cette opération exige des autorisations pour l'action `elasticfilesystem:UpdateFileSystemProtection`.

Syntaxe de la demande

```
PUT /2015-02-01/file-systems/FileSystemId/protection HTTP/1.1
Content-type: application/json
```

```
{
  "ReplicationOverwriteProtection": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[FileSystemId](#)

ID du système de fichiers à mettre à jour.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[ReplicationOverwriteProtection](#)

État de la protection contre le remplacement de la réplication du système de fichiers.

- **ENABLED** – Le système de fichiers ne peut pas être utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est inscriptible. La protection contre le remplacement de la réplication est par défaut **ENABLED**.

- **DISABLED** – Le système de fichiers peut être utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est en lecture seule et ne peut être modifié que par la réplication EFS.
- **REPLICATING** – Le système de fichiers est utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est en lecture seule et n'est modifié que par la réplication EFS.

Si la configuration de réplication est supprimée, la protection par écrasement de réplication du système de fichiers est réactivée et le système de fichiers devient inscriptible.

Type : String

Valeurs valides : ENABLED | DISABLED | REPLICATING

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "ReplicationOverwriteProtection": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ReplicationOverwriteProtection](#)

État de la protection contre le remplacement de la réplication du système de fichiers.

- **ENABLED** – Le système de fichiers ne peut pas être utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est inscriptible. La protection contre le remplacement de la réplication est par défaut ENABLED.
- **DISABLED** – Le système de fichiers peut être utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est en lecture seule et ne peut être modifié que par la réplication EFS.

- **REPLICATING** – Le système de fichiers est utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est en lecture seule et n'est modifié que par la réplication EFS.

Si vous supprimez la configuration de réplication, la protection contre l'écrasement par réplication du système de fichiers est réactivée et le système de fichiers devient accessible en écriture.

Type : String

Valeurs valides : **ENABLED** | **DISABLED** | **REPLICATING**

Erreurs

BadRequest

Renvoyé si la demande est mal formée ou contient une erreur telle qu'une valeur de paramètre non valide ou un paramètre obligatoire manquant.

Code d'état HTTP : 400

FileSystemNotFound

Renvoyé si la `FileSystemId` valeur spécifiée n'existe pas dans celle du Compte AWS demandeur.

Code d'état HTTP : 404

IncorrectFileSystemLifecycleState

Renvoyé si l'état du cycle de vie du système de fichiers n'est pas « disponible ».

Code d'état HTTP : 409

InsufficientThroughputCapacity

Renvoyé si la capacité est insuffisante pour fournir un débit supplémentaire. Cette valeur peut être renvoyée lorsque vous essayez de créer un système de fichiers en mode débit alloué, lorsque vous essayez d'augmenter le débit alloué d'un système de fichiers existant ou lorsque vous essayez de faire passer un système de fichiers existant du mode débit en rafale au mode débit alloué. Réessayez ultérieurement.

HTTP Status Code: 503

InternalServerError

Renvoyé si une erreur s'est produite côté serveur.

Code d'état HTTP : 500

ReplicationAlreadyExists

Renvoyé si le système de fichiers est déjà inclus dans une configuration de réplication. >

Code d'état HTTP : 409

ThroughputLimitExceeded

Renvoie si le mode de débit ou la quantité de débit alloué ne peuvent pas être modifiés car la limite de débit de 1024 Mbits/s a été atteinte.

Code d'état HTTP : 400

TooManyRequests

Renvoyé si vous n'attendez pas au moins 24 heures avant de modifier le mode de débit ou de diminuer la valeur du débit alloué.

Code d'état HTTP : 429

Voir aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

Types de données

Les types de données suivants sont pris en charge :

- [AccessPointDescription](#)
- [BackupPolicy](#)
- [CreationInfo](#)
- [Destination](#)
- [DestinationToCreate](#)
- [FileSystemDescription](#)
- [FileSystemProtectionDescription](#)
- [FileSystemSize](#)
- [LifecyclePolicy](#)
- [MountTargetDescription](#)
- [PosixUser](#)
- [ReplicationConfigurationDescription](#)
- [ResourceIdPreference](#)
- [RootDirectory](#)
- [Tag](#)

AccessPointDescription

Fournit une description d'un point d'accès au système de fichiers EFS.

Table des matières

AccessPointArn

L'Amazon Resource Name (ARN) associé au point d'accès.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}$`

Obligatoire : non

AccessPointId

L'ID du point d'accès, attribué par Amazon EFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:access-point/fsap-[0-9a-f]{8,40}|fsap-[0-9a-f]{8,40})$`

Obligatoire : non

ClientToken

Chaîne opaque spécifiée dans la demande pour garantir la création idempotente.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `.+`

Obligatoire : non

FileSystemId

ID du système de fichiers EFS auquel le point d'accès s'applique.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : non

LifeCycleState

Identifie la phase du cycle de vie du point d'accès.

Type : String

Valeurs valides : `creating | available | updating | deleting | deleted | error`

Obligatoire : non

Name

Nom de ce point d'accès. Il s'agit de la valeur de la balise Name.

Type : chaîne

Obligatoire : non

OwnerId

Identifie Compte AWS le propriétaire de la ressource du point d'accès.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

Obligatoire : non

PosixUser

L'identité POSIX complète, y compris l'ID utilisateur, l'ID de groupe et le groupe secondaire IDs sur le point d'accès utilisé pour toutes les opérations sur les fichiers par les clients NFS utilisant le point d'accès.

Type : objet [PosixUser](#)

Obligatoire : non

RootDirectory

Répertoire du système de fichiers Amazon EFS que le point d'accès expose en tant que répertoire racine aux clients NFS utilisant le point d'accès.

Type : objet [RootDirectory](#)

Obligatoire : non

Tags

Les balises associées au point d'accès, présentées sous la forme d'un tableau d'objets Tag.

Type : tableau d'objets [Tag](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupPolicy

Politique de sauvegarde du système de fichiers utilisée pour créer des sauvegardes quotidiennes automatiques. Si le statut a une valeur égale à **ENABLED**, le système de fichiers est automatiquement sauvegardé. Pour plus d'informations, consultez [Sauvegardes automatiques](#).

Table des matières

Status

Décrit l'état de la politique de sauvegarde du système de fichiers.

- **ENABLED** – EFS sauvegarde automatiquement le système de fichiers.
- **ENABLING** – EFS active les sauvegardes automatiques du système de fichiers.
- **DISABLED** – Les sauvegardes automatiques sont désactivées pour le système de fichiers.
- **DISABLING** – EFS désactive les sauvegardes automatiques du système de fichiers.

Type : String

Valeurs valides : ENABLED | ENABLING | DISABLED | DISABLING

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

CreationInfo

Obligatoire si le `RootDirectory > Path` spécifié n'existe pas. Spécifie le POSIX IDs et les autorisations à appliquer au `RootDirectory > Path` du point d'accès. Si le répertoire racine du point d'accès n'existe pas, EFS le crée avec ces paramètres lorsqu'un client se connecte au point d'accès. Lors de la spécification de `CreationInfo`, vous devez inclure des valeurs pour toutes les propriétés.

Amazon EFS crée un répertoire racine uniquement si vous avez fourni le `CreationInfo : OwnUid`, le `OwnGid` et les autorisations pour le répertoire. Si vous ne fournissez pas ces informations, Amazon EFS ne crée pas le répertoire racine. Si le répertoire racine n'existe pas, les tentatives de montage au moyen du point d'accès échoueront.

Important

Si vous ne fournissez pas de valeur pour `CreationInfo` et que le `RootDirectory` spécifié n'existe pas, les tentatives de montage du système de fichiers à l'aide du point d'accès échouent.

Table des matières

OwnerGid

Spécifie l'ID de groupe POSIX à appliquer à `RootDirectory`. Accepte les valeurs comprises entre 0 et 2^{32} (4294967295).

Type : long

Plage valide : Valeur minimum de 0. Valeur maximale de 4294967295.

Obligatoire : oui

OwnerUid

Spécifie l'ID utilisateur POSIX à appliquer à `RootDirectory`. Accepte les valeurs comprises entre 0 et 2^{32} (4294967295).

Type : long

Plage valide : Valeur minimum de 0. Valeur maximale de 4294967295.

Obligatoire : oui

Permissions

Spécifie les autorisations POSIX à appliquer à `RootDirectory`, sous la forme d'un nombre octal représentant les bits de mode du fichier.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 4.

Modèle : `^[0-7]{3,4}$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Destination

Décrit le système de fichiers de destination dans la configuration de réplication.

Table des matières

FileSystemId

ID du système de fichiers Amazon EFS de destination.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

Region

Le système de fichiers Région AWS dans lequel se trouve le système de fichiers de destination.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Obligatoire : oui

Status

Décrit l'état de la configuration de réplication. Pour plus d'informations sur l'état de réplication, consultez la section [Affichage des détails de réplication](#) dans le guide de l'utilisateur Amazon EFS.

Type : String

Valeurs valides : ENABLED | ENABLING | DELETING | ERROR | PAUSED | PAUSING

Obligatoire : oui

LastReplicatedTimestamp

Heure à laquelle la dernière synchronisation s'est terminée avec succès sur le système de fichiers de destination. Toutes les modifications apportées aux données du système de fichiers source

avant cette date ont été correctement répliquées sur le système de fichiers de destination. Les modifications survenues après cette période risquent de ne pas être entièrement répliquées.

Type : Timestamp

Obligatoire : non

OwnerId

ID du système de fichiers Compte AWS dans lequel réside le système de fichiers de destination.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

Obligatoire : non

RoleArn

Amazon Resource Name (ARN) du rôle IAM dans le compte source qui permet à Amazon EFS d'effectuer la réplication en son nom. Cela est facultatif pour la réplication entre comptes identiques et obligatoire pour la réplication entre comptes.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `arn:(aws[a-zA-Z-]*)?:iam::\\d{12}:role/?[a-zA-Z_0-9+=, .@\\-_/]+`

Obligatoire : non

StatusMessage

Message fournissant des détails sur la configuration PAUSED ou l'ERROR état de la configuration de destination de réplication. Pour plus d'informations sur les messages d'état de réplication, consultez la section [Affichage des détails de réplication](#) dans le guide de l'utilisateur Amazon EFS.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

DestinationToCreate

Décrit le système de fichiers de destination nouveau ou existant pour la configuration de réplication.

- Si vous souhaitez effectuer une réplication vers un nouveau système de fichiers, ne spécifiez pas l'ID du système de fichiers de destination. Amazon EFS crée un nouveau système de fichiers vide. Pour le stockage One Zone, spécifiez la zone de disponibilité dans laquelle créer le système de fichiers. Pour utiliser une AWS Key Management Service clé autre que la clé KMS par défaut, spécifiez-la. Pour plus d'informations, consultez [la section Configuration de la réplication vers le nouveau système de fichiers Amazon EFS](#) dans le guide de l'utilisateur Amazon EFS.

Note

Une fois le système de fichiers créé, vous ne pouvez pas modifier la clé KMS ni le mode de performance.

- Si vous souhaitez effectuer une réplication vers un système de fichiers existant appartenant au même compte que le système de fichiers source, vous devez fournir l'ID ou le nom de ressource Amazon (ARN) du système de fichiers vers lequel effectuer la réplication. La protection contre le remplacement par réplication du système de fichiers doit être désactivée. Pour plus d'informations, consultez la section [Réplication vers un système de fichiers existant](#) dans le guide de l'utilisateur Amazon EFS.
- Si vous répliquez le système de fichiers vers un système de fichiers situé dans un compte différent du système de fichiers source (réplication entre comptes), vous devez fournir l'ARN du système de fichiers et le rôle IAM qui permet à Amazon EFS d'effectuer la réplication sur le compte de destination. La protection contre le remplacement par réplication du système de fichiers doit être désactivée. Pour plus d'informations, consultez la section [Replication Comptes AWS dans](#) le guide de l'utilisateur Amazon EFS.

Table des matières

AvailabilityZoneName

Pour créer un système de fichiers utilisant le stockage Zone unique, spécifiez le nom de la Zone de disponibilité dans laquelle vous souhaitez créer le système de fichiers de destination.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : . +

Obligatoire : non

FileSystemId

L'ID ou l'ARN du système de fichiers à utiliser pour la destination. Pour la réplication entre comptes, il doit s'agir d'un ARN. La réplication de l'écrasement du système de fichiers doit être désactivée. Si aucun ID ou ARN n'est spécifié, un nouveau système de fichiers est créé.

 Note

Lorsque vous configurez initialement la réplication vers un système de fichiers existant, Amazon EFS écrit des données dans le système de fichiers de destination ou en supprime des données existantes afin qu'elles correspondent aux données du système de fichiers source. Si vous ne souhaitez pas modifier les données du système de fichiers de destination, vous devez plutôt les répliquer vers un nouveau système de fichiers. Pour de plus amples informations, veuillez consulter <https://docs.aws.amazon.com/efs/latest/ug/create-replication.html>.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : non

KmsKeyId

Spécifiez la clé AWS Key Management Service (AWS KMS) que vous souhaitez utiliser pour chiffrer le système de fichiers de destination. Si vous ne spécifiez pas de clé KMS, Amazon EFS utilise votre clé KMS par défaut pour Amazon EFS, /aws/elasticfilesystem. Cet ID peut être dans l'un des formats suivants :

- ID de clé - L'identifiant unique de la clé, par exemple 1234abcd-12ab-34cd-56ef-1234567890ab.

- ARN - L'ARN de la clé, par exemple `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- Alias de clé - Un nom d'affichage précédemment créé pour une clé, par exemple `alias/projectKey1`.
- ARN d'alias de clé - L'ARN pour un alias de clé, par exemple `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}|mrk-[0-9a-f]{32}|alias/[a-zA-Z0-9/_-]+|(arn:aws[-a-z]*:kms:[a-zA-Z0-9-]+:\d{12}:((key/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})|(key/mrk-[0-9a-f]{32})|(alias/[a-zA-Z0-9/_-]+))))$`

Obligatoire : non

Region

Pour créer un système de fichiers utilisant le stockage régional, spécifiez le système de fichiers Région AWS dans lequel vous souhaitez créer le système de fichiers de destination. La région doit être activée pour Compte AWS le propriétaire du système de fichiers source. Pour plus d'informations, consultez [la section Gestion Régions AWS](#) dans le Guide de référence AWS général.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Obligatoire : non

RoleArn

Amazon Resource Name (ARN) du rôle IAM dans le compte source qui permet à Amazon EFS d'effectuer la réplication en son nom. Cela est facultatif pour la réplication entre comptes identiques et obligatoire pour la réplication entre comptes.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.\@\_/-]+`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

FileSystemDescription

Une description du système de fichiers.

Table des matières

CreationTime

Heure de création du système de fichiers, en secondes (depuis 1970-01-01T 00:00:00 Z).

Type : Timestamp

Obligatoire : oui

CreationToken

Chaîne opaque spécifiée dans la demande.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : .+

Obligatoire : oui

FileSystemId

ID du système de fichiers, attribué par Amazon EFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

LifeCycleState

Phase du cycle de vie du système de fichiers.

Type : String

Valeurs valides : `creating` | `available` | `updating` | `deleting` | `deleted` | `error`

Obligatoire : oui

NumberOfMountTargets

Le nombre actuel de cibles de montage du système de fichiers. Pour de plus amples informations, veuillez consulter [CreateMountTarget](#).

Type : entier

Plage valide : Valeur minimum de 0.

Obligatoire : oui

OwnerId

Celui Compte AWS qui a créé le système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : `^\d{12})|(\d{4}-\d{4}-\d{4})$`

Obligatoire : oui

PerformanceMode

Mode de performances du système de fichiers.

Type : String

Valeurs valides : `generalPurpose` | `maxIO`

Obligatoire : oui

SizeInBytes

La dernière taille mesurée connue (en octets) des données stockées dans le système de fichiers, dans son champ `Value`, et l'heure à laquelle cette taille a été déterminée dans son champ `Timestamp`. La valeur `Timestamp` est le nombre entier de secondes écoulées depuis 1970-01-01T 00:00:00 Z. La valeur `SizeInBytes` ne représente pas la taille d'un instantané cohérent du système de fichiers, mais elle est finalement cohérente lorsqu'aucune écriture

n'est effectuée dans le système de fichiers. Cela signifie que `SizeInBytes` représente la taille réelle uniquement si le système de fichiers n'est pas Modifié pendant une période supérieure à deux heures. Dans le cas contraire, la valeur ne correspond pas exactement à la taille du système de fichiers à un Moment donné.

Type : objet [FileSystemSize](#)

Obligatoire : oui

Tags

Tags associés au système de fichiers, présentés sous forme de tableau des objets Tag.

Type : tableau d'objets [Tag](#)

Obligatoire : oui

AvailabilityZoneId

Identifiant unique et cohérent de la Zone de disponibilité dans laquelle se trouve le système de fichiers, valide uniquement pour les systèmes de fichiers Zone unique. Par exemple, `use1-az1` il s'agit d'un identifiant de zone de disponibilité pour le Région AWS `us-east-1`, qui possède le même emplacement dans chaque cas. Compte AWS

Type : chaîne

Obligatoire : non

AvailabilityZoneName

Décrit la zone de AWS disponibilité dans laquelle se trouve le système de fichiers et n'est valide que pour les systèmes de fichiers One Zone. Pour de plus amples informations, consultez [Utilisation de classes de stockage EFS](#) dans le Guide de l'utilisateur Amazon EFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : .+

Obligatoire : non

Encrypted

Valeur booléenne qui, si la valeur est true, indique que le système de fichiers est chiffré.

Type : booléen

Obligatoire : non

FileSystemArn

Le nom de ressource Amazon Resource Name (ARN) pour le système de fichiers EFS, au format `arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id`. Exemple avec des exemples de données : `arn:aws:elasticfilesystem:us-west-2:1111333322228888:file-system/fs-01234567`

Type : chaîne

Obligatoire : non

FileSystemProtection

Décrit la protection du système de fichiers.

Type : objet [FileSystemProtectionDescription](#)

Obligatoire : non

KmsKeyId

Identifiant AWS KMS key utilisé pour protéger le système de fichiers chiffré.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^([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/_-]+))))$`

Obligatoire : non

Name

Vous pouvez ajouter des balises à un système de fichiers, y compris une balise Name. Pour de plus amples informations, veuillez consulter [CreateFileSystem](#). Si le système de fichiers possède une balise Name, Amazon EFS renvoie la valeur dans ce champ.

Type : String

Contraintes de longueur : longueur maximale de 256.

Modèle : `^([\p{L}\p{Z}\p{N}_.: /+=\ -@]*)$`

Obligatoire : non

ProvisionedThroughputInMibps

Quantité de débit allouée, mesurée en MiBps, pour le système de fichiers. Valable pour les systèmes de fichiers utilisant ThroughputMode défini sur provisioned.

Type : double

Plage valide : valeur minimum de 1,0.

Obligatoire : non

ThroughputMode

Affiche le mode de débit du système de fichiers. Pour plus d'informations, consultez les [Modes de débit](#) dans le Guide de l'utilisateur Amazon EFS.

Type : String

Valeurs valides : `bursting` | `provisioned` | `elastic`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

FileSystemProtectionDescription

Décrit la protection d'un système de fichiers.

Table des matières

ReplicationOverwriteProtection

État de la protection contre le remplacement de la réplication du système de fichiers.

- **ENABLED** – Le système de fichiers ne peut pas être utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est inscriptible. La protection contre le remplacement de la réplication est par défaut ENABLED.
- **DISABLED** – Le système de fichiers peut être utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est en lecture seule et ne peut être modifié que par la réplication EFS.
- **REPLICATING** – Le système de fichiers est utilisé comme système de fichiers de destination dans une configuration de réplication. Le système de fichiers est en lecture seule et n'est modifié que par la réplication EFS.

Si vous supprimez la configuration de réplication, la protection contre l'écrasement par réplication du système de fichiers est réactivée et le système de fichiers devient accessible en écriture.

Type : String

Valeurs valides : ENABLED | DISABLED | REPLICATING

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

FileSystemSize

La dernière taille mesurée connue (en octets) des données stockées dans le système de fichiers, dans son champ `Value`, et l'heure à laquelle cette taille a été déterminée dans son champ `Timestamp`. La valeur ne représente pas la taille d'un instantané cohérent du système de fichiers, mais elle est finalement cohérente lorsqu'aucune écriture n'est effectuée dans le système de fichiers. Cela signifie que la valeur représente la taille réelle uniquement si le système de fichiers n'est pas modifié pendant une période supérieure à deux heures. Dans le cas contraire, la valeur ne correspond pas nécessairement à la taille exacte du système de fichiers à un moment donné.

Table des matières

Value

La dernière taille mesurée connue (en octets) des données stockées dans le système de fichiers.

Type : long

Plage valide : Valeur minimum de 0.

Obligatoire : oui

Timestamp

Heure à laquelle la taille des données renvoyées sur le champ `Value` a été déterminée. La valeur est le nombre entier de secondes écoulées depuis 1970-01-01T 00:00:00 Z.

Type : Timestamp

Obligatoire : non

ValueInArchive

Dernière taille mesurée connue (en octets) des données stockées dans la classe de stockage `Archive`.

Type : long

Plage valide : Valeur minimum de 0.

Obligatoire : non

ValueInIA

La dernière taille mesurée connue (en octets) des données stockées dans la classe de stockage Accès peu fréquent.

Type : long

Plage valide : Valeur minimum de 0.

Obligatoire : non

ValueInStandard

La dernière taille mesurée connue (en octets) des données stockées dans la classe de stockage Standard.

Type : long

Plage valide : Valeur minimum de 0.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

LifecyclePolicy

Décrit une politique utilisée par la gestion du cycle de vie qui indique à quel moment les fichiers doivent être transférés vers et hors des classes de stockage. Pour plus d'informations, consultez [Gestion du stockage du système de fichiers](#).

Note

Lorsque vous utilisez la commande `put-lifecycle-configuration` CLI ou l'action `PutLifecycleConfiguration` API, Amazon EFS exige que chaque `LifecyclePolicy` objet n'ait qu'une seule transition. Cela signifie que dans un corps de demande, `LifecyclePolicies` doit être structuré comme un tableau d'objets `LifecyclePolicy`, un objet pour chaque transition. Pour plus d'informations, consultez les exemples de demandes dans [PutLifecycleConfiguration](#).

Table des matières

TransitionToArchive

Nombre de jours après le dernier accès aux fichiers dans le stockage principal (classe de stockage standard) pendant lesquels ils ont été transférés vers le stockage d'archives. Les opérations sur les métadonnées, par exemple l'affichage du contenu d'un répertoire, ne sont pas considérées comme des événements d'accès aux fichiers.

Type : String

Valeurs valides : 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

Obligatoire : non

TransitionToIA

Nombre de jours après le dernier accès aux fichiers dans le stockage principal (classe de stockage standard) pendant lesquels les fichiers doivent être transférés vers le stockage à accès peu fréquent (IA). Les opérations sur les métadonnées, par exemple l'affichage du contenu d'un répertoire, ne sont pas considérées comme des événements d'accès aux fichiers.

Type : String

Valeurs valides : 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

Obligatoire : non

TransitionToPrimaryStorageClass

S'il faut remplacer les fichiers vers le stockage principal (standard) après leur accès dans le stockage IA ou dans le stockage d'archives. Les opérations sur les métadonnées, par exemple l'affichage du contenu d'un répertoire, ne sont pas considérées comme des événements d'accès aux fichiers.

Type : String

Valeurs valides : AFTER_1_ACCESS

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

MountTargetDescription

Fournit une description d'une cible de montage.

Table des matières

FileSystemId

L'ID du système de fichiers pour lequel la cible de montage est destinée.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

LifeCycleState

État du cycle de vie de la cible de montage.

Type : String

Valeurs valides : `creating | available | updating | deleting | deleted | error`

Obligatoire : oui

MountTargetId

ID de cible de montage attribué par le système.

Type : String

Contraintes de longueur : longueur minimale de 13. Longueur maximale de 45.

Modèle : `^fsmt-[0-9a-f]{8,40}$`

Obligatoire : oui

SubnetId

ID du sous-réseau de la cible de montage.

Type : String

Contraintes de longueur : longueur minimale de 15. Longueur maximale de 47.

Modèle : `^subnet-[0-9a-f]{8,40}$`

Obligatoire : oui

AvailabilityZoneId

Identifiant unique et cohérent de la Zone de disponibilité dans laquelle réside la cible de montage. Par exemple, `use1-az1` il s'agit d'un ID AZ pour la région `us-east-1` et il a le même emplacement dans chaque région. Compte AWS

Type : chaîne

Obligatoire : non

AvailabilityZoneName

Nom de la Zone de disponibilité dans laquelle se trouve la cible de montage. Les zones de disponibilité sont associées indépendamment aux noms de chacune d'entre elles. Compte AWS. Par exemple, il se peut que votre zone `us-east-1a` de disponibilité ne soit pas la même que celle `us-east-1a` d'une autre Compte AWS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `.+`

Obligatoire : non

IpAddress

IPv4 Adresse de la cible de montage.

Type : String

Contraintes de longueur : longueur minimale de 7. Longueur maximale de 15.

Modèle : `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`

Obligatoire : non

Ipv6Address

IPv6 Adresse de la cible de montage.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 39

Obligatoire : non

NetworkInterfaceId

ID de l'interface réseau créée par Amazon EFS lors de la création de la cible de montage.

Type : chaîne

Obligatoire : non

OwnerId

Compte AWS ID propriétaire de la ressource.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

Obligatoire : non

VpcId

ID du cloud privé virtuel (VPC) dans lequel la cible de montage est configurée.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

PosixUser

L'identité POSIX complète, y compris l'ID utilisateur, l'ID de groupe et tout groupe secondaire IDs, sur le point d'accès utilisé pour toutes les opérations du système de fichiers effectuées par les clients NFS utilisant le point d'accès.

Table des matières

Gid

ID de groupe POSIX utilisé pour toutes les opérations de système de fichiers utilisant ce point d'accès.

Type : long

Plage valide : Valeur minimum de 0. Valeur maximale de 4294967295.

Obligatoire : oui

Uid

ID utilisateur POSIX utilisé pour toutes les opérations de système de fichiers utilisant ce point d'accès.

Type : long

Plage valide : Valeur minimum de 0. Valeur maximale de 4294967295.

Obligatoire : oui

SecondaryGids

Groupe POSIX secondaire IDs utilisé pour toutes les opérations du système de fichiers utilisant ce point d'accès.

Type : Tableau de longueurs

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 16 éléments.

Plage valide : Valeur minimum de 0. Valeur maximale de 4294967295.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ReplicationConfigurationDescription

Décrit la configuration de réplication pour un système de fichiers spécifique.

Table des matières

CreationTime

Décrit le moment où la configuration de réplication a été créée.

Type : Timestamp

Obligatoire : oui

Destinations

Tableau d'objets de destination. Un seul objet de destination est pris en charge.

Type : tableau d'objets [Destination](#)

Obligatoire : oui

OriginalSourceFileSystemArn

Amazon Resource Name (ARN) du système de fichiers EFS source d'origine dans la configuration de réplication.

Type : String

Obligatoire : oui

SourceFileSystemArn

Amazon Resource Name (ARN) du système de fichiers source actuel dans la configuration de réplication.

Type : String

Obligatoire : oui

SourceFileSystemId

ID du système de fichiers Amazon EFS source qui est répliqué.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:file-system/fs-[0-9a-f]{8,40}|fs-[0-9a-f]{8,40})$`

Obligatoire : oui

SourceFileSystemRegion

Le système de fichiers EFS source Région AWS dans lequel se trouve le système de fichiers EFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `^[a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-{0,1}[0-9]{0,1}$`

Obligatoire : oui

SourceFileSystemOwnerId

ID du système de fichiers source Compte AWS dans lequel réside le système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 14.

Modèle : `^(\\d{12})|(\\d{4}-\\d{4}-\\d{4})$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ResourceIdPreference

Décrit le type de ressource et son identifiant préféré pour celui de l'utilisateur Compte AWS, dans la version actuelle Région AWS.

Table des matières

ResourceIdType

Identifie la préférence d'ID de ressource EFS, soit LONG_ID (17 caractères) soit SHORT_ID (8 caractères).

Type : String

Valeurs valides : LONG_ID | SHORT_ID

Obligatoire : non

Resources

Identifie les ressources Amazon EFS auxquelles s'applique le paramètre de préférence d'identification, FILE_SYSTEM et MOUNT_TARGET.

Type : tableau de chaînes

Valeurs valides : FILE_SYSTEM | MOUNT_TARGET

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RootDirectory

Spécifie le répertoire du système de fichiers Amazon EFS auquel le point d'accès donne accès. Le point d'accès expose le chemin du système de fichiers spécifié en tant que répertoire racine de votre système de fichiers aux applications utilisant le point d'accès. Les clients NFS utilisant le point d'accès peuvent uniquement accéder aux données du point d'accès `RootDirectory` et de ses sous-répertoires.

Table des matières

CreationInfo

(Facultatif) Spécifie le POSIX IDs et les autorisations à appliquer aux points d'accès. Si le `RootDirectory > Path` spécifié n'existe pas, EFS crée le répertoire racine à l'aide des paramètres `CreationInfo` lorsqu'un client se connecte à un point d'accès. Lorsque vous spécifiez le `CreationInfo`, vous devez fournir des valeurs pour toutes les propriétés.

 Important

Si vous ne fournissez pas de valeur pour `CreationInfo` et que le `RootDirectory > Path` spécifié n'existe pas, les tentatives de montage du système de fichiers à l'aide du point d'accès échouent.

Type : objet **CreationInfo**

Obligatoire : non

Path

Spécifie le chemin d'accès sur le système de fichiers EFS à exposer en tant que répertoire racine aux clients NFS à l'aide du point d'accès pour accéder au système de fichiers EFS. Un chemin peut comporter jusqu'à quatre sous-répertoires. Si le chemin spécifié n'existe pas, vous devez fournir le `CreationInfo`.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : $^{\wedge}(\vee|(\vee(?!\backslash.)+[^{\wedge}\$ \# < > ; `| \& ? \{ \} ^ * \wedge n] +) \{ 1, 4 \}) \$$

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Tag

Une balise est une paire clé-valeur. Les caractères autorisés sont les lettres, les espaces et les chiffres qui peuvent être représentés au format UTF-8, ainsi que les caractères suivants : + - = . _ : /.

Table des matières

Key

Clé de la balise (chaîne). La clé ne peut pas commencer par aws :.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : `^(?![aA]{1}[wW]{1}[sS]{1}:)([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]+)$`

Obligatoire : oui

Value

Valeur de la clé de balise.

Type : String

Contraintes de longueur : longueur maximale de 256.

Modèle : `^( [\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]* )$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Historique du document

- Version de l'API : 2015-02-01
- Dernière mise à jour de la documentation : 9 juin 2025

Le tableau suivant présente les modifications importantes apportées au Guide de l'utilisateur Amazon Elastic File System après juillet 2018. Pour recevoir des notifications en cas de mise à jour de cette documentation, abonnez-vous au flux RSS.

Modification	Description	Date
Support pour IPv6	Le protocole Internet version 6 (IPv6) est pris en charge sur le service Amazon EFS APIs et les cibles de montage. Pour plus d'informations sur l'API Amazon EFS, consultez la section API Amazon EFS . Pour plus d'informations sur les cibles de montage, consultez la section Gestion des cibles de montage .	9 juin 2025
Augmentation élastique du débit dans certains Régions AWS	Le débit de lecture maximal pour les systèmes de fichiers utilisant le débit élastique dans les régions suivantes est passé de 20 GiBps à 60 GiBps : Asie-Pacifique (Mumbai), Asie-Pacifique (Séoul), Asie-Pacifique (Sydney) et Europe (Londres) . Pour plus d'informations, consultez la section Quotas	2 mai 2025

[Amazon EFS que vous pouvez augmenter.](#)

[Augmentation élastique du débit dans certains Régions AWS](#)

Le débit de lecture maximal pour les systèmes de fichiers utilisant le débit élastique dans des régions spécifiques est de 60. GiBps Dans toutes les autres régions, la limite de débit de lecture pour les systèmes de fichiers utilisant le débit élastique a été augmentée de 10 à 20. GiBps Pour plus d'informations, consultez la section [Quotas Amazon EFS que vous pouvez augmenter.](#)

10 avril 2025

[Quota de points d'accès accru](#)

Le nombre maximum de points d'accès qu'un seul système de fichiers peut avoir est passé de 1 000 à 10 000. Vous pouvez également demander une augmentation de cette limite. Pour plus d'informations, consultez la section [Quotas de ressources que vous pouvez augmenter.](#)

10 février 2025

[Taux de sauvegarde et de restauration améliorés](#)

La vitesse d'exécution des sauvegardes et des restaurations s'est améliorée. Pour plus d'informations, consultez la section [Performances de sauvegarde.](#)

8 janvier 2025

[Augmentation du quota d'IOPS par demande](#)

Vous pouvez désormais demander une augmentation des IOPS pour les systèmes de fichiers EFS à l'aide du mode débit élastique. Pour plus d'informations, consultez la section [Quotas Amazon EFS que vous pouvez augmenter](#).

26 novembre 2024

[Support de réplication entre comptes](#)

Amazon EFS prend en charge la réplication entre comptes. Pour plus d'informations, consultez la section [Réplication des systèmes de fichiers EFS entre Comptes AWS](#) eux.

19 novembre 2024

[Politique AWS gérée existante mise à jour](#)

ReplicationRead, ReplicationWrite, iam:PassRole sont ajoutés à la AmazonElasticFileSystemFullAccess politique. Pour plus d'informations, consultez [AmazonElasticFileSystemFullAccess](#).

7 novembre 2024

[Politique AWS gérée existante mise à jour](#)

ReplicationRead et ReplicationWrite ajouté à AmazonElasticFileSystemServiceRolePolicy. Pour plus d'informations, consultez [AmazonElasticFileSystemServiceRolePolicy](#).

7 novembre 2024

Politique AWS gérée existante mise à jour

Autorisation `ReplicationRead` ajoutée à la `AmazonElasticFileSystemReadOnlyAccess` politique existante. Pour de plus amples informations, veuillez consulter [AmazonElasticFileSystemReadOnlyAccess](#).

7 novembre 2024

Limite de débit élastique augmentée

La limite de débit élastique est passée à 60 gibioctets par seconde (GiBps) pour certaines régions Régions AWS et à 10 GiBps pour toutes les autres régions. Pour plus d'informations, consultez la section [Débit élastique total par défaut pour tous les clients connectés dans chaque Région AWS](#) d'eux.

14 octobre 2024

Politique AWS gérée existante mise à jour

L'élément facultatif `Sid` (ID de déclaration) est désormais inclus dans la déclaration `AmazonElasticFileSystemReadOnlyAccess` de politique. La valeur `Sid` est `ElasticFileSystemReadOnlyAccess`. Pour plus d'informations sur l'élément `Sid` de stratégie, voir [Éléments de stratégie IAM JSON : Sid](#).

7 août 2024

[Limite de débit élastique augmentée](#)

La limite de débit élastique a été augmentée pour des raisons spécifiques Régions AWS. Pour plus d'informations, consultez la section [Débit élastique total par défaut pour tous les clients connectés dans chacun Région AWS](#) d'eux.

31 juillet 2024

[Quota accru pour les cibles de montage](#)

Le nombre maximum de cibles de montage pour chaque cloud privé virtuel (VPC) est passé de 400 à 1 400. Pour plus d'informations, consultez les [quotas de ressources Amazon EFS que vous ne pouvez pas modifier](#).

15 mai 2024

[Limite de débit combiné accrue pour les systèmes de fichiers Elastic](#)

Le débit de lecture et d'écriture combiné maximal est de 1 500 MiBps pour les systèmes de fichiers utilisant le débit élastique et montés à l'aide de la version 2.0 ou ultérieure du client Amazon EFS (amazon-efs-utils version) ou du pilote Amazon EFS CSI (. aws-efs-csi-driver Pour plus d'informations, consultez le tableau récapitulatif des performances dans [Amazon EFS Performance](#).

30 avril 2024

[Limite de débit élastique augmentée](#)

La limite de débit élastique a été augmentée pour des raisons spécifiques Régions AWS. Pour plus d'informations, consultez la section [Débit élastique total par défaut pour tous les clients connectés dans chacun Région AWS](#) d'eux.

13 mars 2024

[Augmentation des IOPS](#)

Les systèmes de fichiers qui utilisent le débit élastique peuvent générer un maximum de 90 000 lectures pour les données rarement consultées. Pour plus d'informations, consultez [Récapitulatif des performances](#).

22 janvier 2024

[Politique AWS gérée existante mise à jour](#)

Autorisation `elasticfilesystem:UpdateFilesystemProtection` ajoutée à la `AmazonElasticFileSystemFullAccess` politique existante pour permettre aux principaux de mettre à jour la protection sur un système de fichiers. Pour plus d'informations, consultez les [misés à jour des politiques AWS gérées par Amazon EFS](#).

27 novembre 2023

[Répliquer dans le système de fichiers existant](#)

Les systèmes de fichiers peuvent désormais être répliqués sur des systèmes de fichiers existants, ce qui facilite la synchronisation des modifications entre les systèmes de fichiers à des fins de restauration. Pour plus d'informations, consultez [Systèmes de fichiers de destination](#).

27 novembre 2023

[Ajout de la protection du système de fichiers](#)

La protection contre le remplacement de la réplication a été ajoutée aux systèmes de fichiers et est activée par défaut. La protection empêche l'utilisation des systèmes de fichiers comme destination dans une configuration de réplication. Pour plus d'informations, veuillez consulter la rubrique [Protection du système de fichiers](#).

27 novembre 2023

[Nouvelle classe de stockage, nouveaux types de systèmes de fichiers et nouvelle politique de cycle de vie](#)

Amazon EFS propose désormais la classe de stockage EFS Archive, les types de systèmes de fichiers et la politique de cycle de vie de transition vers Archive. Pour plus d'informations, consultez [Types de systèmes de fichiers et classes de stockage](#).

26 novembre 2023

[Augmentation des IOPS](#)

Les systèmes de fichiers à débit élastique prennent désormais en charge un maximum de 65 000 opérations IOPS en lecture et 50 000 en écriture pour les données rarement consultées, et 250 000 opérations IOPS en lecture pour les données fréquemment consultées. Pour plus d'informations, consultez [Récapitulatif des performances](#).

26 novembre 2023

[Supprimer la configuration de réplication du système de fichiers source](#)

Désormais, les configurations de réplication peuvent être supprimées du système de fichiers source. Pour plus d'informations, consultez [Suppression d'une configuration de réplication](#).

19 septembre 2023

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs de la région Israël (Tel Aviv).

7 août 2023

[Augmentation des performances des systèmes de fichiers en mode Usage général](#)

Les systèmes de fichiers Amazon EFS en mode Usage général prennent désormais en charge jusqu'à 55 000 opérations en lecture par seconde et 25 000 opérations en écriture. Pour de plus amples informations, veuillez consulter [Quotas pour les systèmes de fichiers Amazon EFS](#).

3 août 2023

[Limite de débit provisionnée augmentée](#)

La limite de débit allouée a été augmentée pour des raisons spécifiques. Régions AWS
Pour plus d'informations, voir [Débit provisionné total par défaut pour tous les clients connectés dans](#) chacun d'eux.
Région AWS

21 juin 2023

[Prise en charge régionale étendue de la réplication EFS](#)

La réplication EFS est désormais disponible Régions AWS dans tous les pays où EFS est disponible. Pour plus d'informations, consultez [Réplication Amazon EFS](#).

28 avril 2023

[Augmentation élastique de la limite de débit](#)

La limite de débit élastique a été augmentée pour des raisons spécifiques Régions AWS. Pour plus d'informations, consultez le tableau [Débit élastique total par défaut pour tous les clients connectés dans chacun Région AWS](#) d'eux.

17 avril 2023

Elastic remplace Bursting comme mode de débit par défaut	Le mode de débit par défaut (et recommandé) pour les systèmes de fichiers est désormais Elastic au lieu de Bursting. Pour plus d'informations, consultez Modes de débit .	13 avril 2023
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs dans la région Asie-Pacifique (Melbourne).	12 avril 2023
Ajout de la prise en charge de macOS Ventura	Amazon EFS peut désormais être installé sur des instances EC2 Mac fonctionnant sous macOS Ventura. Pour plus d'informations, veuillez consulter Distributions prises en charge .	10 avril 2023
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs dans la région Asie-Pacifique (Hyderabad)	16 février 2023
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs dans la Région AWS Europe (Espagne).	19 janvier 2023
La limite de points d'accès pour les systèmes de fichiers a augmenté	Le nombre maximum de points d'accès qu'un seul système de fichiers peut avoir est passé de 120 à 1 000. Pour plus d'informations, consultez Quotas de ressources .	17 janvier 2023

Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs en Europe (Zurich) Région AWS.	15 décembre 2022
Ajout de la prise en charge des politiques de cycle de vie d'un jour	Vous pouvez désormais sélectionner un jour pour la politique de cycle de vie relative à la transition vers l'IA. Pour plus d'informations, consultez Politiques de cycle de vie .	27 novembre 2022
Latences réduites en lecture et en écriture	Les temps de latence en lecture et en écriture des données de fichiers ont été réduits pour les systèmes de fichiers de stockage One Zone et Standard. Pour plus d'informations, consultez Récapitulatif des performances .	27 novembre 2022
Ajout d'un mode de débit supplémentaire	Le mode de débit élastique est ajouté en tant qu'option de débit pour les systèmes de fichiers Amazon EFS. Pour plus d'informations, consultez la section Débit élastique .	27 novembre 2022
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs dans la région du Moyen-Orient (UAE).	17 octobre 2022

[Ajout de la prise en charge de la réplication EFS](#)

Amazon EFS a supprimé une limite précédente selon laquelle la réplication EFS ne prend pas en charge les sockets et les canaux nommés, ou FIFOs.

15 septembre 2022

[La limite du nombre de verrouillages de fichiers par connexion a été augmentée](#)

Le nombre de verrouillages de fichiers par connexion a été augmentée de 8 192 à 65 536. Pour de plus amples informations, veuillez consulter [Quotas pour les clients NFS](#).

4 mai 2022

[Suppression de la limite pour les processus utilisant des verrouillages de fichiers](#)

Amazon EFS a supprimé une limite précédente selon laquelle un maximum de 256 processus sur une seule instance pouvaient utiliser des verrous de fichiers en même temps. Pour de plus amples informations, veuillez consulter [Quotas pour les clients NFS](#).

4 mai 2022

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs dans la Région AWS Asie-Pacifique (Jakarta).

27 janvier 2022

[Ajout de la prise en charge de la réplication EFS](#)

Utilisez la réplication EFS pour répliquer les données et les métadonnées d'un système de fichiers EFS vers un autre système de fichiers EFS Région AWS de votre choix. Pour plus d'informations, consultez [Réplication Amazon EFS](#).

25 janvier 2022

[Le système de fichiers et les ressources de cibles de montage utilisent un format d'ID de ressource à 17 caractères](#)

Le nouveau système de fichiers Amazon EFS et les ressources cibles de montage se voient désormais attribuer 17 caractères IDs. Pour plus d'informations, consultez la section [Utilisation des ressources Amazon EFS](#).

22 octobre 2021

[Ajout de la prise en charge de la hiérarchisation intelligente EFS](#)

La hiérarchisation intelligente EFS utilise la gestion du cycle de vie EFS pour surveiller les modèles d'accès aux fichiers et est conçue pour transférer automatiquement les fichiers vers et depuis les classes de stockage à accès peu fréquent (IA) correspondantes. Pour plus d'informations, veuillez consulter [Hiérarchisation intelligente et gestion du cycle de vie EFS](#).

2 septembre 2021

[Ajout de la prise en charge
du test du format d'ID de
ressource à 17 caractères](#)

Amazon EFS passe de l'utilisa- 5 mai 2021
tion de 8 caractères IDs à
17 caractères IDs pour les
systèmes de fichiers et les
cibles de montage le 1er
octobre 2021. Au cours de
cette transition, vous pouvez
vous inscrire et commencer à
utiliser une ressource IDs de
17 caractères par an Région
AWS . Pour plus d'informa-
tions, consultez la section
[Ressource IDs](#).

Ajout de la prise en charge
du montage de systèmes
de fichiers One Zone depuis
une autre zone de disponibi-
lité à l'aide de l'assistant de
montage Amazon EFS

Vous pouvez désormais 6 avril 2021
utiliser l'assistant de montage
EFS pour monter un système
de fichiers Amazon EFS qui
utilise les classes de stockage
One Zone sur une EC2
instance située dans une autre
zone de disponibilité. Vous
pouvez utiliser la nouvelle
option az pour spécifier
la zone de disponibilité du
système de fichiers Amazon
EFS. Pour plus d'informa-
tions, consultez [Montage de
systèmes de fichiers avec
des classes de stockage One
Zone](#).

[Ajout de la prise en charge des classes de stockage One Zone EFS](#)

Les classes de stockage One Zone Amazon EFS stockent les données de manière redondante dans une zone de disponibilité unique d'une Région AWS. Les classes de stockage EFS One Zone et One Zone-Accès peu fréquent (One Zone-IA) constituent une option rentable pour stocker des données qui ne nécessitent pas la résilience multi-AZ des classes de stockage EFS Standard et Standard-IA. Pour plus d'informations, consultez [Utilisation des classes de stockage EFS](#).

9 mars 2021

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs dans la Région AWS Asie-Pacifique (Osaka).

3 mars 2021

[Support ajouté pour les instances Amazon EC2 macOS exécutant macOS Big Sur](#)

Vous pouvez désormais monter votre système de fichiers Amazon EFS à partir d'instances de EC2 macOS exécutant macOS Big Sur à l'aide de l'assistant de montage EFS ou à l'aide de la commande de montage NFS. Pour plus d'informations, consultez [Montage avec l'assistant de montage EFS](#) ou [Montage de systèmes de fichiers sans l'assistant de montage EFS](#).

23 février 2021

[La nouvelle console Amazon EFS est disponible dans AWS GovCloud \(US\) la région](#)

La nouvelle console Amazon EFS est désormais disponible dans le AWS GovCloud (US) Région AWS.

10 février 2021

[Support ajouté pour la nouvelle CloudWatch métrique Amazon EFS MeteredIO Bytes](#)

Vous pouvez utiliser `MeteredIOBytes` pour mesurer le nombre d'octets pour chaque opération de système de fichiers, y compris les opérations de lecture des données, d'écriture des données et les opérations de métadonnées. Les opérations de lecture sont mesurées à un tiers du taux des autres opérations. Pour plus d'informations, consultez les [CloudWatch métriques Amazon pour Amazon EFS](#).

28 janvier 2021

[Amazon EFS augmente le débit de lecture du système de fichiers de 300 %](#)

Les systèmes de fichiers Amazon EFS mesurent désormais les demandes de lecture à un tiers du taux des autres demandes.

28 janvier 2021

[Support ajouté pour la nouvelle CloudWatch métrique Amazon EFS StorageBytes](#)

Vous pouvez utiliser StorageBytes pour mesurer et surveiller la taille du système de fichiers en octets, y compris la quantité de données stockées dans les classes de stockage Standard et Accès pour fréquent. Pour plus d'informations, consultez les [CloudWatch métriques Amazon pour Amazon EFS](#).

11 janvier 2021

[AWS Transfer Family À utiliser pour accéder aux systèmes de fichiers Amazon EFS](#)

Vous pouvez l'utiliser AWS Transfer Family pour transférer des fichiers vers et depuis vos systèmes de fichiers Amazon EFS. Pour plus d'informations, voir [Utilisation AWS Transfer Family pour accéder aux fichiers de votre système de fichiers EFS](#).

6 janvier 2021

[AWS Systems Manager À utiliser pour gérer le client Amazon EFS \(amazon-efs-utils\)](#)

Vous pouvez l'utiliser AWS Systems Manager pour installer ou mettre à jour automatiquement les clients Amazon EFS (amazon-efs-utils) sur vos EC2 instances. Pour plus d'informations, consultez [Utiliser AWS Systems Manager pour installer ou mettre à jour automatiquement les clients Amazon EFS.](#)

29 septembre 2020

[Imposer la création de systèmes de fichiers EFS chiffrés](#)

Vous pouvez utiliser la clé de condition elasticfilesystem:Encrypted AWS Identity and Access Management (IAM) pour obliger les utilisateurs à créer des systèmes de fichiers Amazon EFS chiffrés au repos. Pour plus d'informations, veuillez consulter [Imposer la création de systèmes de fichiers Amazon EFS chiffrés au repos.](#)

16 septembre 2020

[Le débit par client Amazon EFS a augmenté de 100 %](#)

L'EFS prend désormais en charge jusqu'à 500 % MB/s de débit par client, soit une augmentation de 100 % par rapport à la limite précédente de 250 Mo/s. Pour de plus amples informations, veuillez consulter [Quotas pour les systèmes de fichiers Amazon EFS](#).

23 juillet 2020

[Ajout de la prise en charge des sauvegardes quotidiennes automatiques des systèmes de fichiers Amazon EFS](#)

Lorsque vous créez un système de fichiers à l'aide de la console EFS, les sauvegardes quotidiennes automatiques sont désormais activées par défaut. Pour plus d'informations, consultez [Utilisation AWS Backup avec Amazon EFS](#).

16 juillet 2020

[Le nouveau flux de travail Quick Create simplifie la création de systèmes de fichiers Amazon EFS](#)

L'option Quick Create de la console EFS vous permet de créer un système de fichiers EFS à l'aide des paramètres recommandés par le service avec un seul bouton. Pour plus d'informations, voir [Création de votre système de fichiers EFS](#).

16 juillet 2020

[La nouvelle console Amazon EFS est désormais disponible](#)

La nouvelle console EFS facilite l'utilisation d'Amazon EFS et simplifie la gestion de vos systèmes de fichiers EFS.

16 juillet 2020

[Amazon EFS augmente le débit minimum du système de fichiers](#)

Les systèmes de fichiers Amazon EFS utilisant le débit en rafale ont désormais un débit minimum de 1 Mbits/s. Pour plus d'informations, consultez [Modes de débit](#).

30 juin 2020

[Augmentation des performances des systèmes de fichiers en mode Usage général](#)

Les systèmes de fichiers Amazon EFS en mode Usage général prennent désormais en charge jusqu'à 35 000 opérations de lecture par seconde, soit une augmentation de 400 % par rapport à la limite précédente de 7 000. Pour de plus amples informations, veuillez consulter [Quotas pour les systèmes de fichiers Amazon EFS](#).

1er avril 2020

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs de Pékin et du Ningxia Régions AWS.

22 janvier 2020

[Ajout de la prise en charge de l'autorisation IAM pour les clients NFS](#)

Vous pouvez désormais utiliser AWS Identity and Access Management (IAM) pour gérer l'accès NFS à un système de fichiers Amazon EFS. Pour plus d'informations, consultez [Utilisation d' AWS IAM pour contrôler l'accès NFS à Amazon EFS](#).

13 janvier 2020

[Ajout de la prise en charge des points d'accès EFS](#)

Les points d'accès Amazon EFS sont des points d'entrée spécifiques à l'application dans un système de fichiers Amazon EFS, lesquels facilitent la gestion de l'accès des applications aux jeux de données partagés. Pour de plus amples informations, veuillez consulter [Utilisation des points d'accès Amazon EFS](#).

13 janvier 2020

[Support ajouté pour la restauration AWS Backup partielle.](#)

Vous pouvez désormais restaurer des fichiers et des répertoires spécifiques à l'aide d'une restauration partielle, en plus de restaurer un point de récupération complet. Pour plus d'informations, consultez [Utilisation AWS Backup avec Amazon EFS](#).

13 janvier 2020

[Ajout de la prise en charge des rôles IAM liés à un service](#)

Amazon EFS utilise désormais un rôle lié à un service basé sur IAM, ce qui facilite la configuration d'EFS en ajoutant automatiquement les autorisations nécessaires. Pour plus d'informations, consultez [Utilisation des rôles liés à un service pour Amazon EFS](#).

10 décembre 2019

Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs en Europe (Stockholm) Région AWS.	20 novembre 2019
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs de la région Asie-Pacifique (Hong Kong) Région AWS.	20 novembre 2019
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs d'Amérique du Sud (São Paulo) Région AWS.	20 novembre 2019
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs du Moyen-Orient (Bahreïn). Région AWS	20 novembre 2019
Ajout d'une nouvelle stratégie de gestion du cycle de vie de 7 jours	La gestion du cycle de vie dispose désormais d'une stratégie supplémentaire pour transférer les données vers la classe de stockage économique Infrequent Access (Accès peu fréquent) après 7 jours. Pour plus d'informations, consultez Gestion du cycle de vie EFS .	6 novembre 2019

[Ajout de la prise en charge
des points de terminaison d'un
VPC d'interface](#)

Vous pouvez établir une connexion privée entre votre cloud privé virtuel et Amazon EFS pour appeler l'API EFS. Pour plus d'informations, consultez [Utilisation des points de terminaison d'un VPC](#).

22 octobre 2019

[Montez un système de fichiers
EFS lors du lancement d'une
nouvelle EC2 instance.](#)

Vous pouvez désormais configurer de nouvelles EC2 instances Amazon pour monter vos systèmes de fichiers EFS au lancement dans l'assistant de EC2 lancement d'instance. Pour de plus amples informations, consultez l'[Étape 2. Créez vos EC2 ressources et lancez votre EC2 instance](#).

17 octobre 2019

[Ajout de la prise en charge
des quotas de service](#)

Vous pouvez désormais afficher toutes les limites d'Amazon EFS dans la console Quotas de service. Pour plus d'informations, consultez [Limites Amazon EFS](#).

10 septembre 2019

[Ajout de nouvelles stratégies de gestion du cycle de vie](#)

Lorsque vous utilisez la gestion du cycle de vie, vous pouvez désormais choisir une des quatre stratégies de cycle de vie pour définir le moment où les fichiers sont transférés dans la classe de stockage économique d'accès peu fréquent. Pour plus d'informations, consultez [Gestion du cycle de vie EFS](#).

9 juillet 2019

[La gestion du cycle de vie EFS est désormais disponible sur tous les systèmes de fichiers EFS.](#)

La fonction de gestion du cycle de vie EFS est désormais disponible sur tous les systèmes de fichiers EFS. Une restriction précédente, basée sur la date de création du système de fichiers, est désormais supprimée. Pour plus d'informations, consultez [Gestion du cycle de vie EFS](#).

9 juillet 2019

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs en Europe (Paris) Région AWS.

12 juin 2019

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs de la région Asie-Pacifique (Mumbai) Région AWS.

5 juin 2019

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs du Canada (Centre) Région AWS.

1er mai 2019

[Mise à jour de l'API : les balises font désormais partie de la charge utile des CreateFileSystem opérations](#)

Vous pouvez désormais inclure des balises lors de l'utilisation de l' AWS API et de la CLI CreateFileSystem pour créer un système de fichiers Amazon EFS. Pour plus d'informations, voir [Création CreateFileSystemd'un système de fichiers à l'aide de la AWS CLI.](#)

19 février 2019

[Nouvelles fonctions : classe de stockage EFS Accès peu fréquent et gestion du cycle de vie EFS](#)

La classe de stockage Amazon EFS Accès peu fréquent est une classe de stockage économique pour les fichiers peu consultés. La gestion du cycle de vie EFS transfère automatiquement les fichiers de la classe de stockage Standard à la classe de stockage Accès peu fréquent. Pour plus d'informations, consultez [Classes de stockage EFS.](#)

13 février 2019

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs en Europe (Londres) Région AWS.

23 janvier 2019

[AWS Backup Intégration des services avec Amazon EFS](#)

Les systèmes de fichiers Amazon EFS peuvent être sauvegardés à l'aide AWS Backup d'un service de sauvegarde automatisé, centralisé et entièrement géré pour sauvegarder les données entre les AWS services dans le cloud et sur site. Pour plus d'informations, consultez [AWS Backup et Amazon EFS](#).

16 janvier 2019

[Ajout de la prise en charge de la connexion Transit Gateway aux systèmes de stockage sur site.](#)

Les systèmes de fichiers Amazon EFS sont désormais accessibles en utilisant les connexions Transit Gateway sur les systèmes de stockage sur site. Pour plus d'informations, consultez [Montage à partir d'un autre compte ou VPC](#) et [Procédure : montage d'un système de fichiers à partir d'un autre VPC](#).

6 décembre 2018

[EFS File Sync fait désormais partie du nouveau AWS DataSync service.](#)

AWS DataSync est un service géré de transfert de données qui simplifie la synchronisation de grandes quantités de données entre les systèmes de stockage sur site et les services AWS de stockage. Pour plus d'informations, consultez [Transférer des fichiers depuis des systèmes de fichiers locaux vers Amazon EFS à l'aide AWS DataSync d'Amazon EFS.](#)

26 novembre 2018

[Ajout de la prise en charge des connexions VPN et des connexions d'appairage de VPC entre régions](#)

Amazon EFS est désormais accessible sur les connexions VPN et les connexions d'appairage de VPC entre régions. Pour plus d'informations, consultez [Transférer des fichiers depuis des systèmes de fichiers locaux vers Amazon EFS à l'aide AWS DataSync d'Amazon EFS.](#)

23 octobre 2018

[Ajout de la prise en charge des connexions VPN et des connexions d'appairage de VPC entre régions](#)

Les systèmes de fichiers Amazon EFS sont désormais accessibles sur les connexions VPN et les connexions d'appairage de VPC entre régions. Pour plus d'informations, consultez [Montage à partir d'un autre compte ou VPC](#) et Comment [fonctionne Amazon EFS avec Direct Connect](#) et. VPNs

23 octobre 2018

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs dans la Région AWS Asie-Pacifique (Singapour).

13 juillet 2018

[Présentation du mode Débit alloué](#)

Vous pouvez désormais allouer un débit pour les systèmes de fichiers, nouveaux ou existants, avec le nouveau mode Débit alloué. Pour plus d'informations, consultez [Modes de débit](#).

12 juillet 2018

[Région AWS Support supplémentaire ajouté](#)

Amazon EFS est désormais disponible pour tous les utilisateurs dans la Région AWS Asie-Pacifique (Tokyo).

11 juillet 2018

Le tableau suivant présente les modifications importantes apportées au Guide de l'utilisateur Amazon Elastic File System avant juillet 2018.

Modification	Description	Date de modification
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs dans la AWS Asie-Pacifique (Séoul).	30 mai 2018
Ajout d'un support mathématique CloudWatch métrique	Les mathématiques métriques vous permettent d'interroger plusieurs CloudWatch métriques et d'utiliser des expressions mathématiques pour créer de nouvelles séries chronologiques basées sur ces métriques. Pour de plus amples informations, veuillez consulter Utiliser les mathématiques métriques avec CloudWatch les métriques .	4 avril 2018
Ajout de l'ensemble d'outils amazon-efs-utils open-source et ajout du chiffrement en transit	Les outils amazon-efs-utils sont un ensemble de fichiers exécutables open-source qui simplifient certains aspects de l'utilisation d'Amazon EFS, comme le montage. L'utilisation amazon-efs-utils est gratuite et vous pouvez télécharger ces outils depuis GitHub. Pour de plus amples informations, veuillez consulter Installation du client Amazon EFS. De même, dans cette version, Amazon EFS prend désormais en charge le chiffrement en transit via le tunneling TLS (Transport Layer Security). Pour de plus amples informations, veuillez consulter Chiffrement des données dans Amazon EFS.	4 avril 2018
Limites du système de fichiers mises à jour par Région AWS	Amazon EFS a augmenté la limite du nombre de systèmes de fichiers pour tous les comptes de toutes les Région AWS. Pour de plus amples informations, veuillez consulter Les quotas de ressources Amazon EFS que vous ne pouvez pas Modifier .	15 mars 2018

Modification	Description	Date de modification
Région AWS Support supplémentaire ajouté	Amazon EFS est désormais disponible pour tous les utilisateurs de l'ouest des États-Unis (Californie du Nord) Région AWS.	14 mars 2018
Chiffrement de données au repos	Amazon EFS prend désormais en charge le chiffrement des données au repos. Pour de plus amples informations, veuillez consulter Chiffrement des données dans Amazon EFS .	14 août 2017
Ajout de la prise en charge d'une région supplémentaire	Amazon EFS est maintenant disponible dans la Région Europe (Francfort).	20 juillet 2017
Noms de système de fichiers utilisant le système de noms de domaine (DNS)	Amazon EFS prend désormais en charge les noms DNS pour les systèmes de fichiers. Le nom DNS d'un système de fichiers est automatiquement converti en adresse IP d'une cible de montage dans la zone de disponibilité de l'EC2 instance Amazon connectée. Pour de plus amples informations, veuillez consulter Montage sur Amazon EC2 avec un nom DNS .	20 décembre 2016
Meilleure prise en charge des balises pour les systèmes de fichiers	Amazon EFS prend désormais en charge 50 balises par système de fichiers. Pour plus d'informations sur les balises dans Amazon EFS, consultez Marquage des ressources EFS .	29 août 2016
Disponibilité générale	Amazon EFS est désormais disponible pour tous les utilisateurs dans les régions USA Est (Virginie du Nord), USA Ouest (Oregon) et UE (Irlande).	28 juin 2016

Modification	Description	Date de modification
Augmentation de la limite de système de fichiers	Le nombre de systèmes de fichiers Amazon EFS pouvant être créés par compte et pour chaque Région AWS est passé de 5 à 10.	21 août 2015
Mise à jour de l'exercice de mise en route	L'exercice de mise en route a été mis à jour pour simplifier le processus de mise en route.	17 août 2015
Nouveau guide	Il s'agit de la première version du Guide de l'utilisateur Amazon Elastic File System.	26 mai 2015

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.