aws

Guide de l'utilisateur

Amazon Elastic File System

Amazon Elastic File System: Guide de l'utilisateur

Table of Contents

Qu’est ce qu’Amazon Elastic File System ? 1
Vous utilisez Amazon EFS pour la première fois ? 3
Comment ça marche 4
Présentation 4
Utiliser Amazon EFS avec Amazon EC2 6
Système de fichiers Amazon EFS Régional 6
Systèmes de fichiers Amazon EFS One Zone 7
Comment Amazon EFS fonctionne avec un AWS Direct Connect VPN AWS géré 9
Comment fonctionne Amazon EFS avec AWS Backup 10
Récapitulatif de l’implémentation 11
Authentification et contrôle d’accès 13
Cohérence des données dans Amazon EFS 13
Verrouillage de fichiers 14
Classes de stockage EFS 14
Gestion des cycles de vie 14
Réplication 15
Premiers pas 16
Prérequis 16
Création d'un système de fichiers et lancement de l'instance EC2 17
Transférez des fichiers vers votre système de fichiers 18
Prérequis 18
Nettoyage des ressources 19
Comprendre les types de systèmes de fichiers et les classes de stockage 21
Types de système de fichiers EFS 21
Zones de disponibilité prises en charge pour les systèmes de fichiers One Zone 22
Classes de stockage EFS 24
Optimisation des coûts de stockage 25
Comparer les classes de stockage 25
Tarification par classe de stockage 27
Affichage de classe de stockage 28
Utilisation des ressources 30
ID de ressource 31
Jeton de création et idempotence 31
Création de systèmes de fichiers 32

Autorisations requises pour créer des systèmes de fichiers ... 32
Options de configuration ... 32
Suppression de systèmes de fichiers ... 45
Gérer des cibles de Montage ... 46
Création de groupes de sécurité ... 54
Création de politiques de système de fichiers ... 56
Création de points d'accès ... 59
Supprimer des points d'accès ... 62
Balisage des ressources ... 63
Principes de base des étiquettes ... 63
Restrictions liées aux balises ... 64
Utilisation de balises pour le contrôle d’accès ... 65
Baliser vos ressources ... 65
Installation des outils EFS ... 67
À propos du client EFS ... 67
Distributions prises en charge : ... 69
Installation automatisée du client EFS ... 70
Ce que fait le client Amazon EFS lors de l’installation ... 71
Gestionnaire de systèmes Systèmes d’exploitation pris en charge par le distributeur ... 71
Comment utiliser AWS Systems Manager pour installer ou mettre à jour automatiquement amazon-efs-utils ... 72
Installation manuelle du client EFS ... 74
Installation du client Amazon EFS sur les instances Linux Amazon EC2 ... 74
Pour installer le client Amazon EFS sur d’autres distributions Linux ... 75
Installation du client EFS sur des instances Mac EC2 ... 76
Installation et mise à niveau `botocore` ... 76
Mise à niveau d’`stunnel` ... 77
Désactivation de la vérification du nom d’hôte du certificat ... 79
Activation du protocole de vérification en ligne de certificat (OCSP) ... 79
Montage des systèmes de fichiers ... 81
Utilisation de l’assistant de Montage EFS ... 82
Comment ça marche ... 83
Obtention de journaux de support ... 85
Prérequis ... 86
Montage sur EC2 Linux ... 87
Montage sur Mac EC2 ... 89

Montage depuis une autre région 91
Montage de systèmes de fichiers Zone unique 92
Montage avec autorisation IAM 96
Montage avec points d'accès EFS 97
Montage avec des clients sur site 98
Montage automatique d'EFS 99
Montage de plusieurs instances EC2 109
Montage à partir d'un autre compte ou VPC 110
Utilisation de NFS 114
NFS Support 115
Installation du client NFS 117
Options de montage NFS 119
Montage sur Amazon EC2 avec un nom DNS 121
Montage avec une adresse IP 124
Considérations de Montage supplémentaires 126
Démontage des systèmes de fichiers 128
Résolution des problèmes de montage 129
Le montage du système de fichiers sur l'instance Windows échoue 130
Accès refusé par le serveur 130
Le montage automatique échoue et l'instance ne répond pas 131
Le montage de plusieurs systèmes de fichiers Amazon EFS dans /etc/fstab échoue 131
La commande de montage échoue avec le message d'erreur « type de fs erroné » 132
La commande de montage échoue avec le message d'erreur « option de montage incorrecte » 133
Le montage avec point d'accès échoue 133
Le montage du système de fichiers échoue immédiatement après la création du système de fichiers 134
Le montage du système de fichiers se bloque, puis échoue avec une erreur de dépassement de délai d'attente 134
Le montage d'un système de fichiers avec NFS à l'aide d'un nom DNS échoue 135
Échec du montage d'un système de fichiers avec « nfs ne répond pas » 136
L'état de cycle de vie de la cible de montage est bloqué 136
L'état du cycle de vie cible du montage indique une erreur 137
Le montage ne répond pas 137
Le client monté est déconnecté 138

Les opérations sur un système de fichiers nouvellement monté renvoient l'erreur « mauvaise gestion de fichier » 138
Le démontage d'un système de fichiers échoue 139
Transfert de données 140
En utilisant AWS DataSync 140
En utilisant AWS Transfer Family 141
Conditions préalables à l'utilisation AWS Transfer Family avec Amazon EFS 142
Configuration de votre système de fichiers Amazon EFS pour qu'il fonctionne avec AWS Transfer Family 142
Gestion des systèmes de fichiers 148
Gérer des cibles de Montage 148
Création ou suppression de cibles de Montage dans un VPC 150
Changement de VPC pour votre cible de Montage 151
Mise à jour de la configuration de cible de Montage 152
Gestion du débit 153
Gestion du stockage du système de fichiers 155
Politiques de cycle de vie 155
Opérations sur le système de fichiers pour la gestion du cycle de vie 156
Gestion des politiques de cycle de vie d'un système de fichiers 157
Gestion de l'accès aux systèmes de fichiers chiffrés 160
Exécution d'actions administratives sur les clés Amazon EFS KMS 161
Mesures sur un système de fichiers 162
Objets de mesure 162
Taille du système de fichiers mesurée 163
Débit de mesure 165
Gérer les coûts des systèmes de fichiers avec AWS les budgets 166
Prérequis 167
Création d'un budget des coûts mensuel pour un système de fichiers EFS 167
État du système de fichiers 168
Surveillance EFS 169
Outils de surveillance 170
Outils automatisés 170
Outils de surveillance manuelle 171
Surveillance des métriques avec CloudWatch 171
CloudWatch métriques 172
Comment utiliser les métriques Amazon EFS ? 178

Utilisation des maths de métriques avec Amazon EFS 180
Surveillance de l'état de réussite ou d'échec des tentatives de Montage 185
Accès aux CloudWatch métriques 187
Création d'alarmes 189
Journalisation des appels d'API AWS CloudTrail avec 191
Informations Amazon EFS dans CloudTrail 191
Présentation des entrées des fichiers journaux Amazon EFS 192
Entrées du fichier journal Amazon EFS pour les systèmes de encrypted-at-rest fichiers 199
Performance 201
Récapitulatif des performances 201
Classes de stockage 203
Modes de performances 204
Modes de débit 205
Choix d'un mode de débit 205
Débit élastique 206
Débit alloué 206
Restrictions relatives au débit de commutation et à la modification du montant provisionné . 209
Conseils sur les performances 209
Taille d'E/S Moyen 209
Optimisation des charges de travail exigeant un débit et des IOPS élevés 210
Connexions simultanées 210
Modèle de demande 210
Paramètres de Montage du client NFS 211
Optimisation des performances des petits fichiers 212
Optimisation des performances de disque 212
Optimisation de la taille NFS read_ahead_kb 213
Résolution des problèmes de performances 214
Impossible de créer un système de fichiers EFS 215
Accès refusé aux fichiers autorisés sur le système de fichiers NFS 215
Erreurs lors de l'accès à la console Amazon EFS 215
L'instance Amazon EC2 se bloque 216
Une application qui écrit de grandes quantités de données se bloque 216
Performances médiocres à l'ouverture de plusieurs fichiers en parallèle 217
Paramètres NFS personnalisés entrainant des délais d'écriture 218
La création de sauvegardes avec Oracle Recovery Manager est lente 218
Résolution des problèmes d'AMI et de noyau 219

Impossible d’exécuter la commande chown 219
Le système de fichiers continue à effectuer des opérations plusieurs fois en raison d’un bogue client 220
Client bloqué 220
L’affichage de la liste de fichiers d’un répertoire volumineux prend beaucoup de temps. 220
Sauvegarde des systèmes de fichiers 222
Sauvegardes incrémentielles 222
Cohérence de sauvegarde 223
Performances de sauvegarde 223
Fenêtres de fin de sauvegarde 223
Classes de stockage EFS 224
Autorisations IAM pour créer et restaurer des sauvegardes 224
Sauvegardes à la demande 224
Sauvegardes simultanées 224
Sauvegardes automatiques 225
Activation ou désactivation de sauvegardes automatiques pour les systèmes de fichiers existants 225
Configurez les sauvegardes manuellement 227
Restauration d’un point de récupération 228
Suppression de sauvegardes 229
Répliquer des systèmes de fichiers 231
Configuration de réplication 232
Réplication vers un nouveau système de fichiers 232
Réplication vers un système de fichiers existant 234
Protection du système de fichiers 234
Autorisations nécessaires 235
Coûts 236
Performance 236
Montage d’un système de fichiers de destination 237
Basculement et restauration du système de fichiers 237
Créer des configurations de réplication 238
Affichage des configurations de réplication 241
Supprimer des configuration de réplication 244
Surveillance des emplacements de réplication 246
Procédures 248
Procédure pas à pas : créez et montez un système de fichiers à l'aide du AWS CLI 248

Avant de commencer 249
Configuration du AWS CLI 250
Étape 1 : Créer les ressources Amazon EC2 251
Étape 2 : Créer les ressources Amazon EFS 257
Étape 3 : Monter et tester le système de fichiers 261
Étape 4 : Nettoyer 264
Procédure : Définition d'un serveur web Apache et distribution des fichiers 266
instance EC2 unique pour la distribution de fichiers 267
Plusieurs instances EC2 pour la distribution des fichiers 269
Procédure pas à pas : créer des sous-répertoires inscriptibles par utilisateur 274
Remontage automatique au redémarrage 276
Procédure : monter un système de fichiers EFS sur un client sur site 276
Avant de commencer 278
Étape 1 : créer vos ressources Amazon Elastic File System 279
Étape 2 : Installation du client NFS 281
Étape 3 : Monter le système de fichiers Amazon EFS sur votre client sur site 281
Étape 4 : Nettoyer les ressources et protéger votre compte AWS 283
Facultatif : Chiffrement des données en transit 284
Procédure : montage d'un système de fichiers à partir d'un autre VPC 287
Avant de commencer 288
Étape 1 : Déterminer l'ID de zone de disponibilité de la cible de montage EFS 289
Étape 2 : Déterminer l'adresse IP de la cible de montage 290
Étape 3 : Ajouter une entrée hôte pour la cible de montage 291
Étape 4 : Monter votre système de fichiers à l'aide de l'assistant de montage EFS 291
Étape 5 : Nettoyer les ressources et protéger votre compte AWS 293
Procédure : Application du chiffrement sur un système de fichiers Amazon EFS au repos 294
Application du chiffrement au repos 295
Activer le root squashing à l'aide d'IAM pour NFS 298
Sécurité 301
Chiffrement des données dans Amazon EFS 302
Chiffrement de données au repos 303
chiffrement des données en transit 308
Comment fonctionne le chiffrement des données en transit ? 309
Résolution des problèmes de chiffrement 311
Gestion des identités et des accès 313
Public ciblé 314

Authentification par des identités ... 314
Gestion des accès à l’aide de politiques ... 318
Comment Amazon Elastic File System fonctionne avec IAM ... 321
Exemples de politiques basées sur l’identité ... 329
Exemples de stratégies basées sur les ressources ... 334
Politiques gérées par AWS ... 337
Utilisation de balises avec Amazon EFS ... 344
Utilisation des rôles liés à un service pour Amazon EFS ... 348
Résolution des problèmes ... 353
Contrôle de l’accès aux données du système de fichiers ... 355
Stratégie de système de fichiers par défaut ... 356
Actions EFS pour les clients ... 356
Clés de condition EFS pour les clients NFS ... 356
Exemples de stratégie de système de fichiers ... 357
Contrôle de l’accès réseau ... 357
Utilisation de groupes de sécurité VPC pour les instances Amazon EC2 et les cibles de montage ... 358
Ports source ... 359
Considérations relatives à la sécurité pour l’accès réseau ... 360
Utilisation des points de terminaison d'un VPC ... 361
Utilisateurs, groupes et autorisations de niveau NFS ... 363
Autorisations sur les fichiers et les répertoires ... 364
Exemple de cas d’utilisation et d’autorisations du système de fichiers Amazon EFS ... 364
Autorisations d'identification d'utilisateur et de groupe pour les fichiers et les répertoires d'un système de fichiers ... 366
Aucun écrasement racine ... 367
Mise en cache des autorisations ... 368
Modification de la propriété d’un objet du système de fichiers ... 368
Points d’accès EFS ... 368
Utilisation des points d’accès ... 368
Création d’un point d’accès ... 369
Montage avec points d’accès ... 369
Application forcée d’une identité d’utilisateur ... 370
Application forcée d’un répertoire racine ... 371
Utilisation des points d’accès dans les stratégies IAM ... 373
Blocage de l'accès public aux systèmes de fichiers Amazon EFS ... 374

Blocage de l’accès public avec AWS Transfer Family 375
La signification du mot « public » 375
Validation de conformité 377
Résilience 378
Isolement de réseau 380
Quotas 381
Les quotas Amazon EFS que vous pouvez augmenter 381
Demande d’augmentation de quota 383
Les quotas de ressources Amazon EFS que vous ne pouvez pas Modifier 383
Quotas pour les clients NFS 385
Quotas pour les systèmes de fichiers Amazon EFS 386
Fonctionnalités NFSv4.0 et 4.1 non prises en charge 387
Considérations supplémentaires 388
Résolution des erreurs de traitement de fichiers 388
Échec de la commande avec l’erreur « Quota de disque dépassé » 389
Échec de la commande avec l’erreur « Erreur d’E/S » 389
Échec de la commande avec l’erreur « Le nom de fichier est trop long » 390
Échec de la commande avec l’erreur « Fichier introuvable » 390
Échec de la commande avec l’erreur « Trop de liens » 390
Échec de la commande avec l’erreur « Fichier trop volumineux » 391
API Amazon EFS 392
Point de terminaison d'API 392
Version de l'API 393
Rubriques en relation 393
Utilisation du taux de demandes de l'API de requête pour Amazon EFS 394
Interrogation 394
Réessais ou traitement par lots 394
Calcul de l'intervalle de sommeil 394
Actions 395
CreateAccessPoint 397
CreateFileSystem 405
CreateMountTarget 421
CreateReplicationConfiguration 433
CreateTags 440
DeleteAccessPoint 443
DeleteFileSystem 445

DeleteFileSystemPolicy 449
DeleteMountTarget 452
DeleteReplicationConfiguration 456
DeleteTags 459
DescribeAccessPoints 462
DescribeAccountPreferences 467
DescribeBackupPolicy 470
DescribeFileSystemPolicy 473
DescribeFileSystems 477
DescribeLifecycleConfiguration 483
DescribeMountTargets 487
DescribeMountTargetSecurityGroups 493
DescribeReplicationConfigurations 497
DescribeTags 501
ListTagsForResource 506
ModifyMountTargetSecurityGroups 510
PutAccountPreferences 514
PutBackupPolicy 517
PutFileSystemPolicy 520
PutLifecycleConfiguration 526
TagResource 535
UntagResource 539
UpdateFileSystem 542
UpdateFileSystemProtection 550
Types de données 554
AccessPointDescription 555
BackupPolicy 558
CreationInfo 559
Destination 561
DestinationToCreate 563
FileSystemDescription 565
FileSystemProtectionDescription 570
FileSystemSize 571
LifecyclePolicy 573
MountTargetDescription 575
PosixUser 578

ReplicationConfigurationDescription 580
ResourceIdPreference 582
RootDirectory 583
Tag 585
Historique du document 586
..... dcxiii

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), afin que les applications et outils que vous utilisez aujourd’hui fonctionnent en toute transparence avec Amazon EFS. Amazon EFS est accessible sur la plupart des types d'instances de calcul Amazon Web Services, notamment Amazon EC2, 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 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.

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, consultezPerformances Amazon EFS.

Amazon EFS fournit des file-system-access éléments sémantiques, tels que la cohérence renforcée des données et le verrouillage des fichiers. Pour plus d'informations, consultez 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 plus d'informations, consultez Sécurité 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 du système de fichiers Amazon 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 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 Elastic File System et Contrôle de l'accès réseau aux systèmes de fichiers Amazon EFS pour les clients NFS.

> **Note**
>
> L'utilisation d'Amazon EFS avec des instances Amazon EC2 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 les exercices d'introduction :
   - Premiers pas
   - Procédures

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

- Utilisation des ressources Amazon EFS
- Gestion des systèmes de fichiers Amazon EFS
- API Amazon EFS

Comment fonctionne Amazon EFS

Vous trouverez ci-après une description du fonctionnement d'Amazon EFS, des informations concernant son implémentation et des considérations en matière de sécurité.

Rubriques

- Présentation
- Utiliser Amazon EFS avec Amazon EC2
- Comment Amazon EFS fonctionne avec un AWS Direct Connect VPN AWS géré
- Comment fonctionne Amazon EFS avec AWS Backup
- Récapitulatif de l'implémentation
- Authentification et contrôle d'accès
- Cohérence des données dans Amazon EFS
- Classes de stockage EFS
- Réplication

Présentation

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, monter ce système de fichiers sur vos instances Amazon EC2, puis lire et écrire des données vers et depuis votre système de fichiers. Vous pouvez monter un système de fichiers Amazon 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 génération actuelle, tel que ceux trouvés dans les dernières AMI Amazon Linux, Amazon Linux 2, Redhat, Ubuntu et macOS Big Sur AMI en parallèle avec l'assistant de montage EFS Amazon. Pour obtenir des instructions, veuillez consulter Installation des outils Amazon EFS.

Pour obtenir une liste des Amazon Machine Images (AMI) Amazon EC2 Linux et macOS qui prennent en charge ce protocole, consultez NFS Support. Pour certaines AMI, vous aurez besoin d'installer un client NFS pour monter votre système de fichiers sur votre instance Amazon EC2. Pour obtenir des instructions, veuillez consulter Installation du client NFS.

Vous pouvez accéder à votre système de fichiers Amazon EFS simultanément à partir de plusieurs clients NFS, afin que les applications qui s'étendent au-delà d'une simple connexion puissent accéder

à un système de fichiers. Amazon EC2 et d'autres instances de calcul AWS exécutées dans plusieurs zones de disponibilité au sein d'une même 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 Amazon EFS, consultez le Référence générale d'Amazon Web Services.

Pour accéder à votre système de fichiers Amazon EFS dans un VPC, vous créez une ou plusieurs cibles de montage dans le VPC.

- Pour les systèmes de fichiers régionaux, vous pouvez créer une cible de montage dans chaque zone de disponibilité dans Région AWS.
- 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.

Pour plus d'informations, consultez Classes de stockage EFS.

Une cible de montage fournit une adresse IP pour un point de terminaison NFSv4.1 sur lequel vous pouvez monter un système de fichiers Amazon EFS. Vous devez monter votre système de fichiers à l'aide de son nom DNS (Domain Name Service) qui se résout en l'adresse IP de la cible de montage EFS, dans la même zone de disponibilité que votre instance EC2. 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 instances EC2 de cette zone de disponibilité partagent alors cette cible de montage.

> **Note**
>
> Un système de fichiers Amazon EC2 peut seulement avoir des cibles de montage 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.

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 Utilisation des utilisateurs, des groupes et des autorisations au niveau du système de fichiers réseau (NFS).

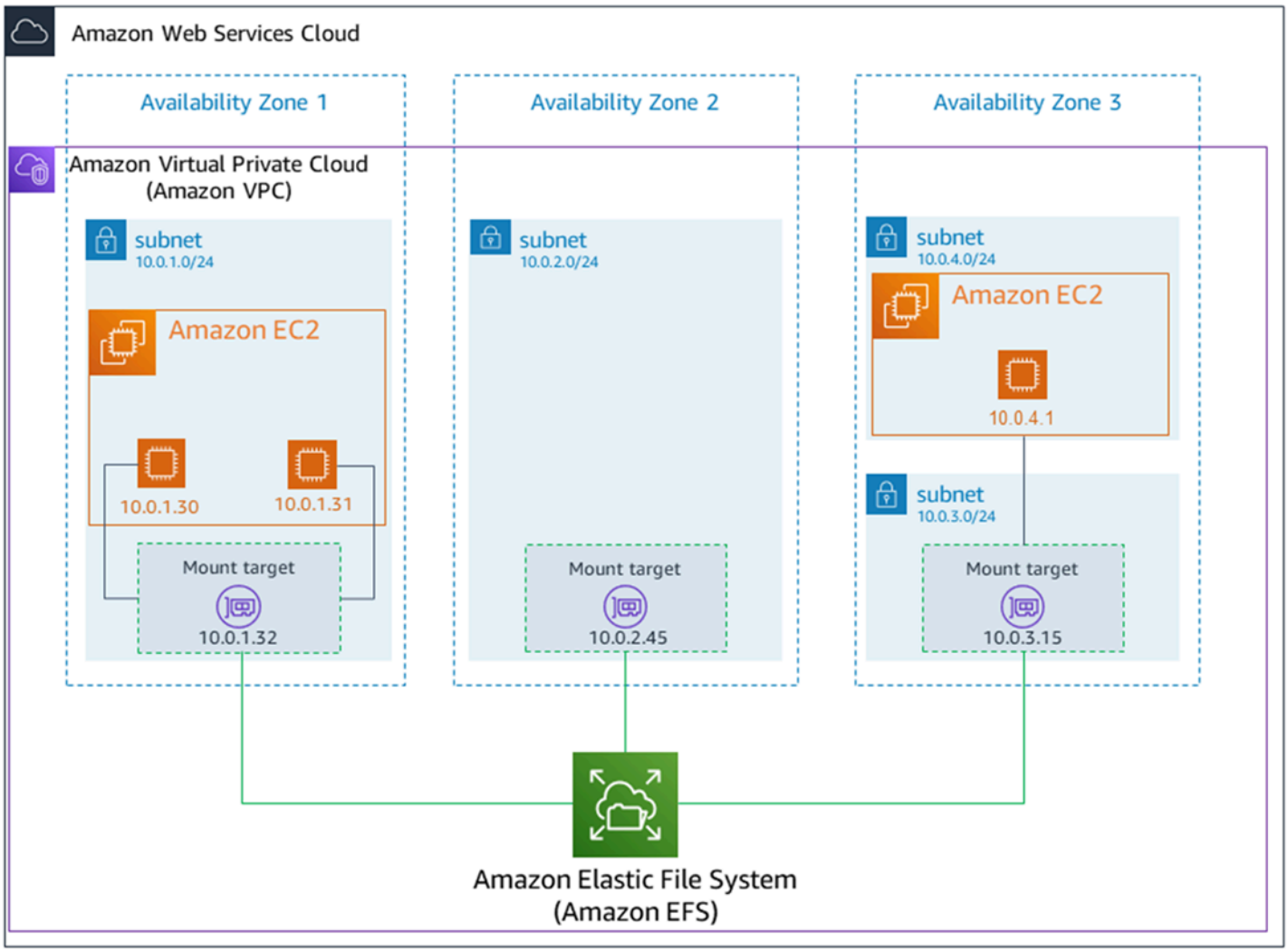
Vous pouvez monter vos systèmes de fichiers Amazon EFS sur les serveurs de votre centre de données sur site lorsque vous êtes connecté à votre Amazon VPC AWS Direct Connect AWS VPN ou vous pouvez monter vos systèmes de fichiers EFS sur des serveurs sur site pour migrer des ensembles de données vers EFS,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

Utiliser Amazon EFS avec Amazon EC2

Cette section explique comment les systèmes de fichiers Amazon EFS Régional et One Zone sont montés sur des instancesré EC2 dans un Amazon VPC.

Système de fichiers Amazon EFS Régional

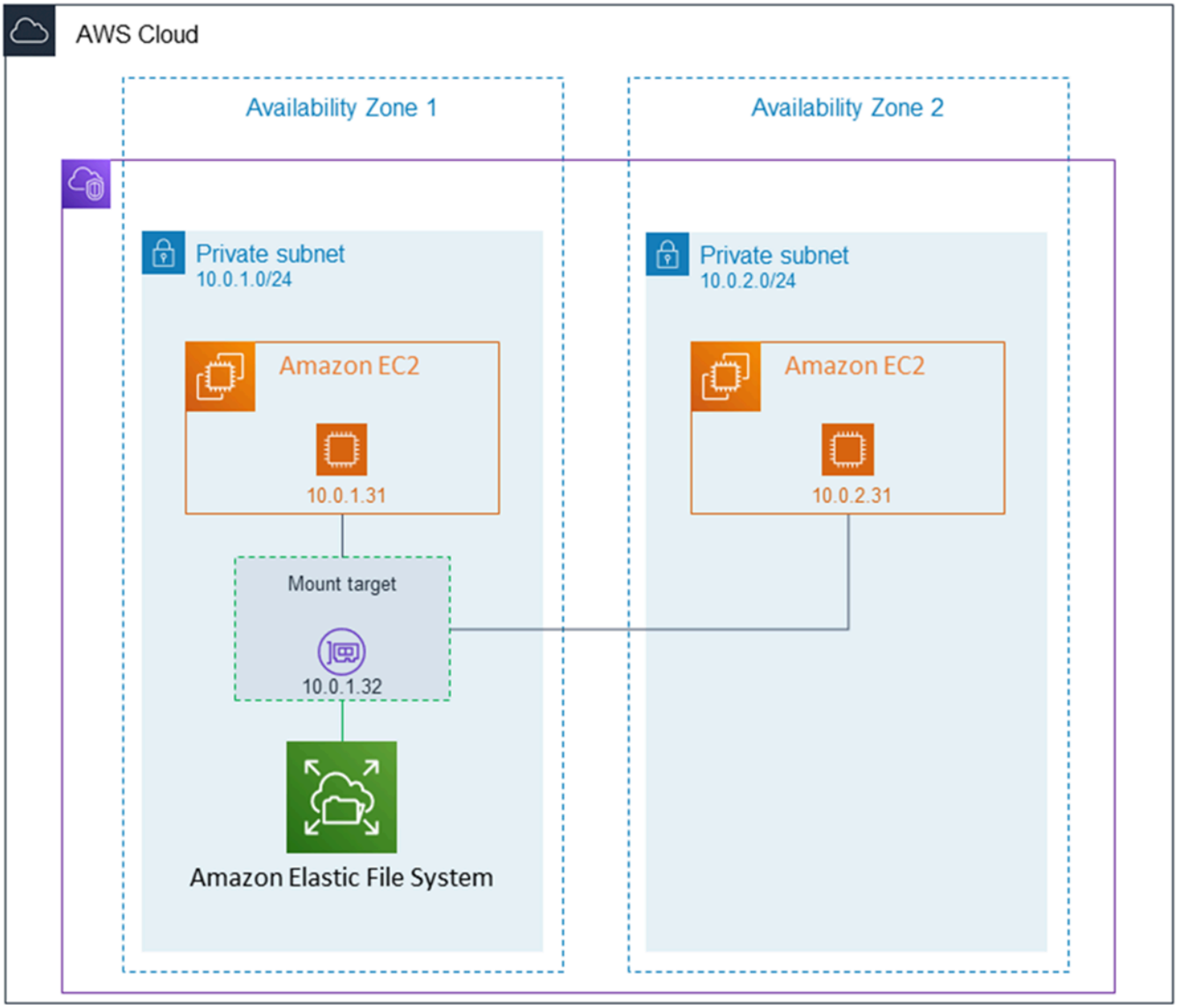
L'illustration suivante montre plusieurs instances EC2 accédant à un système de fichiers Amazon EFS configuré pour plusieurs zones de disponibilité dans une Région AWS.



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 plus d'informations, consultez Utilisation de l'assistant de Montage EFS pour Monter les systèmes de fichiers EFS.

Systèmes de fichiers Amazon EFS One Zone

L'illustration suivante montre plusieurs instances EC2 accédant à un système de fichiers One Zone à partir de différentes zones de disponibilité dans 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'instance EC2 sur laquelle vous le montez.

Dans cet exemple, l'instance EC2 de la zone de disponibilité us-west-2c paiera les frais d'accès aux données EC2 pour accéder à une cible de montage dans une autre zone de disponibilité. Pour plus d'informations, consultez Montage de systèmes de fichiers Zone unique.

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

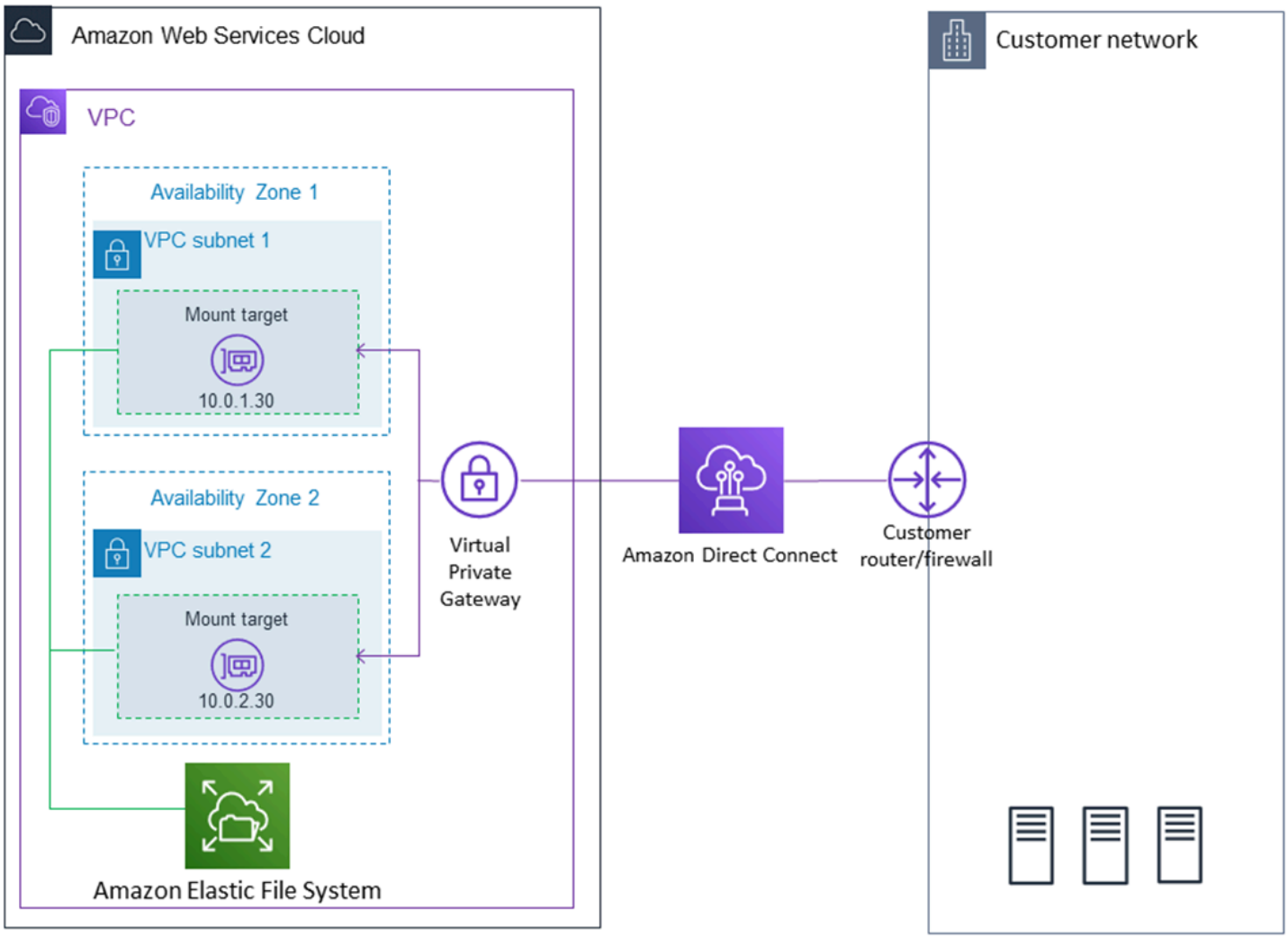
En utilisant un système de fichiers Amazon EFS monté sur un serveur sur site, vous pouvez migrer les données sur site vers le système de fichiers AWS Cloud hébergé dans un système de fichiers Amazon EFS. Vous pouvez également tirer parti de la transmission par rafales. En d'autres termes, vous pouvez déplacer des données à partir de vos serveurs sur site vers Amazon EFS et les analyser sur une flotte d'instances Amazon EC2 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 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 Procédure : Créer et monter un système de fichiers sur site avec AWS Direct Connect et VPN.

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 deSauvegarde de vos systèmes de fichiers Amazon EFS.

Récapitulatif de l'implémentation

Dans Amazon EFS, un système de fichiers est la ressource principale. Chaque système de fichiers possède des propriétés, comme un ID, un jeton de création, l'heure de création, la taille du système fichier en octets, le nombre de cibles de montage créées pour le système de fichiers et l'état du cycle de vie du système de fichiers. Pour plus d'informations, consultez CreateFileSystem.

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 sous-répertoire `efs-mount-point` en dehors de votre répertoire de base sur votre instance EC2 ou votre serveur sur site. 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,wsize=1048576,hard,timeo=600,retrans=2,noresvport file-
  system-DNS-name:/ ~/efs-mount-point
  ```

  Pour plus d'informations, consultez 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 plus d'informations, consultez Utilisation des points d'accès Amazon EFS.

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 Procédure pas à pas : créez un système de fichiers Amazon EFS et montez-le sur une instance Amazon EC2 à l'aide du AWS CLI.
- Vous pouvez également gérer ces ressources par programmation comme suit :
  - Utilisez les AWS kits de développement logiciel (SDK) : les AWS kits de développement logiciel simplifient 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.
  - Appeler l'API Amazon EFS directement depuis votre application Si vous ne pouvez pas utiliser les kits SDK pour une raison quelconque, vous pouvez effectuer les appels d'API Amazon EFS directement à partir de 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.

Authentification et contrôle d’accès

Vous devez disposer d’informations d’identification valides pour effectuer des requêtes d’API EFS, comme la création d’un système de fichiers. En outre, vous devez également disposer d’autorisations pour créer ou accéder aux 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 Elastic File System.

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 d’IAM pour contrôler l’accès aux données du système 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.

En fonction du 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 opérations de lecture/écriture ne vérifient pas la présence de verrouillages 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.

Classes de stockage EFS

Amazon EFS propose différentes classes de stockage pour différents besoins de stockage de données. Standard est la première classe de stockage dans laquelle les données sont écrites et la classe de stockage pour les données fréquemment consultées. Pour les fichiers moins fréquemment consultés, Amazon EFS propose les classes de stockage EFS Infrequent Access (IA) et EFS Archive. La classe de stockage IA est optimisée en termes de coûts pour les données consultées quelques fois par trimestre, tandis que la classe de stockage Archive est optimisée en termes de coûts pour les données consultées seulement quelques fois par an ou moins. Pour plus d'informations sur les classes de stockage Amazon EFS, consultez Classes de stockage 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 plus d'informations, consultez Gestion du stockage du système de fichiers.

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 plus d'informations, voir Répliquer des systèmes de fichiers.

Débuter avec Amazon Elastic File System

Amazon Elastic File System

Découvrez comment démarrer rapidement avec Amazon Elastic File System (Amazon EFS). Dans cet exercice de mise en route, vous allez créer votre système de fichiers EFS et lancer votre instance EC2. Vous allez également transférer des fichiers vers votre système de fichiers EFS en utilisant AWS DataSync puis en nettoyant vos ressources.

Les étapes suivantes sont incluses dans cet exercice de mise en route.

1. Passez en revue les conditions requises pour effectuer cet exercice de mise en route
2. Créez votre système de fichiers EFS et lancez votre instance EC2
3. Transférez des fichiers vers votre système de fichiers Amazon EFS à l'aide de AWS DataSync
4. Nettoyez les ressources et protégez votre AWS compte

Conditions préalables pour démarrer

Avant de commencer l'exercice de mise en route, assurez-vous de remplir les conditions suivantes :

- Vous êtes configuré avec Amazon EC2 et vous êtes habitué au lancement d'instances EC2. 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 Configuration pour utiliser Amazon EC2.
- Vos ressources Amazon VPC, Amazon EC2 et Amazon EFS sont toutes regroupées dans les mêmes Région AWS. Cet exercice utilise la région de l'ouest des États-Unis (Oregon) (us-west-2).
- Vous avez un VPC par défaut Région AWS que vous utilisez pour cet exercice de mise en route. 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 pour les instances Amazon EC2 et les cibles de montage
- 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 à l'aide des commandes AWS Command Line Interface (AWS CLI) pour effectuer les appels d'API Amazon EFS. Pour plus

d'informations, consultez Procédure pas à pas : créez un système de fichiers Amazon EFS et montez-le sur une instance Amazon EC2 à l'aide du AWS CLI.

Créez votre système de fichiers EFS et lancez votre instance EC2

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

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

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

Pour obtenir des instructions sur la création et le montage de votre système de fichiers EFS lors de la création d'un lancement d'instance EC2, consultez Utiliser Amazon EFS avec Amazon EC2.

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 instance EC2 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'instance EC2.
3. Lancez l'instance EC2 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, consultezCréation de systèmes de fichiers Amazon EFS.

Transférez des fichiers vers votre système de fichiers Amazon 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.

Conditions préalables au transfert de fichiers vers Amazon EFS à l'aide de AWS DataSync

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. Ces systèmes de fichiers sont, par exemple, ceux situés dans un centre de données sur site, les systèmes de fichiers en cloud autogérés et les systèmes de fichiers Amazon EFS.
- Vous êtes configuré pour utiliser DataSync. Pour en savoir plus, consultez la section Configuration avec 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 l'utilisation du transfert de fichiers DataSync 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 instance EC2 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

Ce guide contient des procédures que vous pouvez utiliser pour explorer davantage Amazon EFS. Avant d'effectuer cette étape de nettoyage, vous pouvez utiliser les ressources que vous avez créées et auxquelles vous vous êtes connecté dans cet exercice de mise en route dans le cadre de ces procédures pas à pas. Pour plus d'informations, consultez Procédures. Une fois que vous avez suivi les procédures, ou si vous ne voulez pas aller plus de l'avant, suivez les étapes ci-après pour nettoyer vos ressources et protéger votre Compte AWS.

Pour nettoyer les ressources et protéger votre compte

1. Connectez-vous à votre instance EC2 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'instance Amazon EC2 que vous avez lancée pour cet exercice de démarrage. Pour obtenir des instructions, consultez la section Résiliation d'instances Amazon EC2 dans le guide de l'AWS IAM Identity Center utilisateur.
6. Supprimez le groupe de sécurité que vous avez créé pour cet exercice de démarrage. 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.

Comprendre les types de systèmes de fichiers et les classes de stockage Amazon 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 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.

  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, consultezZones 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	Non résilient 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 ID Région AWS et AZ de chaque zone de disponibilité dans laquelle vous pouvez utiliser les systèmes de fichiers One Zone. Pour voir le mappage des identifiants AZ aux zones de disponibilité de votre compte, consultez la section Identifiants de zone de disponibilité 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	Identifiants de zone de disponibilité pris en charge
USA Est (Ohio)	us-east-2	use2-az1, use2-az2, use2-az3
US East (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
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

Région AWS Nom	Région AWS Code	Identifiants de zone de disponibilité pris en charge
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
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.

Optimisation des coûts de stockage

Les classes de stockage IA et Archive sont optimisées en termes de coûts pour les fichiers qui ne nécessitent pas les performances de latence du stockage standard. La latence du premier octet lors de la lecture à partir de l'une ou l'autre des classes de stockage peu utilisées est plus élevée que celle de la classe de stockage standard.

Grâce à la gestion du cycle de vie, vous pouvez optimiser les coûts de stockage en hiérarchisant automatiquement les données entre les classes de stockage en fonction des modèles d'accès de votre charge de travail. Vous pouvez déplacer des fichiers des classes de stockage IA ou Archive vers la classe de stockage Standard en définissant la politique de transition vers le cycle de vie standard sur votre système de fichiers. Ce paramètre fait passer les fichiers d'IA ou d'Archive à la version Standard lors de leur accès. Si vous souhaitez que vos fichiers restent dans la classe de stockage Standard fréquemment utilisée, désactivez la gestion du cycle de vie sur le système de fichiers. Pour de plus amples informations, veuillez consulter Gestion du stockage du système de fichiers.

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 Performances Amazon EFS.

Classe de stockage	Conçues pour	Latence de lecture du premier octet	Durabilité (conçu pour) [1]	Disponibilité SLA	Zones de disponibilité	Frais de facturation minimaux par fichier [2]	Durée minim de stock
Norme EFS	Données actives nécessitant une latence rapide inférieure à la milliseconde	Moins d'une milliseconde	99,999999999 % (11 9)	99,99 % (régional) 99,9 % (une zone)	=>3 (Régional) 1 (une zone)	Ne s'applique pas	Ne s'appe pas
Accès peu fréquent à l'EFS	Données inactives auxquelles on ne accède que quelques fois par trimestre.	Des dizaines de millisecondes				128 KIB	Ne s'appe pas
Archive EFS	Données inactives consultées quelques fois par an ou moins	Des dizaines de millisecondes		99,9 % (régional)	=>3 (Régional)	128 KIB	90 jou

Note

[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 midi (heure du Pacifique) répartiront les fichiers d'une valeur inférieure à 128 KiB dans la classe IA. Pour plus d'informations sur la façon dont Amazon EFS mesure et facture les fichiers individuels

et les métadonnées, consultezMesure : Comment Amazon EFS rapporte les tailles des systèmes de fichiers et des objets.

Tarification 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, consultezMesure : Comment Amazon EFS rapporte les tailles des systèmes de fichiers et des objets.

Des tarifs supplémentaires s'appliquent aux systèmes de fichiers qui utilisent un débit alloué ou en rafale.

- 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, consultezModes 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 la gestion du cycle de vie AWS Backup et la gestion du cycle de vie, consultezClasses de stockage EFS.

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.

Affichage de la taille des données de stockage dans la console Amazon EFS

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 plus d'informations, consultez Accès aux CloudWatch métriques.

Affichage de la taille des données de stockage à l'aide du 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 Mesures des objets du système de fichiers Amazon EFS.

Utilisation des ressources Amazon 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 en lecture et en écriture simultané à partir de plusieurs instances Amazon EC2. 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 les instances EC2 de votre cloud privé virtuel (VPC) sur Amazon VPC à l'aide du protocole Network File System versions 4.0 et 4.1 (NFSv4). Pour plus d'informations, consultez Comment fonctionne Amazon EFS.

À titre d'exemple, supposons qu'une ou plusieurs instances EC2 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.
- Créer des 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 instance Amazon EC2, vous devez créer des cibles de montage dans les sous-réseaux VPC.
- Créer des groupes de sécurité : une instance et une cible de montage ont toutes deux besoin de groupes de sécurité associés. 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 de la cible de montage qui autorise l'accès à partir d'une instance EC2 spécifique. Ensuite, vous pouvez monter le système de fichiers uniquement sur cette instance EC2.

Rubriques

- ID de ressource
- Jeton de création et idempotence
- Création de systèmes de fichiers Amazon EFS
- Suppression des systèmes de fichiers Amazon EFS

- Gérer des cibles de Montage
- Création de groupes de sécurité
- Création de politiques de système de fichiers
- Création de points d'accès
- Supprimer des points d'accès
- Balisage des ressources Amazon EFS

ID de ressource

Amazon EFS attribue des identifiants (ID) de ressource uniques à toutes les ressources EFS lors de leur création. Tous les ID de ressource EFS 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 le mois d'octobre 2021, les ID attribués au système de fichiers et aux ressources des cibles de montage nouvellement créés utilisaient 8 caractères après le tiret (par exemple, `fs-12345678`). De mai à octobre 2021, nous avons modifié les ID de ces types de ressource pour utiliser 17 caractères après le tiret (par exemple, `fs-1234567890abcdef0`). Selon le moment où votre compte a été créé, vous pouvez disposer de ressources de systèmes de fichiers et de cibles de montage avec des ID courts, bien que toutes les nouvelles ressources de ces types reçoivent les ID longs : 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 Amazon EFS

Vous découvrirez ci-dessous comment créer un système de fichiers Amazon EFS à l'aide du AWS Management Console et du AWS CLI.

Rubriques

- Autorisations requises pour créer des systèmes de fichiers
- Options de configuration pour les systèmes de fichiers

Autorisations 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 Elastic File System.

Options de configuration pour les systèmes de fichiers

Vous pouvez créer un système de fichiers à l’aide de la console Amazon EFS ou à l’aide de l’ AWS Command Line Interface (AWS CLI). Vous pouvez également créer des systèmes de fichiers par programmation en utilisant directement AWS les SDK ou l'API Amazon EFS. Si vous utilisez l'API

Amazon EFS ou un AWS SDK, vous pouvez utiliser l'action d'API `CreateFileSystem` EFS pour créer des politiques de système de fichiers.

Lorsque vous créez un système de fichiers Amazon EFS à l'aide du flux de création personnalisé de la console ou de l' AWS CLI, vous pouvez choisir des paramètres pour les fonctionnalités du système de fichiers et des options de configuration suivantes.

Type de système de fichiers

Le type de système de fichiers détermine la disponibilité et la durabilité selon lesquelles un système de fichiers Amazon EFS stocke les données dans une Région AWS. Vous avez les choix suivants pour votre système de fichiers :

- 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. 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.
- Choisissez Une zone pour créer un système de fichiers qui stocke les données et les métadonnées de manière redondante dans une seule zone de disponibilité. Les systèmes de fichiers qui utilisent des classes de stockage ne peuvent avoir qu'une seule cible de montage. Cette dernière doit se trouver dans la zone de disponibilité dans laquelle le système de fichiers est créé.

Sauvegardes automatiques

Lorsque vous créez un système de fichiers à l'aide de la console, les sauvegardes automatiques sont toujours activées par défaut . Lorsque vous créez un système de fichiers à l'aide de l'interface de ligne de commande ou de l'API, les sauvegardes automatiques sont activées par défaut uniquement lorsque ces systèmes de fichiers utilisent des systèmes de fichiers One Zone. Pour plus d'informations, consultez Sauvegardes automatiques.

Stratégie de cycle de vie

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.

- TransitionToArchive définie sur 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 des AWS SDK, 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, consultez Gestion du stockage du système de fichiers.

Chiffrement

Vous pouvez activer le chiffrement au repos lors de la création d'un système de fichiers. Si vous activez le chiffrement au repos pour votre système de fichiers, toutes les données et métadonnées stockées sur celui-ci sont chiffrées. Vous pouvez activer le chiffrement des données en transit ultérieurement, lors du montage du système de fichiers. Pour plus d'informations sur le chiffrement Amazon EFS, consultez Chiffrement des données dans Amazon EFS.

Pour créer les cibles de montage du système de fichiers dans votre VPC, vous devez spécifier des sous-réseaux VPC. La console pré-remplit la liste des VPC de votre compte qui se trouvent dans la Région AWS sélectionnée. Tout d'abord, vous sélectionnez votre VPC, puis la console affiche la liste des zones de disponibilité dans le VPC. Pour chaque zone de disponibilité, vous pouvez sélectionner un sous-réseau de la liste ou utiliser le sous-réseau par défaut, s'il existe. Une fois que vous avez sélectionné un sous-réseau, vous pouvez spécifier une adresse IP disponible dans le sous-réseau ou laisser Amazon EFS choisir automatiquement une adresse.

Modes de débit

Vous avez le choix entre trois modes de débit :

- Élastique (recommandé) : il fournit un débit qui augmente ou diminue automatiquement en temps réel, afin de répondre aux besoins en performances de votre charge de travail.

  > **Note**
  >
  > Le débit élastique n'est disponible que pour les systèmes de fichiers dotés du mode de performance General Purpose.

- Provisionné : il fournit le niveau de débit que vous spécifiez, 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.

Pour plus d’informations, consultez Modes de débit.

> **Note**
>
> Des frais supplémentaires sont associés à l’utilisation des débits Élastique et Provisionné. Pour de plus amples informations, consultez la tarification Amazon EFS.

Modes de performances

Lors de la création d'un système de fichiers, vous sélectionnez également un mode de performances. Vous avez le choix entre deux modes : Usage général et E/S max.

- Le mode Usage général 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 mode Max E/S n’est pas pris en charge pour les systèmes de fichiers Zone unique ou les systèmes de fichiers qui utilisent le débit élastique.

> **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.

Pour plus d’informations, consultez Modes de performances.

Création rapide d'un système de fichiers doté de paramètres recommandés (console)

Au cours de cette étape, 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 d'un système de fichiers avec des paramètres personnalisés (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 :

   - Sauvegardes automatiques activées. Pour de plus amples informations, veuillez consulter Sauvegarde de vos systèmes de fichiers Amazon EFS.
   - Les cibles de Montage sont configurées avec les paramètres suivants :
     - Créé dans chaque zone de disponibilité Région AWS dans laquelle le système de fichiers est créé.
     - Situé dans les sous-réseaux par défaut du VPC que vous avez sélectionné.
     - Utilisation du groupe de sécurité par défaut du VPC : vous pouvez gérer les groupes de sécurité une fois le système de fichiers créé.

     Pour de plus amples informations, veuillez consulter Gestion de l'accessibilité réseau du système de fichiers.
   - Type de système de fichiers régional : pour de plus amples informations, veuillez consulter Types de système de fichiers EFS.
   - Performance à usage général : pour de plus amples informations, veuillez consulter Modes de performances.
   - Débit élastique – Pour plus d'informations, consultez Modes de débit.
   - Chiffrement des données au repos activé à l'aide de votre clé par défaut pour Amazon EFS (`aws/elasticfilesystem`) — Pour plus d'informations, consultezChiffrement de données au repos.
   - gestion du cycle de vie : Amazon EFS crée le système de fichiers selon les politiques de cycle de vie suivantes :
     - Transition vers IA définie sur 30 jours depuis le dernier accès.
     - TransitionToArchive définie sur 90 jours depuis le dernier accès.

- Transition vers Standard définie sur Aucun.

Pour de plus amples informations, veuillez consulter Gestion du stockage du système de fichiers.

Après avoir créé le système de fichiers, vous pouvez personnaliser ses paramètres, à l'exception de la disponibilité et de la durabilité, du chiffrement et du mode de performance.

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 État du système de fichiers.

Création d'un système de fichiers avec des paramètres personnalisés (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 de plus amples informations sur la création d'un système de fichiers à l'aide des paramètres recommandés par le service, veuillez consulter Création rapide d'un système de fichiers doté de paramètres recommandés (console).

Création d'un système de fichiers Amazon EFS avec des paramètres personnalisés en quatre étapes, à l'aide de la console :

- 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 la boîte de dialogue Création d'un 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 par le service. 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, choisissez une option de disponibilité :

      - Choisissez Régional pour créer un système de fichiers qui stocke les données et les métadonnées du système de fichiers de manière redondante dans toutes les zones de disponibilité d'une Région AWS. Régional offre les niveaux les plus élevés de disponibilité et de durabilité.
      - Choisissez One Zone pour créer un système de fichiers qui stocke les données et les métadonnées de manière redondante dans 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. Pour plus d'informations, consultez Classes de stockage EFS.

   c. Les sauvegardes automatiques sont activées par défaut. Vous pouvez désactiver les sauvegardes automatiques en décochant la case. Pour plus d'informations, consultez Sauvegarde de vos systèmes de fichiers Amazon EFS.

   d. 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 stockage du système de fichiers.

e. Pour le Chiffrement, le chiffrement des données au repos est activé par défaut. Amazon EFS utilise votre AWS Key Management Service (AWS KMS) clé de service EFS (`aws/elasticfilesystem`) par défaut. Pour choisir une clé KMS différente pour le chiffrement, ouvrez les Personnaliser les paramètres 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.

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.

      Les systèmes de fichiers Amazon EFS mesurent les demandes de lecture à un tiers du taux des autres demandes. Une fois que vous avez indiqué 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 Modes de débit.

   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 plus d'informations, consultez 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 Cloud privé virtuel (VPC) dans lequel vous souhaitez que les instances EC2 se connectent à votre système de fichiers. Pour plus d'informations, consultez Gestion de l'accessibilité réseau du système de fichiers.
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.
   - Adresse IP : par défaut, Amazon EFS choisit automatiquement l'adresse IP parmi celles disponibles dans le sous-réseau. Vous pouvez également saisir une adresse IP spécifique qui se trouve dans le sous-réseau. Bien que les cibles de montage possèdent une adresse IP unique, elles constituent des ressources réseau redondantes à haute disponibilité.
   - Groupes de sécurité : vous pouvez spécifier un ou plusieurs groupes de sécurité pour la cible de montage. Pour plus d'informations, consultez Utilisation de groupes de sécurité VPC pour les instances Amazon EC2 et les cibles de montage.

Pour ajouter un autre groupe de sécurité ou pour modifier le groupe de sécurité, sélectionnez Choisir des groupes de sécurité et ajoutez un autre groupe de sécurité à la liste. Si vous ne souhaitez pas utiliser le groupe de sécurité par défaut, vous pouvez le supprimer. Pour plus d'informations, consultez Création de groupes de sécurité.

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 plus d'informations, consultez Utilisation d'IAM pour contrôler l'accès aux données du système de fichiers.

1. Dans les Options de politique, vous pouvez choisir l'une des combinaisons des politiques préconfigurées disponibles :
   - Empêcher l'accès à la racine par défaut
   - Appliquer l'accès en lecture seule par défaut
   - Appliquer le chiffrement en transit pour tous les clients
2. Utilisez l'Éditeur de politique pour personnaliser une politique préconfigurée ou pour créer la vôtre. Lorsque vous choisissez l'une des politiques préconfigurées, la définition de la politique JSON apparaît dans l'éditeur de politique. Vous pouvez modifier le fichier JSON pour créer la politique de votre choix. Pour annuler vos modifications, choisissez Effacer.

   Les politiques préconfigurées sont de nouveau disponibles dans les Options de politique.
3. 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 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.

Création d'un système de fichiers (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 qui utilise les classes de stockage EFS Archive, avec les sauvegardes automatiques activées, utilisez la commande d'interface de ligne de commande Amazon EFS `create-file-system` (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 bursting \
--region aws-region \
--tags Key=key,Value=value Key=key1,Value=value1 \
--profile adminuser
```

  Par exemple, la commande `create-file-system` suivante crée un système de fichiers dans la Région AWS `us-west-2`. 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 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.

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

- L'exemple suivant présente la création d'un système de fichiers qui utilise la classe de stockage Standard dans la zone de disponibilité `us-west-2a` à l'aide de la propriété `availability-zone-name`.

```
aws efs create-file-system \
--creation-token MyFirstFS \
```

```
--availability-zone-name us-west-2a \
--backup \
--encrypted \
--performance-mode generalPurpose \
--throughput-mode bursting \
--region us-west-2 \
--tags Key=Name,Value="Test File System" Key=developer,Value=rhoward \
--profile adminuser
```

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 des systèmes de fichiers Amazon 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 plus d'informations, consultez Supprimer des configuration de réplication.

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

Supprimer un système de fichiers (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.

Supprimer un système de fichiers (CLI)

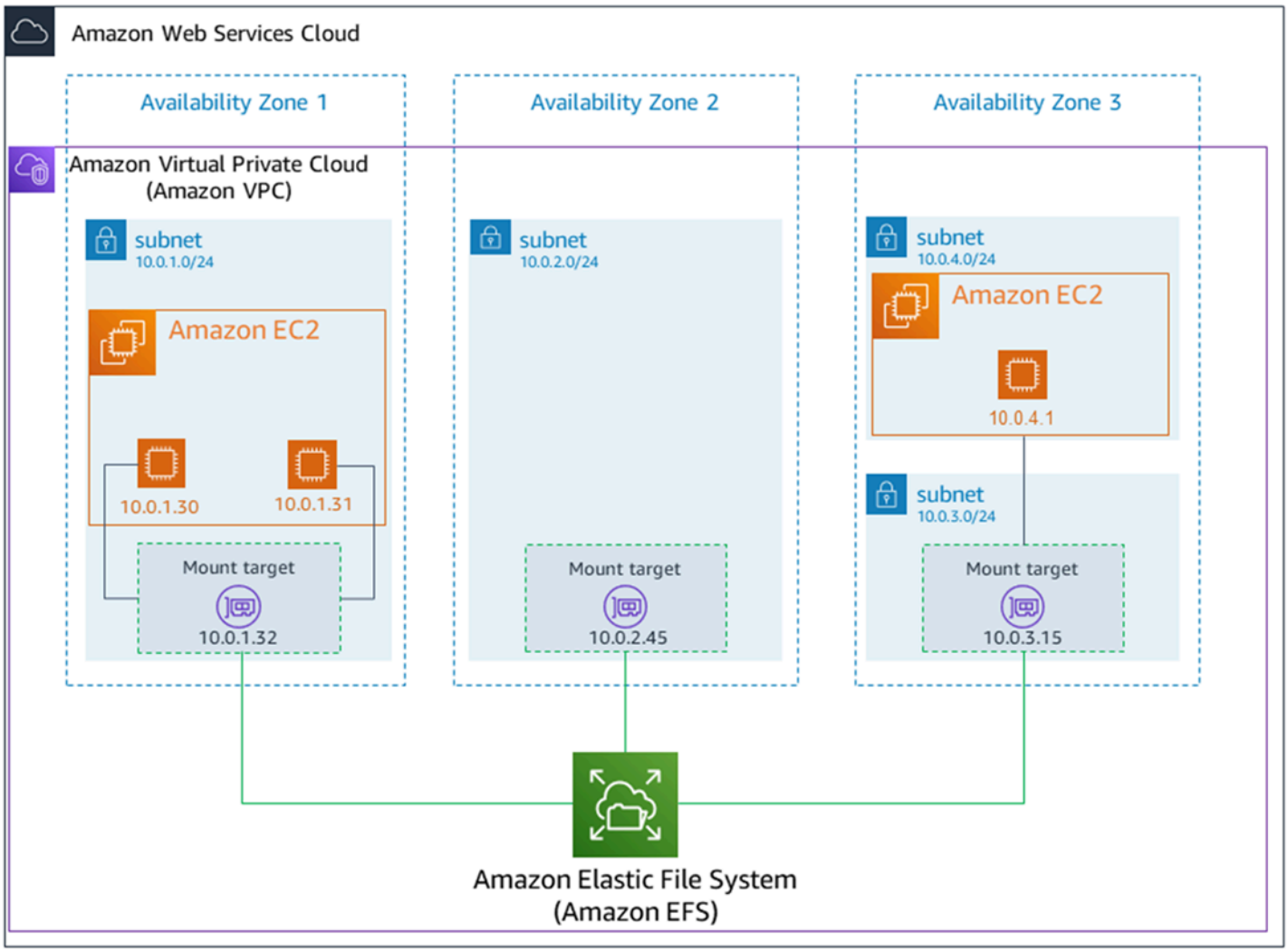
Avant de pouvoir utiliser la AWS CLI commande pour supprimer un système de fichiers, vous devez supprimer toutes les cibles de montage et tous les points d'accès créés pour le système de fichiers.

Pour des exemples de AWS CLI commandes, voirÉtape 4 : Nettoyer.

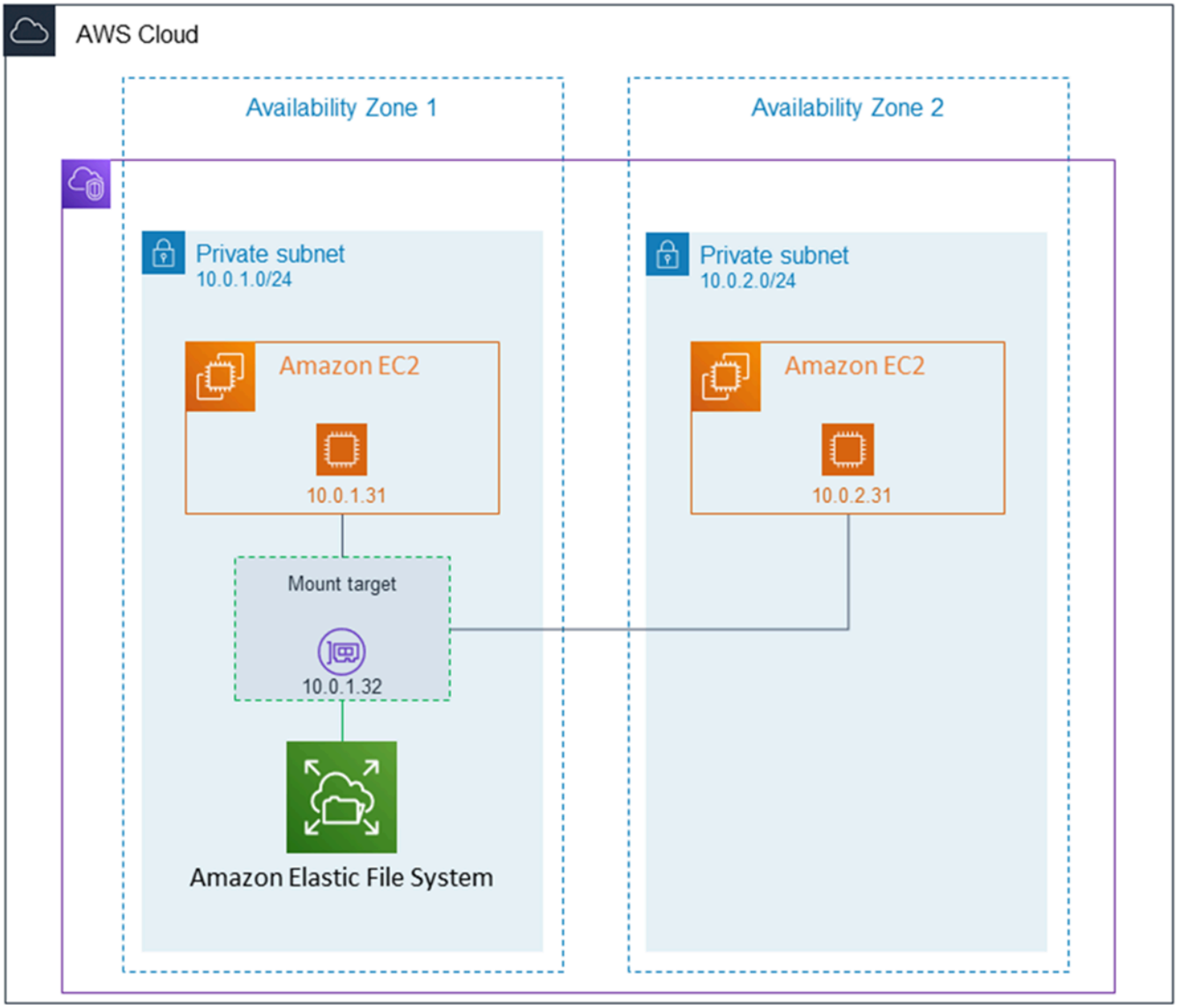
Gérer des cibles de Montage

Après avoir créé un système de fichiers Amazon EFS, vous pouvez créer des cibles de montage. Pour les systèmes de fichiers Amazon 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.



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'instance EC2 dans la zone de disponibilité `us-west2c` 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 :

- Gestions 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'instance Amazon EC2 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 plus d'informations, consultez Utilisation des utilisateurs, des groupes et des autorisations au niveau du système de fichiers réseau (NFS).

Vous pouvez créer des cibles de montage pour un système de fichiers à l'aide du AWS Management Console AWS CLI, ou par programmation à l' AWS aide des SDK. Si vous utilisez la console, vous pouvez créer des cibles de montage lorsque vous créez un système de fichiers pour la première fois ou que ce dernier créé.

Pour obtenir des instructions sur la création de cibles de montage à l'aide de la console Amazon EFS lors de la création d'un système de fichiers, consultezÉtape 2 : configurer l'accès réseau.

Gérer les cibles de montage (console)

Utilisez la procédure suivante pour ajouter ou modifier des cibles de montage pour un système de fichiers Amazon EFS existant.

Pour gérer les cibles de montage sur un système de fichiers 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. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers. La page Systèmes de fichiers affiche les systèmes de fichiers EFS de votre compte.
3. Choisissez le système de fichiers pour lequel vous souhaitez gérer les cibles de montage en choisissant son Nom ou l'ID du système de fichiers pour afficher la page de détails de ce dernier.
4. Choisissez Réseau pour afficher la liste des cibles de montage existantes.
5. Choisissez Gérer pour afficher la page de la Zone de disponibilité et apporter des modifications.

   Sur cette page, pour les cibles de montage existantes, vous pouvez ajouter et supprimer des groupes de sécurité ou supprimer la cible de montage. Vous pouvez également créer de nouvelles cibles de montage.

   > **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.

- Pour supprimer un groupe de sécurité d'une cible de montage, choisissez X à côté de l'ID du groupe de sécurité.
- Pour ajouter un groupe de sécurité à une cible de montage, choisissez Sélectionner les groupes de sécurité pour afficher la liste des groupes de sécurité disponibles. Vous pouvez également saisir un ID de groupe de sécurité dans le champ de recherche en haut de la liste.
- Pour mettre en file d'attente une cible de montage en vue de sa suppression, choisissez Supprimer.

> **Note**
>
> Avant de supprimer une cible de montage, démontez le système de fichiers.

- Pour ajouter une cible de montage, choisissez Ajouter une cible de montage. Cette option est uniquement disponible pour les systèmes de fichiers qui utilisent des classes de stockage régionales EFS, et si aucune cible de montage n'existe déjà dans chaque zone de disponibilité pour la Région AWS.

6. Choisissez Enregistrer pour enregistrer les changements.

Pour modifier le VPC d'un système de fichiers Amazon EFS (console)

Pour modifier le VPC pour la configuration réseau d'un système de fichiers, vous devez supprimer toutes les cibles de montage existantes 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. La page Systèmes de fichiers affiche les systèmes de fichiers EFS de votre compte.
3. Pour le système de fichiers dont vous souhaitez modifier le VPC, choisissez le Nom ou l'ID du système de fichiers. La page de détails de ce système de fichiers s'affiche.
4. Choisissez Réseau pour afficher la liste des cibles de montage existantes.
5. Choisissez Gérer. La page Zone de disponibilité apparaît.
6. Supprimez toutes les cibles de montage affichées sur la page.
7. Choisissez Enregistrer pour enregistrer les modifications et supprimer les cibles de montage. L'onglet Réseau présente les cibles de montage avec un statut suppression.

8. Lorsque le statut de toutes les cibles de montage est supprimée, choisissez Gérer. La page Zone de disponibilité apparaît.
9. Choisissez le nouveau VPC dans la liste Virtual Private Cloud (VPC).
10. Choisissez Ajouter une cible de montage pour ajouter une nouvelle cible de montage. Pour chaque cible de montage ajoutée, saisissez les informations suivantes :
    - Une Zone de disponibilité
    - Un ID de sous-réseau
    - Une adresse IP, ou conservez le paramètre Automatique
    - Un ou plusieurs groupes de sécurité
11. Choisissez Enregistrer pour appliquer les modifications apportées au VPC et à la cible de montage.

Gestion des cibles de montage (CLI)

> **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.

Pour créer une cible de montage (CLI)

- Pour créer une cible de montage utilisez la commande d'interface de ligne de commande `create-mount-target` (l'opération correspondante est CreateMountTarget), comme illustré ci-après.

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

L'exemple suivant présente la commande avec des exemples de données.

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

```
--file-system-id fs-0123467 \
--subnet-id  subnet-b3983dc4 \
--security-group sg-01234567 \
--region us-east-2 \
--profile adminuser
```

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.

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

Pour extraire la liste des cibles de montage pour un système de fichiers (CLI)

- Vous pouvez également extraire une liste des cibles de montage créées pour un système de fichiers à l'aide de la commande d'interface de ligne de commande describe-mount-targets (l'opération correspondante est DescribeMountTargets), comme illustré ci-après.

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

```
{
    "MountTargets": [
        {
            "OwnerId": "111122223333",
            "MountTargetId": "fsmt-48518531",
            "FileSystemId": "fs-a576a6dc",
            "SubnetId": "subnet-88556633",
            "LifeCycleState": "available",
            "IpAddress": "172.31.25.203",
            "NetworkInterfaceId": "eni-0123456789abcdef1",
            "AvailabilityZoneId": "use2-az2",
            "AvailabilityZoneName": "us-east-2b"
        },
```

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

Pour supprimer une cible de montage existante (CLI)

- Pour supprimer une cible de montage existante, utilisez la `delete-mount-target` AWS CLI commande (l'opération correspondante estDeleteMountTarget), 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 \
```

Pour modifier le groupe de sécurité d'une cible de montage existante

- 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 estModifyMountTargetSecurityGroups) 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
  ```

Pour plus d'informations, consultez Procédure pas à pas : créez un système de fichiers Amazon EFS et montez-le sur une instance Amazon EC2 à l'aide du AWS CLI.

Création de groupes de sécurité

Des groupes de sécurité sont associés à une instance Amazon EC2 et à une cible de montage. Ces groupes de sécurité font office de pare-feu virtuel contrôlant le trafic entre elles. Si vous n'indiquez pas 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.

Quoi qu'il en soit, pour autoriser le trafic entre une instance EC2 et une cible de montage (et donc le système de fichiers), vous devez configurer les règles suivantes dans ces groupes de sécurité :

- Les groupes de sécurité que vous associez à une cible de montage doivent autoriser l'accès entrant pour le protocole TCP sur le port NFS à partir de toutes les instances EC2 sur lesquelles vous voulez monter le système de fichiers.
- Chaque instance EC2 qui monte le système de fichiers doit avoir un groupe de sécurité qui autorise l'accès sortant à la cible de montage sur le port NFS.

Pour modifier les groupes de sécurité associés aux cibles de montage de vos systèmes de fichiers EFS, consultez Gérer des cibles de Montage.

Pour plus d'informations sur les groupes de sécurité, consultez les groupes de sécurité Amazon EC2 pour les instances Linux dans le guide de l'utilisateur Amazon EC2.

> **Note**
>
> La section suivante, spécifique à Amazon EC2, explique comment créer des groupes de sécurité pour que vous puissiez utiliser Secure Shell (SSH) pour vous connecter à toutes les instances qui ont monté des systèmes de fichiers Amazon EFS. Si vous n'utilisez pas SSH pour vous connecter à vos instances Amazon EC2, vous pouvez ignorer cette section.

Création d'un groupe de sécurité à l'aide de la console

Vous pouvez utiliser le AWS Management Console pour créer des groupes de sécurité dans votre VPC. Pour connecter votre système de fichiers Amazon EFS à votre instance Amazon EC2, vous devez créer deux groupes de sécurité : le premier pour votre instance Amazon EC2 et le second pour votre cible de montage Amazon EFS.

1. Créez deux groupes de sécurité dans votre VPC. Pour obtenir des instructions, consultez la section Créer un groupe de sécurité dans le guide de l'utilisateur Amazon VPC.
2. Sur la console VPC, vérifiez les règles par défaut pour ces groupes de sécurité. Les deux groupes de sécurité doivent avoir uniquement une règle sortante qui autorise le trafic en sortie.
3. Vous devez autoriser un accès supplémentaire aux groupes de sécurité comme suit :

    a. Ajoutez une règle au groupe de sécurité EC2 pour autoriser l'accès SSH à l'instance sur le port 22, comme illustré ci-après. Cette opération est utile si vous prévoyez d'utiliser un client SSH comme PuTTY pour vous connecter à votre instance EC2 et l'administrer via une interface de terminal. Vous pouvez éventuellement limiter l'adresse Source.

Pour obtenir des instructions, consultez la section Ajouter des règles à un groupe de sécurité dans le guide de l'utilisateur Amazon VPC.

b. Ajoutez une règle au groupe de sécurité cible de montage pour autoriser l'accès entrant depuis le groupe EC2Security sur le port TCP 2049. Le groupe de sécurité attribué en tant que source est le groupe de sécurité associé à l'instance EC2.

   Pour afficher les groupes de sécurité associés aux cibles de montage de vos systèmes de fichiers, dans la console EFS, sélectionnez l'onglet Réseau sur la page de détails du système de fichiers. Pour plus d'informations, consultez Gérer des cibles de Montage.

> **Note**
>
> Vous n'avez pas besoin d'ajouter une règle sortante, car la règle sortante par défaut autorise tout le trafic en sortie. (Si vous supprimer la règle sortante par défaut, 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).

4. Vérifiez que les deux groupes de sécurité autorisent maintenant l'accès entrant et l'accès sortant, comme décrit dans cette section.

Création d'un groupe de sécurité à l'aide de la CLI

Pour un exemple montrant comment créer des groupes de sécurité à l'aide du AWS CLI, voirÉtape 1 : Créer les ressources Amazon EC2.

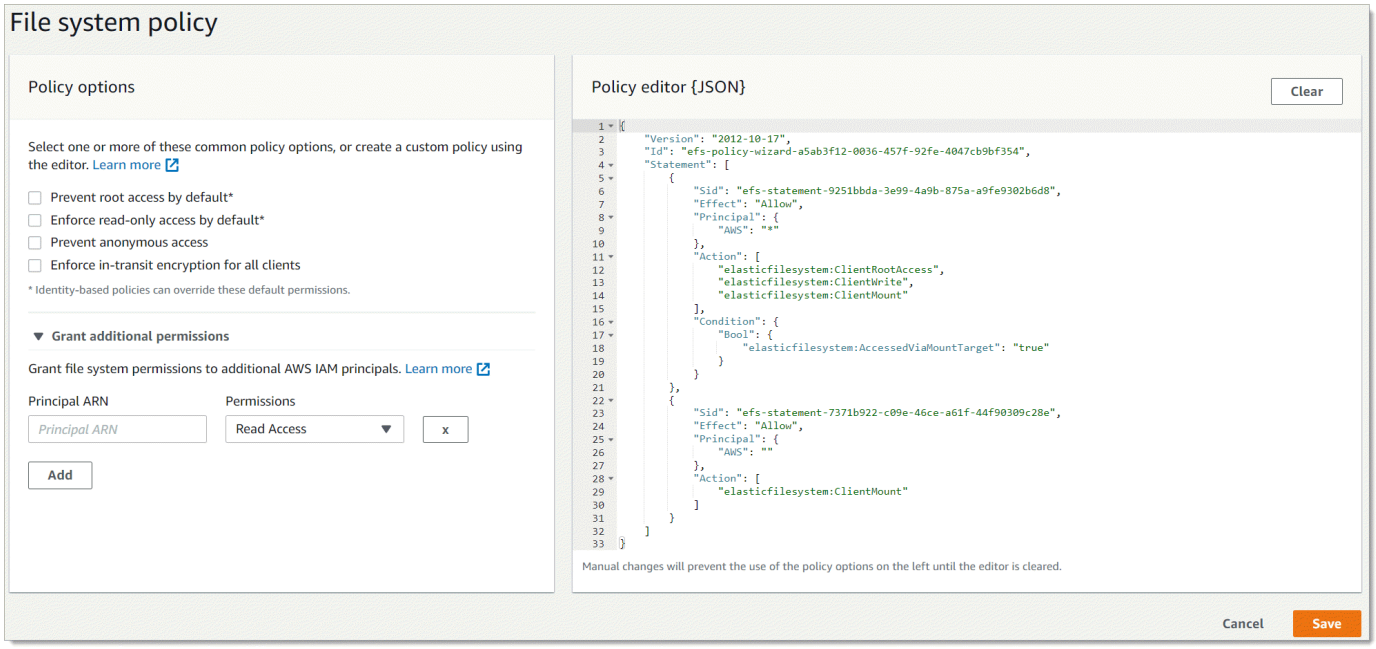
Création de politiques de système de fichiers

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 AWS les SDK ou l'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 d'IAM pour contrôler l'accès aux données du système de fichiers.

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

Création d'une politique de système de fichiers (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. La page de détails de ce système de fichiers s'affiche.
4. Choisissez Politique du système de fichiers, puis Modifier. La page Politique du système de fichiers s'affiche.



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.

Création d'une politique de système de fichiers (CLI)

Dans l'exemple suivant, la commande put-file-system-policyCLI 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 des points d'accès Amazon EFS à l'aide du AWS Management Console ou du AWS CLI. Vous pouvez également créer des points d'accès par programmation à l'aide des AWS SDK ou de l'API Amazon EFS directement. Vous ne pouvez pas modifier un point d’accès une fois qu’il a été créé. Un système de fichiers peut avoir 1 000 points d’accès maximum. Pour plus d’informations sur les points d’accès EFS, consultez Utilisation des points d’accès Amazon EFS.

Création d'un point d'accès (console)

Vous pouvez créer et supprimer des points d'accès Amazon EFS à l' AWS Management Console aide de l'API et des kits SDK Amazon EFS AWS Command Line Interface (AWS CLI). Vous ne

pouvez pas modifier un point d'accès une fois qu'il a été créé. Un système de fichiers peut avoir 1 000 points d'accès maximum.

> **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 des 1 000 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.

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 plus d'informations, consultez 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 plus d'informations, consultez 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.
- ID de groupes secondaires : saisissez une liste facultative d'identifiants d'ID de groupes secondaires séparés par des virgules.

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 plus d'informations, consultez 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 groupe 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.

Création d'un point d'accès (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={OwnerUid=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 des 1 000 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.

Supprimer un point d'accès (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.

Supprimer un point d'accès (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
```

Balisage des ressources Amazon EFS

Pour vous aider à gérer vos ressources Amazon EFS, vous pouvez attribuer vos propres métadonnées à chaque ressource sous la forme de balises. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou 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.

Marquer une ressource de système de fichiers ou de point d'accès (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.

Marquer un système de fichiers ou une ressource de point d'accès (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

Installation des outils Amazon EFS

Le package `amazon-efs-utils` est une collection open source d'outils Amazon EFS, également appelée client Amazon EFS. Vous trouverez ci-dessous une description du client Amazon EFS. Le client Amazon EFS inclut l'assistant de montage Amazon EFS, qui facilite le montage des systèmes de fichiers EFS. L'utilisation du client EFS permet d'utiliser Amazon CloudWatch pour surveiller l'état de montage d'un système de fichiers EFS. Pour monter votre système de fichiers Amazon EFS sur votre instance d'Amazon EC2, vous devez commencer par installer un client NFS.

Rubriques

- À propos du client Amazon EFS
- Utilisation AWS Systems Manager pour installer ou mettre à jour automatiquement le client Amazon EFS
- Installation manuelle du client Amazon EFS
- Installation et mise à niveau botocore
- Mise à niveau d'stunnel

À propos du client Amazon EFS

Le client Amazon EFS (`amazon-efs-utils`) est une collection open source d'outils Amazon EFS. L'utilisation du client Amazon EFS est gratuite, que vous pouvez télécharger GitHub ici : https://github.com/aws/efs-utils.

Le `amazon-efs-utils` package est préinstallé sur Amazon Linux 2023 (AL2023), Amazon Linux 2 (AL2) et Amazon Linux (AL1) Amazon Machine Images (AMI). Le package est disponible dans les référentiels de packages Amazon Linux et vous pouvez générer et installer le package sur d'autres distributions Linux. Vous pouvez également l'utiliser AWS Systems Manager pour installer ou mettre à jour automatiquement le package. Pour plus d'informations, consultez Utilisation AWS Systems Manager pour installer ou mettre à jour automatiquement le client Amazon EFS.

> **Note**
>
> L'AMI Amazon Linux (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.

Le client Amazon EFS inclut un assistant de montage et des outils qui facilitent le chiffrement des données en transit pour les systèmes de fichiers Amazon EFS. Un assistant de montage est un programme que vous utilisez lorsque vous montez un type spécifique de système de fichiers. Nous vous recommandons de recourir à l'aide au montage incluse dans le client Amazon EFS pour monter vos systèmes de fichiers Amazon EFS. L'utilisation du client Amazon EFS simplifie le montage des systèmes de fichiers EFS et peut améliorer les performances des systèmes de fichiers. Pour plus d'informations sur le client EFS et l'aide au montage, consultez Montage des systèmes de fichiers 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 Amazon EFS avec le protocole TLS (Transport Layer Security), celui-ci procède à la vérification du nom d'hôte du certificat. L'assistant de montage Amazon EFS 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 Amazon EFS à l'aide de TLS échoue.
> Une fois que vous avez installé le package`amazon-efs-utils`, pour mettre à niveau la version de stunnel de votre système, 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 instances EC2. Pour plus d'informations, consultez Utilisation AWS Systems Manager pour installer ou mettre à jour automatiquement le client Amazon EFS.
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 2 (AL2)	rpm	`systemd`
CentOS 7, 8	rpm	`systemd`
Amazon Linux (AL1) 09/2017 **Note** L'AMI Amazon Linux (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 ou ultérieurement (version 2.0 et ultérieure).	rpm	`upstart`
Debian 9, 10	deb	`systemd`
Fedora 28 - 32	rpm	`systemd`
macOS Big sur		`launchd`
macOS Monterey		`launchd`
macOS Ventura		`launchd`

Distribution	Type de package	Système **`init`**
OpenSUSE Leap, Tumbleweed	rpm	`systemd`
Oracle 8	rpm	`systemd`
Red Hat Enterprise Linux (RHEL) 7, 8, 9	rpm	`systemd`
SUSE Linux Enterprise Server (SLES) 12, 15	rpm	`systemd`
Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS	deb	`systemd`

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

Utilisation AWS Systems Manager pour installer ou mettre à jour automatiquement le client Amazon EFS

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 du `amazon-efs-utils` package sur vos instances 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 instances Amazon EC2.
- Automatisez le processus de maintien de vos instances Amazon EC2 dans un état défini.

Pour plus d’informations, consultez le AWS Systems Manager guide de l’utilisateur.

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 instances Amazon EC2 à l’aide de Systems Manager, il prend les mesures 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 plus d’informations, consultez Surveillance de l’état de réussite ou d’échec des tentatives de Montage.
- Pour les instances EC2 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`).

Gestionnaire de systèmes Systèmes d’exploitation pris en charge par le distributeur

Vos instances EC2 doivent exécuter l’un des systèmes d’exploitation suivants pour pouvoir être utilisées pour mettre à jour AWS Systems Manager 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 2 (AL2)	2.0	x86_64, arm64 (Amazon Linux 2, types d’instances A1)
Amazon Linux (AL1)	2017,09, 2018,03	x86_64

Plateforme	Version de plateforme	Architecture
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)
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)

Comment utiliser AWS Systems Manager pour installer ou mettre à jour automatiquement amazon-efs-utils

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. Configurer 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 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 instances Amazon EC2. Pour de plus amples informations, veuillez consulter Étape 4 : Créer un profil d'instance IAM pour Gestionnaire des systèmes.

Étape 2 : Configuration d'une association utilisée par State Manager pour installer ou mettre à jour le client Amazon EFS

Le package `amazon-efs-utils` est inclus dans Distributor et est prêt à être déployé sur des instances EC2 gérées. Pour voir la dernière version disponible pour l'installation, vous pouvez utiliser la AWS Systems Manager console ou votre outil de ligne de AWS commande préféré. `amazon-efs-utils` Pour accéder à Distributor, ouvrez le site https://console.aws.amazon.com/systems-manager/ et sélectionnez Distributor dans le panneau de navigation de gauche. Localisez AmazonEFSUtils dans la section Owned by Amazon. Choisissez AmazonEFSUtils pour voir les détails du package. Pour plus d'informations, consultez Voir package.

À l'aide de State Manager, vous pouvez installer ou mettre à jour le package `amazon-efs-utils` sur vos instances EC2 gérées immédiatement ou selon un calendrier. De plus, vous pouvez vous assurer que `amazon-efs-utils` automatiquement installé sur les nouvelles instances EC2. 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 instances EC2 nouvelles et existantes en tant que cibles afin d'installer ou de mettre à jour automatiquement AmazonEFSUtils. 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 instances EC2 avec les 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 AmazonEFSUtils 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 plusieurs systèmes de fichiers Amazon EFS sur plusieurs instances EC2, consultezMontage d'EFS sur plusieurs instances EC2 à l'aide de AWS Systems Manager.

Installation manuelle du client Amazon EFS

Vous pouvez installer manuellement le client Amazon EFS sur vos instances Linux Amazon EC2 exécutant Amazon Linux 2023 (AL2023), Amazon Linux 2 (AL2), Amazon Linux (AL1), d'autres distributions Linux prises en charge, ainsi que sur des instances Mac EC2 exécutant macOS Big Sur, macOS Monterey et macOS Ventura.

Les procédures d'installation de ces systèmes d'exploitation sont décrites dans les sections suivantes. Pour obtenir des instructions sur l'installation et la mise à jour du client Amazon EFS, consultez la section Installation dans le `amazon-efs-utils` fichier README sur Github.

Rubriques

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

Installation du client Amazon EFS sur les instances Linux Amazon EC2

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

- Les référentiels de packages Amazon machine image (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 dépôt AWS efs-utils GitHub . Pour plus d'informations sur l'installation `amazon-efs-utils` du package depuis GitHub, consultezPour installer le client Amazon EFS sur d'autres distributions Linux.

> **Note**
>
> - Si vous utilisez AWS Direct Connect, vous trouverez les instructions d'installation dansProcédure : Créer et monter un système de fichiers sur site avec AWS Direct Connect et VPN.
> - L'AMI Amazon Linux (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 Linux Amazon EC2

1. Assurez-vous d'avoir créé une instance EC2 AL2023, Amazon Linux 2 (AL2) ou Amazon Linux (AL1). 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 sur la procédure à suivre, voir Se connecter à votre instance Linux depuis Linux ou macOS à l'aide de SSH.
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 Amazon Linux 2023 (AL2023), Amazon Linux 2 (AL2), Amazon Linux (AL1), 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 Mac EC2 exécutant macOS Big Sur, macOS Monterey ou macOS Ventura

Le package `amazon-efs-utils` peut être installé sur des instances Mac EC2 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 l'installation `amazon-efs-utils` sur votre instance EC2, 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 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 surveiller le succès ou l'échec des tentatives de montage de vos systèmes de fichiers Amazon EFS dans CloudWatch Logs. Pour plus d'informations, consultez Surveillance de l'état de réussite ou d'échec des tentatives de Montage.

Pour obtenir des instructions sur l'installation et la mise à niveau`botocore`, consultez la section Installation `botocore` dans le `amazon-efs-utils` fichier README sur Github.

Mise à niveau d'**`stunnel`**

Le chiffrement des données en transit avec l'aide au montage Amazon EFS nécessite la version 0penSSL 1.0.2 ou une plus récente, et une version de `stunnel` qui prend en charge du protocole OCSP (Online Certificate Status Protocol) et de la vérification du nom d'hôte du certificat. L'assistant de montage utilise le programme `stunnel` pour sa fonctionnalité 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 de Linux, le montage d'un système de fichiers Amazon EFS à l'aide de TLS échoue.

Après avoir installé l'assistant de montage Amazon EFS, vous pouvez mettre à niveau la version de stunnel de votre système en suivant les instructions ci-après :

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. Remplacez *`latest-stunnel-version`* 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 Mac EC2 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 exécutant 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.

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. Dans le cadre du service, EFS surveille en permanence le statut du certificat et émet de nouveaux certificats pour remplacer les certificats révoqués qu'il détecte.

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. Si un certificat TLS EFS est révoqué, Amazon publie un bulletin de sécurité et met à disposition 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
```

Montage des systèmes de fichiers EFS

Dans les sections suivantes, vous apprendrez à Monter votre système de fichiers Amazon EFS avec l'assistant au Montage Amazon EFS. De plus, vous apprendrez à remonter automatiquement votre système de fichiers après tout redémarrage du système à l'aide du fichier `fstab`. À l'aide de l'assistant de Montage EFS, vous disposez des options suivantes pour Monter votre système de fichiers Amazon EFS :

- Montage sur des instances EC2 prises en charge
- Montage avec autorisation IAM
- Montage avec points d'accès Amazon EFS
- Montage avec un client Linux sur site
- Montage automatique des systèmes de fichiers EFS lors du redémarrage d'une instance EC2
- Montage d'un système de fichiers lors de la création d'une nouvelle instance EC2

> **Note**
>
> Amazon EFS ne prend pas en charge le Montage à partir d'instances Windows Amazon EC2.

L'assistant de Montage EFS fait partie du package `amazon-efs-utils`. Le package `amazon-efs-utils` est une collection d'outils Amazon EFS. Pour de plus amples informations, veuillez consulter Installation manuelle du client Amazon EFS.

Lorsque l'assistant de Montage Amazon EFS n'était pas disponible, nous recommandions de Monter vos systèmes de fichiers Amazon EFS à l'aide du client NFS Linux standard. Pour de plus amples informations, veuillez consulter Utilisation du système de fichiers réseau pour monter des systèmes de fichiers EFS.

Rubriques

- Utilisation de l'assistant de Montage EFS pour Monter les systèmes de fichiers EFS
- Utilisation du système de fichiers réseau pour monter des systèmes de fichiers EFS
- Considérations de Montage supplémentaires
- Résolution des problèmes de montage

Utilisation de l’assistant de Montage EFS pour Monter les systèmes de fichiers EFS

L’assistant de Montage EFS vous aide à Monter vos systèmes de fichiers EFS sur vos instances EC2 Linux et Mac exécutant les distributions prises en charge répertoriées dans À propos du client Amazon EFS.

L’assistant de Montage Amazon EFS simplifie le Montage de vos systèmes de fichiers. Il inclut les options de Montage Amazon EFS recommandées par défaut. En outre, l’assistant de Montage intègre un système de journalisation à des fins de dépannage. Si vous rencontrez un problème avec votre système de fichiers Amazon EFS, vous pouvez partager ces journaux avec le AWS Support. Pour plus d’informations sur le Montage de votre système de fichiers, consultez Montage des systèmes de fichiers EFS.

> **Note**
>
> Amazon EFS ne prend pas en charge le Montage à partir d’instances Windows Amazon EC2.

Rubriques

- Comment ça marche
- Obtention de journaux de support
- Conditions préalables à l’utilisation de l’assistant de Montage EFS
- Montage sur des instances Linux Amazon EC2 à l’aide de l’assistant de Montage EFS
- Montage sur des instances Mac Amazon EC2 à l’aide de l’assistant de Montage EFS
- Montage de systèmes de fichiers Amazon 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 avec des clients Linux sur site à l'aide de l'assistant de montage EFS et du VPN AWS Direct Connect
- Montage automatique de votre système de fichiers EFS Amazon
- Montage d'EFS sur plusieurs instances EC2 à l'aide de AWS Systems Manager
- Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC

Comment ça marche

L'assistant de Montage définit un nouveau type de système de fichiers réseau, appelé `efs`, qui est entièrement compatiole avec la commande standard `mount` dans Linux. L'assistant de Montage prend également en charge le Montage automatique d'un système de fichiers au Moment du démarrage d'instance en utilisant des entrées dans le fichier de configuration`/etc/fstab`.

> **Warning**
>
> Utilisez l'option `_netdev`, utilisée pour identifier les systèmes de fichiers réseau lors du Montage automatique de votre système de fichiers. Si l'option `_netdev` est manquante, votre instance EC2 peut cesser 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 en tant qu'option de Montage pour votre système de fichiers `stunnel`, l'assistant de Montage initialise un processus client et un processus superviseur 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 compatiole, 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.

Options de Montage utilisées par le client Amazon 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 Linux EC2

  `nfsvers=4.0`— utilisé lors du Montage sur des instances Mac EC2 compatioles 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.
- `wsize=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 Mac EC2 exécutant macOS Big Sur, Monterey et Ventura.

Obtention de journaux de support

L'aide au Montage intègre la journalisation pour votre système de fichiers Amazon 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 processus `amazon-efs-mount-watchdog` garantit que chaque processus stunnel de Montage est en cours d'exécution et arrête le stunnel lorsque le système de fichiers 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 utiliser un système de fichiers Amazon EFS sur une instance Amazon EC2 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 Amazon EFS – Vous créez les 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 instance EC2, vous encourez des frais EC2 standard pour les données envoyées entre 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 Zone unique situé dans une Zone de disponibilité différente de celle de l'instance EC2.
  - 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 instance Amazon EC2 utilisant l'une des distributions Linux ou macOS prises en charge - Les distributions prises en charge pour le Montage de votre système de fichiers à l'aide de 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**
>
> Les instances Mac EC2 exécutant macOS Big Sur ne prennent en charge que NFS 4.0.

- L'assistant de Montage Amazon EFS est installé sur l'instance EC2. L'assistant de Montage est un outil inclus dans le package `amazon-efs-utils` d'utilitaires. Pour plus d'informations sur l'installation de `amazon-efs-utils`, consultez Installation automatisée du client EFS et Installation manuelle `amazon-efs-utils`.
- L'instance EC2 est dans un VPC – L'instance EC2 connectée doit être 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 Jeux d'options DHCP dans le Guide de l'utilisateur Amazon VPC.
- Le VPC a des noms d'hôtes DNS activés – Le VPC de l'instance EC2 connectée doit avoir des noms d'hôtes DNS activés. Pour plus d'informations, consultez Affichage des noms d'hôte DNS pour votre instance EC2 dans le Guide l'utilisateur Amazon VPC.
- Pour les instances EC2 et les systèmes de fichiers différents Régions AWS : si l'instance EC2 et le système de fichiers que vous montez sont situés dans des Régions AWS emplacements différents, vous devrez modifier la `region` propriété dans le `efs-utils.conf` fichier. Pour plus d'informations, consultez Montage de systèmes de fichiers Amazon EFS à partir d'un autre Région AWS.

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

Ce processus nécessite les éléments suivants :

- Vous avez installé le package `amazon-efs-utils` sur l'instance EC2. 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 Amazon EFS à l'aide de l'assistant de Montage sur les instances Linux EC2

1. Ouvrez une fenêtre de terminal sur votre instance EC2 via Secure Shell (SSH), et connectez-vous avec le nom d'utilisateur approprié. Pour plus d'informations, voir Se connecter à votre instance Linux depuis Linux ou macOS à l'aide de SSH.
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'instance EC2 et le système de fichiers que vous Montez se trouvent dans des emplacements différents Région AWS, reportez-vous à Montage de systèmes de fichiers Amazon EFS à partir d'un autre Région AWS pour Modifier la propriété`region` dans le fichier `efs-utils.conf`.

   - 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 Montez *`file-system-id`* et `efs` à la place de *`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 Mac Amazon EC2 à l'aide de l'assistant de Montage EFS

Ce processus nécessite les éléments suivants :

- Vous avez installé le package `amazon-efs-utils` sur l'instance Mac EC2. Pour de plus amples informations, veuillez consulter Installation du client Amazon EFS sur des instances Mac EC2 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 Mac EC2 exécutant macOS Big Sur, Monterey ou Ventura. Les autres versions de macOS ne sont pas prises en charge.

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

Pour Monter votre système de fichiers Amazon EFS à l'aide de l'assistant de Montage EFS sur des instances Mac EC2 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 Se connecter à votre instance à l'aide de SSH pour les instances Mac, dans le guide de l'utilisateur Amazon EC2.
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 Mac EC2, que vous utilisiez ou non l'option `tls` 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 Mac EC2 sans utiliser le chiffrement en transit, utilisez l'option `notls`, 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 Amazon EFS à partir d'un autre Région AWS

Si vous montez votre système de fichiers EFS à partir d'une instance Amazon EC2 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 propriété de la région dans **`efs-utils.conf`**

1. Accédez au terminal pour votre instance EC2 via Secure Shell (SSH) et connectez-vous avec le nom d'utilisateur approprié. Pour plus d'informations sur la manière de procéder, consultez la section Connexion à votre instance Linux à l'aide de SSH dans le guide de l'utilisateur Amazon EC2.
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 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 Amazon EFS Zone unique 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 calcul Amazon EC2 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 avez installé `amazon-efs-utils package` sur l'instance EC2. Pour de plus amples informations, veuillez consulter Installation manuelle 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 Zone unique sur EC2 dans une autre Zone de disponibilité

Si vous Montez un système de fichiers Zone unique sur une instance EC2 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 utilisez `/etc/fstab` pour Monter un système de fichiers Zone unique EFS sur une instance EC2 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'entrée `/etc/fstab`.

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

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

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 instance EC2 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,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0
```

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

Pour plus d'informations sur la façon de Modifier le fichier `/etc/fstab` et sur les valeurs utilisées dans cette commande, consultez Utilisation de NFS pour Monter automatiquement les 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 le système de fichiers Amazon EFS avec Amazon ECS pour partager des données du système de fichiers dans l'ensemble de votre flotte d'instances de conteneur afin que vos tâches aient accès au même stockage persistant, quelle que soit l'instance sur laquelle elles atterrissent. Pour utiliser les systèmes de fichiers Amazon EFS Zone unique 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 Zone unique à partir d'Amazon EKS, vous pouvez utiliser le pilote Amazon EFS Container Storage Interface (CSI), qui prend en charge les points d'accès Amazon 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 Amazon EFS Zone unique,

vous pouvez utiliser cette option `nodeSelector` 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 Amazon 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 Amazon EFS sur des instances Linux à l'aide de l'autorisation AWS Identity and Access Management (IAM), vous devez utiliser l'assistant de montage EFS. Pour plus d'informations sur l'utilisation d'une autorisation IAM pour les clients NFS, consultez Utilisation d'IAM pour contrôler l'accès aux données du système de fichiers.

Vous devrez 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'instance EC2

Si vous procédez à un Montage avec autorisation IAM d'une instance Amazon EC2 avec un profil d'instance, utilisez les options de Montage `tls` et `iam` présentées ci-dessous.

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

Pour procéder automatiquement à un Montage avec autorisation IAM sur une instance ayant un profil d'instance, ajoutez la ligne suivante au fichier `/etc/fstab` sur l'instance EC2.

```
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 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` sur l'instance EC2.

```
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
```

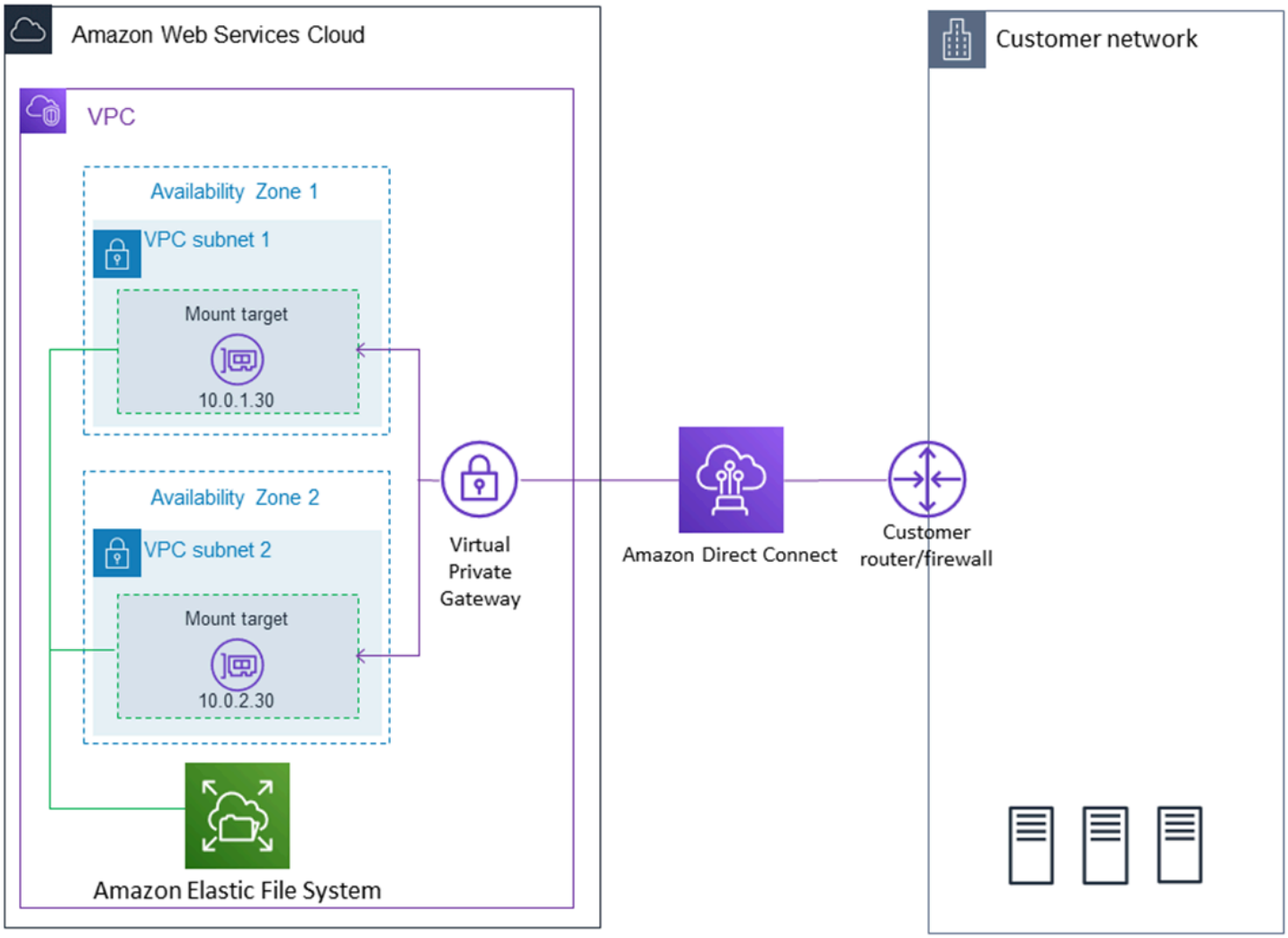
Pour procéder automatiquement au Montage d'un système de fichiers à l'aide d'un point d'accès, ajoutez la ligne suivante au fichier `/etc/fstab` sur l'instance EC2.

```
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 Amazon EFS.

Montage avec des clients Linux sur site à l'aide de l'assistant de montage EFS et du VPN AWS Direct Connect

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.



Pour plus d'informations sur l'utilisation `amazon-efs-utils` d'un AWS Direct Connect VPN pour monter des systèmes de fichiers Amazon EFS sur des clients Linux locaux, consultezProcédure : Créer et monter un système de fichiers sur site avec AWS Direct Connect et VPN.

Montage automatique de votre système de fichiers EFS Amazon

Vous pouvez configurer une instance Amazon EC2 pour Monter automatiquement un système de fichiers EFS lorsqu'il redémarre à l'aide de l'assistant de Montage EFS ou de NFS.

- Utilisation de l'assistant de Montage EFS
  - Attachez un système de fichiers EFS lorsque vous créez une nouvelle instance EC2 Linux à l'aide de l'assistant de lancement d'instance EC2.
  - En mettant à jour le fichier EC2 `/etc/fstab` afin d'y insérer une entrée pour le système de fichiers EFS.
- Utilisation de NFS sans l'assistant de Montage EFS pour mettre à jour le fichier `/etc/fstab` EC2, afin de prendre en charge les instances EC2 Linux et Mac.

> **Note**
>
> L'assistant de Montage EFS ne prend pas en charge le Montage automatique sur les instances Mac Amazon EC2 exécutant macOS Big Sur ou Monterey. Vous pouvez plutôt utiliser NFS pour configurer le fichier /etc/fstab sur une instance Mac EC2 afin de Monter automatiquement un système de fichiers EFS.

Rubriques

- Utilisation de l'assistant de Montage EFS pour remonter automatiquement les systèmes de fichiers EFS
- Utilisation de NFS pour Monter automatiquement les systèmes de fichiers EFS

Utilisation de l'assistant de Montage EFS pour remonter automatiquement les systèmes de fichiers EFS

Utilisez l'assistant de Montage EFS pour configurer `/etc/fstab` sur les instances Linux EC2 afin de remonter automatiquement vos systèmes de fichiers EFS au redémarrage de l'instance.

Rubriques

- Attachez un système de fichiers EFS lors de la création d'une instance EC2 pour activer le Montage automatique au redémarrage
- Utilisation de /etc/fstab avec l'assistant de Montage EFS pour remonter automatiquement les systèmes de fichiers EFS

Attachez un système de fichiers EFS lors de la création d'une instance EC2 pour activer le Montage automatique au redémarrage

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`.

Lorsque vous créez une instance Linux Amazon EC2 à l'aide de l'assistant de lancement d'instance EC2, vous pouvez la configurer de sorte qu'elle Monte automatiquement votre système de fichiers Amazon EFS. L'instance EC2 Monte automatiquement le système de fichiers lors du premier lancement de l'instance et chaque fois qu'elle redémarre.

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

Avant d'effectuer cette procédure, assurez-vous d'avoir créé votre système de fichiers Amazon EFS. Pour plus d'informations, consultez Création rapide d'un système de fichiers doté de paramètres recommandés (console) dans l'exercice de mise en route d'Amazon EFS.

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

Avant de lancer une instance d'Amazon EC2 et de vous y connecter, vous devez créer une paire de clés, sauf si vous avez déjà une. Suivez les étapes décrites dans Configuration pour utiliser Amazon

EC2 dans le guide de l'utilisateur Amazon EC2 pour créer une paire de clés. Si vous disposez déjà d'une paire de clés, vous pouvez l'utiliser pour cet exercice.

Pour configurer votre instance EC2 pour Monter un système de fichiers EFS automatiquement au lancement

1. Ouvrez la console Amazon EC2 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 affiché en regard de l'ID du système de fichiers correspond au point de Montage que l'instance EC2 utilisera, et vous pouvez le 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 instance EC2 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 instance EC2 est maintenant configurée pour Monter le système de fichiers EFS lors du lancement et à chaque redémarrage.

Utilisation de **`/etc/fstab`** avec l'assistant de Montage EFS pour remonter automatiquement les systèmes de fichiers EFS

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 Linux EC2 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 Amazon EFS ne prennent pas en charge le Montage automatique utilisant `/etc/fstab` avec l'assistant de Montage EFS sur les instances Mac Amazon EC2 exécutant macOS Big Sur ou Monterey. Au lieu de cela, vous pouvez utiliser NFS avec `/etc/fstab` pour Monter automatiquement votre système de fichiers sur des instances Mac EC2 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 outils `amazon-efs-utils` peuvent être installés sur les AMI (Amazon Machine Images) Amazon Linux et Amazon Linux 2. Pour plus d'informations sur `amazon-efs-utils`, consultez Installation des outils 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 Amazon EFS que vous souhaitez remonter automatiquement. Pour de plus amples informations, veuillez consulter Création rapide d'un système de fichiers doté de paramètres recommandés (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 Linux EC2. Pour de plus amples informations, veuillez consulter Installation des outils Amazon EFS.

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

1. Connectez-vous à votre instance EC2 :

   - Pour vous connecter à votre instance à partir d'un ordinateur exécutant macOS ou Linux, spécifiez le fichier .pem dans votre commande SSH. Pour ce faire, utilisez l'option `-i` et le chemin d'accès à votre clé privée.
   - Pour vous connecter à votre instance depuis un ordinateur exécutant Windows, vous pouvez utiliser l'un MindTerm ou l'autre des systèmes PuTTY. Pour utiliser PuTTY, installez-le et convertissez le fichier .pem en fichier .ppk.

   Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur Amazon EC2 :

   - Connectez-vous à votre instance Linux depuis Windows avec PuTTY

- Connectez-vous à votre instance Linux depuis Linux ou macOS à l'aide de SSH

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 procéder automatiquement à un Montage avec autorisation IAM sur une instance Amazon EC2 ayant un profil d'instance, ajoutez la ligne suivante au fichier `/etc/fstab`.

     ```
     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,iam,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 l'option `_netdev` est manquante, votre instance EC2 peut cesser 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.

5. Testez l'entrée `fstab` en utilisant la commande `mount` avec l'option `'fake'` ainsi que les options `'all'` et `'verbose'`.

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

Votre instance EC2 est maintenant configurée pour le Montage du système de fichiers EFS à chaque redémarrage.

> **Note**
>
> Il peut arriver que votre instance Amazon EC2 doive démarrer quel que soit l'état de votre système de fichiers Amazon 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
`file-system-id` `:/`	ID de votre système de fichiers Amazon EFS. Vous pouvez obtenir cet ID depuis la console ou par programmation à partir de la CLI ou d'un AWS SDK.
`efs-mount-point`	Point de Montage du système de fichiers EFS sur votre instance EC2.
`efs`	Type de système de fichiers. Lorsque vous utilisez l'assistant de Montage, ce type est toujours `efs`.
`mount options`	Options de Montage pour le système de fichiers. Il s'agit d'une liste séparée par des virgules des options suivantes : • `_netdev` – 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.

Champ	Description
	• `noresvport` – 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. • `tls` – Cette option active le chiffrement des données en transit. • `iam` – Utilisez cette option pour procéder à un Montage avec autorisation IAM sur un Amazon EC2 ayant un profil d'instance. L'utilisation de l'option de Montage `iam` nécessite également l'utilisation de l'option `tls`. Pour de plus amples informations, veuillez consulter Utilisation d'IAM pour contrôler l'accès aux données du système de fichiers. • `awsprofile=` *`namedprofile`* – Utilisez cette option avec les options `iam` et `tls` 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 d'IAM pour contrôler l'accès aux données du système de fichiers. • `accesspoint=` *`access-point-id`* – Utilisez cette option avec l'option `tls` 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 Amazon EFS.
`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 `fsck` vérifie les systèmes de fichiers au démarrage. Pour les systèmes de fichiers EFS, cette valeur doit être `0` pour indiquer que `fsck` ne doit pas s'exécuter au démarrage.

Utilisation de NFS pour Monter automatiquement les systèmes de fichiers EFS

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

1. Connectez-vous à votre instance EC2 :

   - Pour vous connecter à votre instance à partir d'un ordinateur exécutant macOS ou Linux, spécifiez le fichier .pem dans votre commande SSH. Pour ce faire, utilisez l'option `-i` et le chemin d'accès à votre clé privée.
   - Pour vous connecter à votre instance depuis un ordinateur exécutant Windows, vous pouvez utiliser l'un MindTerm ou l'autre des systèmes PuTTY. Pour utiliser PuTTY, installez-le et convertissez le fichier .pem en fichier .ppk.

   Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur Amazon EC2 :

   - Connectez-vous à votre instance Linux depuis Windows avec PuTTY
   - Connectez-vous à votre instance Linux depuis Linux ou macOS à l'aide de SSH
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`.

   - Remplacez *`file_system_id par l'ID`* du système de fichiers que vous Montez.
   - Remplacez *`aws-region`* par celui dans lequel se Région AWS trouve le système de fichiers, tel que. `us-east-1`
   - Remplacez Mo*`unt_point par le point`* de Montage du système de fichiers.

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

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

Champ	Description
file-system-id :/	ID de votre système de fichiers Amazon EFS. Vous pouvez obtenir cet ID depuis la console ou par programmation à partir de la CLI ou d'un AWS SDK.
efs-mount-point	Point de Montage du système de fichiers EFS sur votre instance EC2.
nfs4	Spécifie le type de système de fichiers.
mount options	Liste séparée par des virgules d'options de Montage pour le système de fichiers : • nfsvers=4.1 — spécifie l'utilisation de NFS v4.1. • rsize=1048576 — 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. 1048576est la plus grande taille possible. • wsize=1048576 — 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'écritur e de données dans un fichier d'un système de fichiers EFS. 1048576est la plus grande taille possible. • 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 décisecon des (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 sur 600 décisecondes (60 secondes). Si vous devez Modifier le paramètre de délai (timeo), nous vous

Champ	Description
	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) 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` – 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 `dump` ; `0` indique à l'utilitaire `dump` de ne pas sauvegarder le système de fichiers.
`0`	Indique à l'utilitaire `fsck` de ne pas s'exécuter au démarrage.

Montage d'EFS sur plusieurs instances EC2 à l'aide de AWS Systems Manager

Vous pouvez monter des systèmes de fichiers EFS sur plusieurs instances Amazon EC2 à distance et en toute sécurité sans avoir à vous connecter aux instances à l'aide de la AWS Systems Manager Run commande. Pour plus d'informations sur AWS Systems Manager Run Command, voir AWS Systems Manager Exécuter la commande 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 instances EC2 sont lancées avec un profil d'instance qui inclut la politique d'autorisation `AmazonElasticFileSystemsUtils`. Pour plus d'informations, consultez 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 instances EC2. Vous pouvez utiliser AWS Systems Manager pour installer automatiquement le package sur vos instances. Pour plus d'informations, consultez Étape 2 : Configuration d'une association utilisée par State Manager pour installer ou mettre à jour le client Amazon EFS.

Pour Monter plusieurs systèmes de fichiers EFS sur plusieurs instances EC2 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- RunShell Script.
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 Linux Amazon EC2 à l’aide de l’assistant de Montage EFS ou Montage sur des instances Mac Amazon EC2 à l’aide de l’assistant de Montage EFS.
7. Sélectionnez les instances EC2 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 Amazon EFS avec une 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.

Montage à l'aide d'IAM ou des points d'accès à partir d'un autre VPC

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

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 des outils 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 l'`elasticfilesystem:DescribeMountTarget`action 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"},
            "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 de VPC ou une passerelle de transit pour connecter les VPC, les instances Amazon EC2 dans un VPC peuvent accéder aux systèmes de fichiers EFS d'un autre VPC, même si les VPC appartiennent à des comptes différents.

  Une passerelle de transit est un hub de transit de réseau que vous pouvez utiliser pour relier votre VPC et vos réseaux 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 de VPC est une connexion de mise en réseau entre deux VPC. Ce type de connexion permet d'acheminer le trafic entre ces derniers à l'aide d'adresses IPv4 (Internet Protocol version 4) ou IPv6 (Internet Protocol version 6) privées. Vous pouvez utiliser le peering VPC pour connecter des VPC au sein d'un même Région AWS ou entre eux. Région 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 instance EC2 :

- Pour vous connecter à votre instance à partir d'un ordinateur exécutant macOS ou Linux, spécifiez le fichier .pem dans votre commande SSH. Pour ce faire, utilisez l'option `-i` et le chemin d'accès à votre clé privée.
- Pour vous connecter à votre instance depuis un ordinateur exécutant Windows, vous pouvez utiliser l'un MindTerm ou l'autre des systèmes PuTTY. Pour utiliser PuTTY, installez-le et convertissez le fichier .pem en fichier .ppk.

Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur Amazon EC2 :

- Connectez-vous à votre instance Linux depuis Windows avec PuTTY
- Connectez-vous à votre instance Linux depuis Linux ou macOS à l'aide de SSH

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 d'IAM pour contrôler l'accès aux données du système 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 Amazon EFS.

Montage de systèmes de fichiers Amazon 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`.

Montage depuis un autre Compte AWS dans le même VPC

À l'aide de VPC partagés, vous pouvez monter un système de fichiers Amazon EFS appartenant à l'un Compte AWS d'entre eux à partir d'instances Amazon EC2 appartenant à un autre. Compte AWS Pour plus d’informations sur la configuration d’un VPC partagé, consultez Travailler avec des VPC partagés dans le Guide d’appairage Amazon VPC.

Une fois que vous avez configuré le partage de VPC, les instances EC2 peuvent Monter le système de fichiers EFS en utilisant la résolution de nom système de nom de domaine (DNS) ou l’assistant de Montage EFS. Nous vous recommandons d’utiliser l’assistant de Montage EFS pour Monter vos systèmes de fichiers EFS.

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

> **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 plus d’informations, consultez Installation des outils Amazon EFS.

Dans la section suivante, vous pouvez apprendre à installer le client NFS (Network File System) et à monter votre système de fichiers Amazon EFS sur une instance d’Amazon EC2. 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**
>
> Avant de monter un système de fichiers, vous devez créer, configurer et lancer vos ressources AWS associées. Pour obtenir des instructions complètes, veuillez consulter Débuter avec Amazon Elastic File System Amazon Elastic File System.

> **Note**
>
> Avant de monter votre système de fichiers, vous devez créer des groupes de sécurité VPC pour vos instances Amazon EC2 et des cibles de montage avec l'accès entrant et sortant requis. Pour plus d'informations, consultez Utilisation de groupes de sécurité VPC pour les instances Amazon EC2 et les cibles de montage.

Rubriques

- NFS Support
- Installation du client NFS
- Options de montage NFS recommandées
- Montage sur Amazon EC2 avec un nom DNS
- Montage avec une adresse IP

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 les instances d'Amazon EC2. Bien que NFSv4.0 soit pris en charge, nous vous recommandons d'utiliser NFSv4.1. Le montage de votre système de fichiers Amazon EFS sur votre instance d'Amazon EC2 nécessite également un client NFS qui prend en charge le protocole NFSv4 que vous avez choisi. Les instances Mac Amazon EC2 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 plus d'informations, consultez 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.

> **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.

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

Dépannage des versions d’AMI et de noyau

Pour résoudre les problèmes liés à certaines versions d’AMI ou de noyau lors de l’utilisation d’Amazon EFS à partir d’une instance EC2, consultez Résolution des problèmes d’AMI et de noyau.

Installation du client NFS

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

Pour vous connecter à votre instance EC2 et installer le client NFS

1. Connectez-vous à votre instance EC2. Tenez compte des éléments suivants pour la connexion à l’instance :

   - Pour vous connecter à votre instance à partir d’un ordinateur exécutant macOS ou Linux, spécifiez le fichier .pem associé au client SSH avec l’option `-i` et le chemin d’accès à la clé privée.
   - Pour vous connecter à votre instance depuis un ordinateur exécutant Windows, vous pouvez utiliser l'un MindTerm ou l'autre des systèmes PuTTY. Si vous prévoyez d’utiliser PuTTY, vous devez l’installer et exécuter la procédure suivante pour convertir le fichier .pem en fichier .ppk.

   Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur Amazon EC2 :

   - Connexion à votre instance Linux à partir de Windows à l’aide de PuTTY
   - Connexion à votre instance Linux à l’aide de SSH

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

   ```
   $ sudo yum -y update
   $  sudo reboot
   ```
3. Une fois le redémarrage effectué, reconnectez-vous à votre instance EC2.

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 AMI Amazon EC2 Ubuntu, installez le client NFS avec 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 (autrement dit, si vous créez une AMI personnalisée), vous devez inclure, au minimum, le module de noyau client NFSv4.1 et l'assistant de montage d'espace utilisateur NFS4 approprié.

> **Note**
>
> Si vous choisissez Amazon Linux AMI 2016.03.0 ou Amazon Linux AMI 2016.09.0 lors du lancement de votre instance Amazon EC2, vous n'aurez pas besoin d'installer `nfs-utils`, car il est déjà inclus par défaut dans l'AMI.

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 de votre système de fichiers EFS Amazon

Options de montage NFS recommandées

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.

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

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 est résolu en l'adresse IP de la cible du montage Amazon EFS dans la même zone de disponibilité que votre instance Amazon EC2. Si vous utilisez une cible de montage dans une zone de disponibilité différente de celle de votre instance Amazon EC2, vous encourez des frais EC2 standard pour les données envoyées entre 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 descriptions détaillées des valeurs par défaut, consultez les pages `man fstab` et `man nfs` de 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 de la cible de montage qui autorise l'accès NFS entrant depuis le groupe de sécurité EC2. Pour plus d'informations, consultez Utilisation de groupes de sécurité VPC pour les instances Amazon EC2 et les cibles de montage.

- 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 sera automatiquement résolu en l'adresse IP de la cible de montage dans la zone de disponibilité de l'instance Amazon EC2 en cours de connexion. 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 de système de fichiers, vous pouvez monter un système de fichiers sur votre instance Amazon EC2 Linux avec la commande suivante.

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

- 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 de macOS compatible (Big Sur, Monterey, Ventura) avec la commande suivante.

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

> **Important**
>
> Vous devez utiliser `mountport=2049` pour vous connecter correctement au système de fichiers EFS lors du montage sur des instances EC2 Mac 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
```

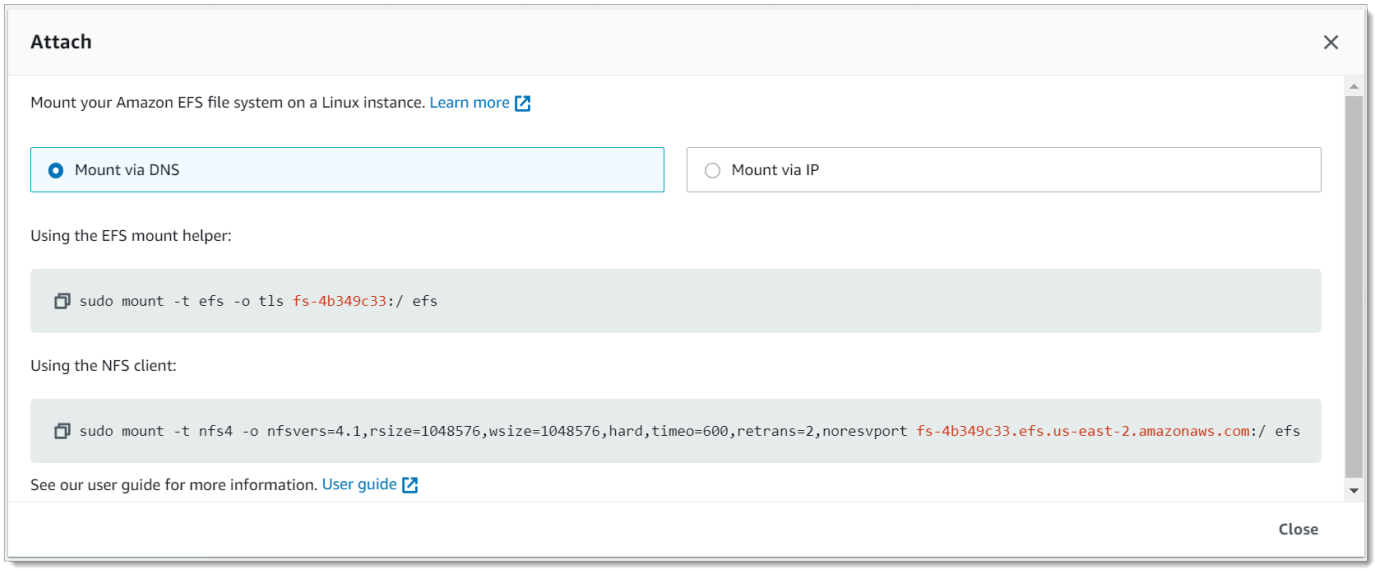
> **Note**
>
> La résolution des noms DNS de la cible de montage dans les zones de disponibilité est prise en charge.

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'instance EC2 de connexion doit être à l'intérieur d'un VPC et elle doit être configurée pour l'utilisation du serveur DNS fourni par Amazon. Pour plus d'informations sur le serveur DNS Amazon, consultez Jeux d'options DHCP dans le Guide de l'utilisateur Amazon VPC.
- La Résolution DNS et les Noms d'hôte DNS doivent être activés pour le VPC de l'instance EC2 en cours de connexion. Pour plus d'informations, consultez Affichage des noms d'hôte DNS pour votre instance EC2 dans le Guide l'utilisateur Amazon VPC.
- L'instance EC2 en cours de connexion doit être 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 Procédure : Créer et monter un système de fichiers sur site avec AWS Direct Connect et VPN et Procédure : montage d'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, vous pouvez utiliser des instances d'Amazon EC2 pour monter un système de fichiers à l'aide de l'adresse IP d'une cible de montage. Le montage par adresse IP fonctionne dans les environnements où DNS est désactivé, comme les VPC avec les noms d'hôte DNS 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

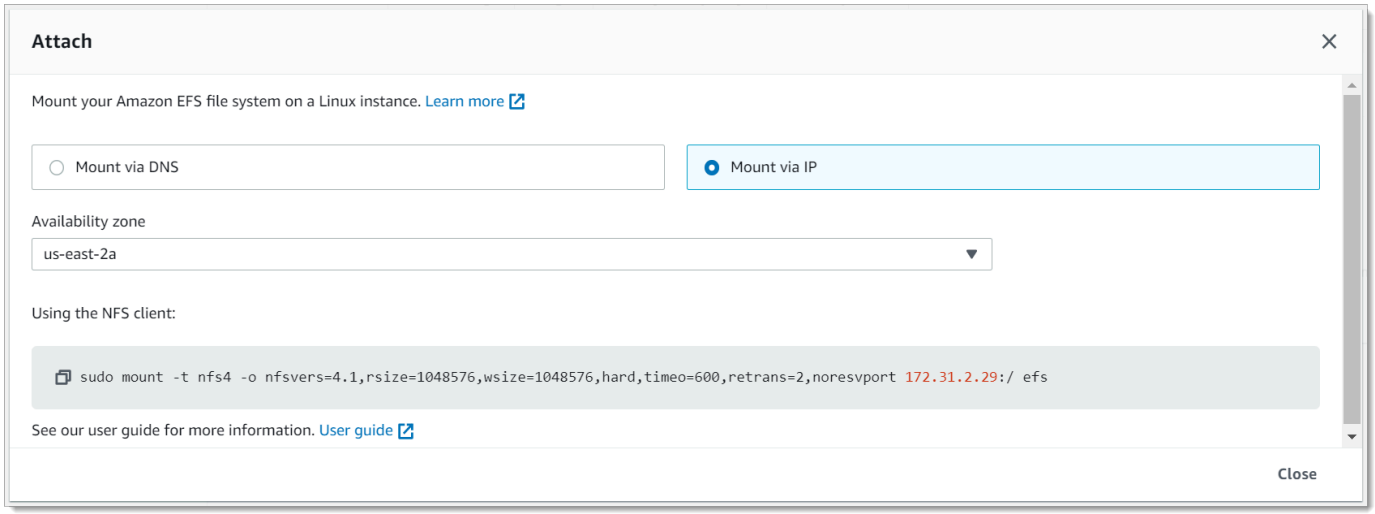
système de fichiers à l'aide de son nom DNS par défaut. Lors de la connexion à l'adresse IP d'une cible de montage, les instances EC2 doivent être montées à l'aide de l'adresse IP de la cible de montage dans la même zone de disponibilité que l'instance de connexion.

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 au groupe de sécurité de la cible de montage qui autorise l'accès NFS entrant depuis le groupe de sécurité EC2. Pour plus d'informations, consultez Utilisation de groupes de sécurité VPC pour les instances Amazon EC2 et les cibles de montage.

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 commande `mount`, vous pouvez monter un système de fichiers sur votre instance Linux Amazon EC2 à l'aide de la commande suivante.

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

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

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

> **Important**
>
> Vous devez utiliser `mountport=2049` pour 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

Considérations de Montage supplémentaires

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.
- `wsize=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 Amazon EFS dans la même Zone de disponibilité que votre instance Amazon EC2 sans appeler de ressources externes. Si vous utilisez une cible de Montage dans une Zone de disponibilité différente de celle de votre instance Amazon EC2, vous encourez des frais EC2 standard pour les données envoyées entre 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 descriptions détaillées des valeurs par défaut, consultez les pages `man fstab` et `man nfs` de la documentation Linux.

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

Démontage des systèmes de fichiers

Avant de supprimer un système de fichiers, il est conseillé de le démonter à partir de chacune des instances Amazon EC2 auxquelles il est connecté. Vous pouvez démonter un système de fichiers sur votre instance Amazon EC2 en exécutant la commande `umount` sur l'instance elle-même. Vous ne pouvez pas démonter un système de fichiers Amazon EFS par AWS CLI le AWS Management Console biais du ou de l'un des AWS SDK. Pour démonter un système de fichiers Amazon EFS connecté à une instance Amazon EC2 exécutant Linux, utilisez la commande `umount` comme suit :

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

Example – Identifier le statut de Montage d'un système de fichiers &EFS; et le démonter

```
$ 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% /
```

Résolution des problèmes de montage

Vous trouverez ci-dessous des informations sur le dépannage des problèmes de montage du système de fichiers pour Amazon EFS.

- Le montage du système de fichiers sur l'instance Windows échoue
- Accès refusé par le serveur
- Le montage automatique échoue et l'instance ne répond pas
- Le montage de plusieurs systèmes de fichiers Amazon EFS dans /etc/fstab échoue
- La commande de montage échoue avec le message d'erreur « type de fs erroné »
- La commande de montage échoue avec le message d'erreur « option de montage incorrecte »
- Le montage avec point d'accès échoue
- Le montage du système de fichiers échoue immédiatement après la création du système de fichiers

- Le montage du système de fichiers se bloque, puis échoue avec une erreur de dépassement de délai d'attente
- Le montage d'un système de fichiers avec NFS à l'aide d'un nom DNS échoue
- Échec du montage d'un système de fichiers avec « nfs ne répond pas »
- L'état de cycle de vie de la cible de montage est bloqué
- L'état du cycle de vie cible du montage indique une erreur
- Le montage ne répond pas
- Le client monté est déconnecté
- Les opérations sur un système de fichiers nouvellement monté renvoient l'erreur « mauvaise gestion de fichier »
- Le démontage d'un système de fichiers échoue

Le montage du système de fichiers sur l'instance Windows échoue

Le montage d'un système de fichiers sur une instance Amazon EFS sous Microsoft Windows échoue.

Action à exécuter

N'utilisez pas Amazon EFS avec les instances EC2 Windows ; cela n'est pas pris 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 tentez de monter le système de fichiers à l'aide d'IAM, assurez-vous d'utiliser l'option `-o iam` dans votre commande mount. 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 d'IAM pour contrôler l'accès aux données du système 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 l'option `_netdev` est manquante, votre instance EC2 peut cesser 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 commande `ExecStart` doit pointer vers le système de fichiers réseau (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 commande `ExecStart` doit pointer vers EFS au lieu de NFS4 pour 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 efs
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 instance Amazon EC2. 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 plus d'informations, consultez 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 Network File System versions 4.0 et 4.1 (NFSv4.1). Pour vérifier si c'est le cas, vous pouvez exécuter la commande suivante :

```
$ grep CONFIG_NFS_V4_1 /boot/config*
```

Si la commande précédente retourne `# CONFIG_NFS_V4_1 is not set`, NFSv4.1 n'est pas pris en charge sur votre distribution Linux. Pour une liste des Amazon Machine Images (AMI) pour Amazon Elastic Compute Cloud (Amazon EC2) qui prennent en charge NFSv4.1, 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 plus d'informations, consultez Utilisation des points d'accès Amazon EFS.

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

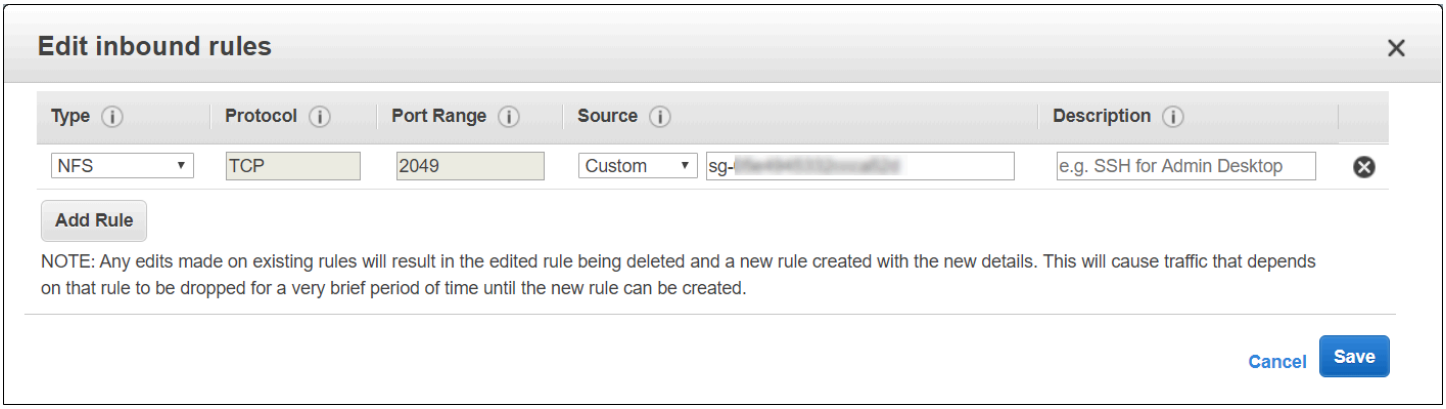
La commande de montage du système de fichiers se bloque pendant une minute ou deux, puis échoue avec une erreur de dépassement de délai d'attente au bout d'une ou deux minutes. Le code suivant en présente un exemple.

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

[2+ minute wait here]
mount.nfs: Connection timed out
$Â
```

Action à exécuter

Cette erreur peut se produire si l'instance Amazon EFS ou les groupes de sécurité de la cible de 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 à partir du groupe de sécurité EC2.



Pour plus d'informations, consultez Création de groupes de sécurité.

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,wsize=1048576,hard,timeo=600,retrans=2,noresvport file-system-id.efs.aws-region.amazonaws.com:/ mnt
mount.nfs: Failed to resolve server file-system-id.efs.aws-region.amazonaws.com:
  Name or service not known.

$
```

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'instance Amazon EC2.
- Assurez-vous qu'il existe une cible de montage dans le même VPC que l'instance Amazon EFS. 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 plus d'informations, consultez Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC.
- Connectez votre instance Amazon EC2 à l'intérieur 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 le VPC Amazon de l'instance Amazon EC2 qui se connecte a activé les noms d'hôte DNS. 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 des outils 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 plus d'informations, consultez Options de montage NFS recommandées.

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 instance Amazon EC2 a été connectée à un système d'un fichier et une cible de montage avec une adresse IP spécifiée, et qu'ensuite ce système de fichiers et cette cible de montage ont été supprimés. Ce problème peut se produire si vous créez un nouveau système de fichiers pour vous connecter à cette instance Amazon EC2 avec la même adresse IP de cible de montage.

Action à exécuter

Vous pouvez résoudre cette erreur en démontant le système de fichiers, puis en le remontant sur l'instance Amazon EFS. 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 Amazon EFS

Vous pouvez utiliser AWS Transfer Family et AWS DataSync transférer des données dans 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, consultezUtilisation AWS DataSync pour transférer des données vers Amazon EFS.

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 vers Amazon EFS.

Rubriques

- Utilisation AWS DataSync pour transférer des données vers Amazon EFS
- Utilisation AWS Transfer Family pour transférer des données vers Amazon EFS

Utilisation AWS DataSync pour transférer des données vers Amazon EFS

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 les serveurs de fichiers NFS (Network File System), SMB (Server Message Block), le stockage d'objets autogéré, les compartiments Amazon AWS Snowcone S3, les systèmes de fichiers Amazon EFS et les systèmes de fichiers FSx for 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 Débuter avec Amazon Elastic File System Amazon Elastic File System et le Guide de l'utilisateur AWS DataSync.

Utilisation AWS Transfer Family pour transférer des données vers Amazon EFS

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 AWS Support.

Rubriques

- Conditions préalables à l'utilisation AWS Transfer Family avec Amazon EFS
- Configuration de votre système de fichiers Amazon EFS pour qu'il fonctionne avec 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 plus d’informations, consultez Blocage de l'accès public aux systèmes de fichiers Amazon EFS.
  - Modifiez la politique du système de fichiers pour activer l’accès intercompte. Pour plus d’informations, consultez Configuration de l’accès intercompte pour Transfer Family.

Configuration de votre système de fichiers Amazon EFS pour qu'il fonctionne avec 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 identifiants POSIX 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 les identifiants POSIX alloués à ces derniers.
- 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 identifiants POSIX alloués aux utilisateurs de Transfer Family. Dans cet exemple, un utilisateur crée un répertoire nommé `transferFam` sous le point de montage 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 instance EC2 Amazon. Amazon EFS prend uniquement en charge le montage par des instances EC2 basées sur Linux.
2. Montez votre système de fichiers EFS s'il n'est pas déjà monté sur l'instance EC2. Pour plus d'informations, consultez 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 Amazon 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 sur les ARN, consultez ARN IAM dans le Guide de l'utilisateur 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",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "elasticfilesystem:ClientRootAccess",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ],
            "Condition": {
                "Bool": {
                    "elasticfilesystem:AccessedViaMountTarget": "true"
```

```
                }
            }
        },
        {
            "Sid": "Grant-cross-account-access",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ]
        }
    ]
}
```

La 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",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "elasticfilesystem:ClientRootAccess",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientMount"
            ],
            "Condition": {
                "Bool": {
                    "elasticfilesystem:AccessedViaMountTarget": "true"
                }
            }
        },
        {
            "Sid": "Grant-cross-account-access",
            "Effect": "Allow",
            "Principal": {
```

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

Gestion des systèmes de fichiers Amazon EFS

Les tâches de gestion des systèmes de fichiers consistent à créer et à supprimer des systèmes de fichiers et à gérer les étiquettes, les sauvegardes des systèmes de fichiers, l'accès et l'accessibilité au réseau avec les cibles de Montage des systèmes de fichiers existants.

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.

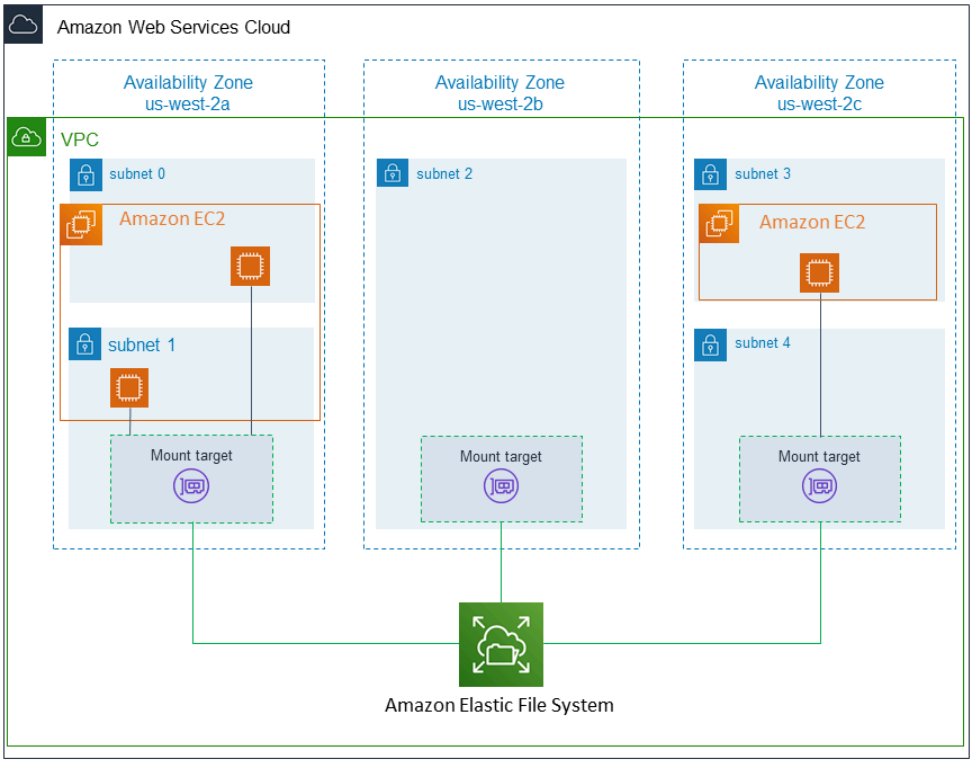
Rubriques

- Gestion de l'accessibilité réseau du système de fichiers
- Gestion du débit du système de fichiers
- Gestion du stockage du système de fichiers
- Gestion de l'accès aux systèmes de fichiers chiffrés
- Mesure : Comment Amazon EFS rapporte les tailles des systèmes de fichiers et des objets
- Gestion des coûts du système de fichiers Amazon EFS à l'aide de AWS Budgets
- État du système de fichiers

Gestion de l'accessibilité réseau du système de fichiers

Vous montez votre système de fichiers sur Amazon EC2 ou sur une autre instance de AWS calcul de votre cloud privé virtuel (VPC) à l'aide d'une cible de montage que vous créez pour le système de fichiers. La gestion de l'accessibilité réseau d'un système de fichiers consiste à gérer les cibles de Montage d'un système de fichiers.

L'illustration suivante Montre comment les instances EC2 d'un VPC accèdent à un système de fichiers Amazon EFS à l'aide d'une cible de Montage.



L'illustration représente trois instances EC2 lancées dans différents sous-réseaux VPC qui accèdent à un système de fichiers Amazon 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 instances EC2 lancées dans l'un de ses sous-réseaux peuvent partager la même cible de Montage.

La gestion des cibles de Montage fait référence aux activités suivantes :

- Création et suppression de cibles de Montage dans un VPC – Vous devez au Moins créer une cible de Montage dans chaque Zone de disponibilité à partir de laquelle vous souhaitez accéder au système de fichiers.
- Mise à jour de la configuration de la cible de Montage – Lorsque vous créez une cible de Montage, vous lui associez des groupes de sécurité. Un groupe de sécurité fonctionne comme un pare-feu virtuel contrôlant le trafic vers et depuis la cible de Montage. Vous pouvez ajouter des règles entrantes pour contrôle l'accès à la cible de Montage et par conséquent au système de fichiers.

Après avoir créé une cible de Montage, vous pouvez si vous le souhaitez Modifier les groupes de sécurité qui lui sont affectés.

Les sections suivantes fournissent des informations sur la gestion de l'accessibilité réseau de votre système de fichiers.

Rubriques

- Création ou suppression de cibles de Montage dans un VPC
- Changement de VPC pour votre cible de Montage
- Mise à jour de la configuration de cible de Montage

Création ou suppression de cibles de Montage dans un VPC

Pour accéder à un système de fichiers Amazon EFS dans un VPC, vous devez avoir des cibles de Montage. Pour un système de fichiers Amazon EFS, les affirmations suivantes s'appliquent :

- Vous pouvez créer une cible de Montage dans chaque Zone de disponibilité.
- 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 instances EC2 de la Zone de disponibilité peuvent partager la cible de Montage unique.

> **Note**
>
> Nous vous recommandons de créer une cible de Montage dans chacune des Zones de disponibilité. Le Montage d'un système de fichiers sur une instance EC2 dans une Zone de disponibilité via une cible de Montage créée dans une autre Zone de disponibilité représente un certain coût. Pour plus d'informations, consultez 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.

Si vous supprimez une cible de Montage, l'opération défait de force 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 plus d'informations, consultez Gérer des cibles de Montage.

> **Note**
>
> Avant de supprimer la cible de Montage d'un système de fichiers, démontez le système de fichiers. Pour plus d'informations, consultez Démontage des systèmes de fichiers.

Vous pouvez utiliser un système de fichiers uniquement dans un VPC à la fois. Autrement dit, vous pouvez créer des cibles de Montage pour le système de fichiers dans un seul VPC à la fois. Si vous souhaitez accéder au système de fichiers à partir d'un autre VPC, vous devez d'abord supprimer les cibles de Montage depuis le VPC actuel. Ensuite, créez des nouvelles cibles de Montage dans un autre VPC.

À l'aide du AWS Management Console, du AWS CLI, et de l'API, vous pouvez créer et gérer des cibles de montage sur des systèmes de fichiers. Pour les cibles de Montage existantes, vous pouvez ajouter et supprimer des groupes de sécurité, ou supprimer la cible de Montage. Pour de plus amples informations, veuillez consulter Gérer des cibles de Montage.

Changement de VPC pour votre cible de Montage

Vous pouvez utiliser un système de fichiers Amazon EFS dans un seul 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 Amazon EFS à partir de ces cibles :

- Instances Amazon EC2 dans le Cloud
- instances EC2 dans un VPC connecté par appairage de 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 de VPC est une connexion de mise en réseau entre deux VPC qui permet de router le trafic entre ces derniers. La connexion peut utiliser des adresses Internet Protocol version 4 (IPv4) privées ou Internet Protocol 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 accéder au système de fichiers depuis les instances EC2 d'un autre VPC, vous devez :

- Supprimer les cibles de Montage actuelles.
- Changer le VPC.
- Créer de nouvelles cibles de Montage

Pour plus d'informations sur l'exécution de ces étapes dans le AWS Management Console, voirPour modifier le VPC d'un système de fichiers Amazon EFS (console).

Utilisation de la CLI

Pour utiliser un système de fichiers dans un autre VPC, vous devez d'abord supprimer toutes les cibles de Montage que vous avez précédemment créées dans un VPC. Ensuite, créez des nouvelles cibles de Montage dans un autre VPC. Pour obtenir des exemple de commandes AWS CLI , consultez Gestion des cibles de montage (CLI).

Mise à jour de la configuration de cible de Montage

Après avoir créé une cible de Montage pour votre système de fichiers, vous pouvez si vous le souhaitez mettre à jour les groupes de sécurité qui sont actifs. Vous ne pouvez pas Modifier l'adresse IP d'une cible de Montage existante. Pour Modifier une adresse IP, supprimez la cible de Montage et créez-en une nouvelle avec la nouvelle adresse. La suppression d'une cible de Montage défait les Montages de système de fichiers existants.

> **Note**
>
> Avant de supprimer la cible de Montage d'un système de fichiers, démontez le système de fichiers.

Chaque cible de Montage a également une adresse IP. Lorsque vous créez une cible de Montage, vous pouvez choisir une adresse IP du sous-réseau dans lequel vous placez la cible de Montage. Si vous omettez une valeur, Amazon EFS sélectionne une adresse IP inutilisée de ce sous-réseau.

Il n'existe aucune opération Amazon EFS pour Modifier l'adresse IP après la création d'une cible de Montage. Par conséquent, vous ne pouvez pas Modifier l'adresse IP par programmation ou à

l’aide de l’ AWS CLI. La console vous permet cependant de Modifier l’adresse IP. En arrière-plan, la console supprime la cible de Montage et la crée de nouveau.

> **Warning**
>
> Si vous Modifiez l’adresse IP d’une cible de Montage, vous défaites les Montages de système de fichiers existants et vous devez remonter le système de fichiers.

Aucune des Modifications de configuration apportées à l’accessibilité réseau du système de fichiers n’a d’incidence sur le système de fichiers lui-même. Votre système de fichiers et vos données restent inchangés.

Modification d’un groupe de sécurité

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 instance EC2 de communiquer avec le système de fichiers.

Pour plus d'informations sur les groupes de sécurité, consultez les groupes de sécurité Amazon EC2 pour les instances Linux dans le guide de l'utilisateur Amazon EC2.

Pour modifier le groupe de sécurité d'une cible de montage, consultezGérer des cibles de Montage.

Gestion du débit du système de fichiers

Elastic est le mode de débit par défaut 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.

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, consultezModes de débit.

> **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 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.

Pour gérer le débit du système de fichiers (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 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.

Pour gérer le débit du système de fichiers (CLI)

- Utilisez la commande update-file-systemCLI ou l'action UpdateFileSystem API pour modifier le mode de débit d'un système de fichiers.

Gestion du stockage du système de fichiers

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 pour 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.

Politiques de cycle de vie

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. 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 depuis IA ou Archive vers le stockage standard, qui fournit des latences de lecture inférieures à la milliseconde pour les données fréquemment consultées. Par défaut, les fichiers ne sont pas replacés dans le stockage standard et restent dans la classe de stockage IA ou Archive. 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 Gestion des politiques de cycle de vie d'un système de fichiers.

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. Une fois que la gestion du cycle de vie a transféré un fichier vers les classes de stockage IA ou Archive, le fichier y reste indéfiniment, sauf si la politique de transition vers la norme est définie, qui demande à la gestion du cycle de vie de replacer les fichiers vers la norme en cas d'accès.

Les opérations sur les métadonnées, par exemple l'affichage du contenu d'un répertoire, ne sont pas comptabilisées comme un 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.

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 les fichiers vers ou depuis le stockage IA et Archive varie en fonction de la taille du fichier et de la charge de travail du système de fichiers.

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. 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.

Gestion des politiques de cycle de vie d'un système de fichiers

Lorsque vous créez un système de fichiers Amazon EFS qui utilise les paramètres recommandés par le service à l'aide du AWS Management Console, les politiques de cycle de vie du système de fichiers utilisent les paramètres par défaut suivants :

- 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.

Pour de plus amples informations sur la création d'un système de fichiers avec des paramètres recommandés par le service, veuillez consulter Création rapide d'un système de fichiers doté de paramètres recommandés (console).

Vous pouvez configurer les politiques de cycle de vie une fois le système de fichiers créé ou lors de la création d'un système de fichiers avec des paramètres personnalisés.

Les valeurs possibles pour les politiques de transition vers IA et de Transition vers Archive sont les suivantes :

- Aucun
- 1 jour depuis le dernier accès
- 7 jours depuis le dernier accès
- 14 jours depuis le dernier accès
- 30 jours depuis le dernier accès
- 60 jours depuis le dernier accès
- 90 jours depuis le dernier accès
- 180 jours depuis le dernier accès
- 270 jours depuis le dernier accès
- 365 jours depuis le dernier accès

Les valeurs possibles pour la politique Transition vers le cycle de vie standard sont les suivantes :

- Aucun
- Au premier accès

Vous pouvez configurer les politiques de cycle de vie à l'aide des AWS Management Console et AWS CLI, comme décrit dans les procédures suivantes.

Gérer des stratégies de cycle de vie sur un système de fichiers existant (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, vous pouvez Modifier les politiques de cycle de vie suivantes :

   - Réglez Transition vers IA sur l’un des paramètres disponibles. Pour arrêter de déplacer des fichiers vers le stockage IA, choisissez Aucun.
   - Définissez Transition vers Archive sur l’un des paramètres 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, définissez ce paramètre sur Aucun.
6. Choisissez Enregistrer les Modifications pour enregistrer vos Modifications.

Gérer les politiques de cycle de vie sur un système de fichiers existant (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
- Utilisation de politiques de clé dans AWS KMS dans le Guide du développeur AWS Key Management Service
- Utilisation d'octrois dans le AWS Key Management Service Guide du 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 `enabled` état pour que les utilisateurs puissent accéder au contenu d'un système de encrypted-at-rest fichiers chiffré à l'aide de cette clé.

Exécution d'actions administratives sur les clés Amazon EFS KMS

Ci-dessous, vous trouverez comment activer, désactiver ou supprimer les clés KMS associées à votre système de fichiers Amazon EFS. Vous pourrez également en savoir plus sur le comportement à attendre de votre système de fichiers lorsque vous effectuez ces actions.

Gestion de l'accès à la clé KMS pour un système de fichiers

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 encrypted-at-rest fichiers.
- Les systèmes de encrypted-at-rest fichiers 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 encrypted-at-rest fichiers continue de fonctionner, mais cesse de fonctionner après un certain temps.

Vous pouvez empêcher l'accès à un système de encrypted-at-rest fichiers monté 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 .

Mesure : Comment Amazon EFS rapporte les tailles des systèmes de fichiers et des objets

Les sections suivantes décrivent comment Amazon EFS indique les tailles des systèmes de fichiers et des objets au sein d'un système de fichiers.

Mesures des objets du système de fichiers Amazon EFS

Les objets que vous pouvez consultez dans un système Amazon EFS sont les fichiers normaux, les répertoires, les liens symboliques et les fichiers spéciaux (FIFO et sockets). Chacun de ces objets est mesuré pour 2 Kio (kibioctets) 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'incrémentation 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'incrémentation 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'incrémentation 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` de NFSv4.1, il inclut la taille actuelle des données mesurées de l'objet au lieu de la taille de ses métadonnées. Vous pouvez utiliser deux utilitaires pour mesurer l'utilisation disque d'un fichier : duet `stat`. Voici un exemple d'utilisation de l'duutilitaire sur un fichier vide qui inclut l'`-k`option permettant de renvoyer le résultat en kilo-octets.

```
$ du -k file
4      file
```

L'exemple suivant montre comment utiliser l'`stat`utilitaire 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 Amazon EFS

La taille mesurée d'un système de fichiers Amazon 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 cohérence 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 Amazon EFS de différentes manières :

- À l'aide de la describe-file-systems AWS CLI commande et de l'opération DescribeFileSystemAPI, 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 mode Bursting Throughput.

- 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 Amazon pour Amazon EFS.

- Exécutez la commande `df` dans Linux à l'invite de terminal d'une instance EC2.

  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 plus d'informations, consultez 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, consultezAccès aux CloudWatch métriques. Pour plus d'informations sur la métrique `StorageBytes`, consultez CloudWatch Métriques Amazon 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 Amazon EFS utilisant le mode de débit élastique mesurent et facturent les métadonnées lues sous forme d'opérations de lecture et les métadonnées écrivent sous forme d'opérations d'écriture. Les opérations de métadonnées sont mesurées par incréments de 4 KiB et les opérations de données sont mesurées par incréments de 32 KiB.

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.

Gestion des coûts du système de fichiers Amazon EFS à l'aide de AWS Budgets

Vous pouvez planifier et gérer les coûts de votre système de fichiers Amazon EFS à l'aide de AWS Budgets.

Vous pouvez travailler avec AWS les budgets depuis la AWS Billing and Cost Management console. Pour utiliser AWS les budgets, vous devez créer un budget de coûts mensuel pour vos systèmes de fichiers EFS. Vous pouvez configurer votre budget pour vous avertir si vos coûts sont susceptioles de dépasser votre Montant budgété, puis effectuer des ajustements pour maintenir votre budget selon vos besoins.

L'utilisation des AWS budgets entraîne des coûts. Pour les budgets réguliers Comptes AWS, vos deux premiers budgets sont gratuits. Pour plus d'informations sur AWS les budgets, y compris les coûts, consultez la section Gérer vos coûts avec les budgets dans le guide de AWS Billing l'utilisateur.

Vous pouvez définir des budgets personnalisés pour les coûts et l'utilisation d'Amazon EFS au niveau du compte Région AWS, du service ou du tag en utilisant des paramètres budgétaires. Dans la section suivante, vous trouverez une description détaillée de la manière de configurer un budget de coûts sur un système de fichiers EFS avec AWS Budgets. Pour ce faire, utilisez des balises de répartition des coûts.

Prérequis

Pour effectuer les procédures décrites dans les sections suivantes, assurez-vous que vous disposez des éléments suivants :

- Un système de fichiers EFS
- Une politique AWS Identity and Access Management (IAM) avec les autorisations suivantes :
  - Accès à la AWS Billing and Cost Management console.
  - Capacité à effectuer les actions `elasticfilesystem:CreateTags` et `elasticfilesystem:DescribeTags`.

Création d'un budget des coûts mensuel pour un système de fichiers EFS

La création d'un budget des coûts mensuel pour votre système de fichiers Amazon EFS à l'aide de balises est un processus en trois étapes.

Créer un budget des coûts mensuel pour votre système de fichiers EFS à l'aide de balises

1. Créez une balise qui servira à identifier le système de fichiers pour lequel vous souhaitez suivre les coûts. Pour savoir comment procéder, veuillez consulter la section Balisage des ressources Amazon EFS.
2. Dans la console de facturation et de gestion des coûts, activez la balise en tant que balise de répartition des coûts. Pour obtenir une procédure détaillée, consultez Activation des balises de répartition des coûts dans le AWS Billing Guide de l'utilisateur.
3. Dans la console Billing and Cost Management, sous Budgets, créez un budget de coûts mensuel dans AWS Budgets. Pour une procédure détaillée, consultez Création d'un budget de coûts dans le AWS Billing Guide de l'utilisateur.

Après avoir créé votre budget des coûts mensuel EFS, vous pouvez l'afficher dans le tableau de bord Budgets qui présente les données budgétaires suivantes :

- L'utilisation et les coûts déjà engagés pour un budget pendant cette période budgétaire.
- Vos coûts budgétisés pour la période budgétaire.
- Votre prévision des coûts pour la période budgétaire.
- Un pourcentage qui Montre vos coûts par rapport au Montant budgété.
- Un pourcentage qui indique vos coûts prévus par rapport au Montant budgété.

Pour plus d'informations sur l'affichage de votre budget des coûts EFS, consultez Affichage de vos budgets dans le AWS Billing Guide de l'utilisateur..

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 plus d'informations, consultez Suppression des systèmes de fichiers Amazon EFS.
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 des systèmes de fichiers Amazon 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 plus d'informations, consultez : • Restauration d'un point de récupération. • Classes de stockage EFS • Répliquer des systèmes de fichiers

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 sorte 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
- Surveillance des métriques Amazon EFS 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 plus d'informations, consultez Surveillance des métriques Amazon EFS 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 la section Monitoring Log Files 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 vérifier également les fichiers journaux sur le système 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.

Surveillance des métriques Amazon EFS 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 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.

CloudWatch Métriques Amazon pour Amazon EFS

Les métriques Amazon EFS utilisent l'espace de noms `EFS` et fournissent des métriques relatives à 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`.

L'espace de noms `AWS/EFS` inclut les métriques suivantes.

`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.

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 mode débit en rafale, 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`

Le 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 mesurées à un tiers du taux des autres opérations.

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`

`TotalIOBytes`

Le nombre réel 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. Il s'agit de la quantité réelle générée par votre application, et non du débit mesuré par le système de fichiers. Il se peut qu'il soit supérieur aux chiffres indiqués dans`PermittedThroughput`.

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 y a une connexion par instance Amazon EC2 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).

Comment utiliser les métriques 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 `TotalIOBytes` pour consultez votre débit.
Comment puis-je suivre le nombre d'instances Amazon EC2 qui sont 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	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.

Comment... ?	Métriques pertinentes
transmission par rafales ?	

Utilisation de CloudWatch métriques pour surveiller les performances de débit

Les CloudWatch mesures de surveillance du débit (`TotalIOBytes`, `ReadIOBytesWriteIOBytes`, et`MetadataIOBytes`) 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` à`PermittedThroughput`.

`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.

Utilisation des maths de métriques avec Amazon EFS

À l'aide des mathématiques métriques, vous pouvez interroger plusieurs CloudWatch métriques 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 Utiliser les mathématiques 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	• `DataReadIOBytes` • `DataWriteIOBytes` • `MetadataIOBytes` • `TotalIOBytes`	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	• `TotalIOBytes`	sum	1 minute
m2	• `DataReadIOBytes`	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	`MeteredIOBytes`	sum	1 minute
m2	`PermittedThroughput`	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 (`DataReadIOBytesDataWriteIOBytes` 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`	sum	1 minute

ID	Métriques utilisables	Statistique	Période
	• `MetadataIOBytes`		
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 de l’état de réussite ou d’échec 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 instance EC2 afin d'utiliser les CloudWatch 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. Installer `amazon-efs-utils` sur l'instance EC2 qui Monte le système de fichiers. Pour plus d'informations, consultez Utilisation AWS Systems Manager pour installer ou mettre à jour automatiquement le client Amazon EFS ou Installation manuelle du client Amazon EFS.
2. Installer `botocore` sur l'instance EC2 qui Montera le système de fichiers. Pour plus d'informations, consultez 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
   ```
4. 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}
```

5. Associez la politique `AmazonElasticFileSystemsUtils` AWS gérée au rôle IAM que vous avez attaché à l'instance EC2 ou aux AWS informations d'identification configurées sur votre instance. Vous pouvez utiliser Systems Manager à cette fin. Pour obtenir plus d'informations, consultezÉtape 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

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Sélectionnez Groupes de journalisation dans la barre de navigation de gauche.
3. Choisissez le groupe de journaux /aws/efs/utils. Vous verrez un flux de journal pour chaque combinaison d'instance Amazon EC2 et de système de fichiers EFS.
4. 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.

Accès aux CloudWatch métriques

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

Les procédures suivantes vous Montrent comment accéder aux métriques à l'aide de ces différentes outils.

Pour consulter CloudWatch les métriques et les alarmes dans la 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 afficher les métriques à l'aide de la 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 Amazon CloudWatch API Reference.

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. Pour plus d'informations, consultez Procédure : Application du chiffrement sur un système de fichiers Amazon EFS au repos.

> **Note**
>
> Actuellement, vous ne pouvez pas appliquer le chiffrement en transit.

Les procédures suivantes expliquent comment créer des alarmes pour Amazon EFS.

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 être sur le point de créer. Sélectionnez Create Alarm (Créer une alerte).

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.

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 le Guide de l’utilisateur AWS CloudTrail.

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 afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec 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 :

- Présentation de la création d’un journal d’activité
- CloudTrail Services et intégrations pris en charge
- 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 appels d'API Amazon EFS sont enregistrés 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": "111122223333"
}
```


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": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/user1",
        "accountId": "111122223333",
        "accessKeyId": "A111122223333",
        "userName": "user1",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-10-23T22:45:41Z"
            }
        },
        "invokedBy": "elasticfilesystem.amazonaws.com”
    },
    "eventTime": "2019-10-23T22:45:41Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateServiceLinkedRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "user_agent",
    "requestParameters": {
        "aWSServiceName": "elasticfilesystem.amazonaws.com”
    },
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument":
 "111122223333-10-111122223333Statement111122223333Action111122223333AssumeRole111122223333Effe
%22%3A%20%22Allow%22%2C%20%22Principal%22%3A%20%7B%22Service%22%3A%20%5B%22
 elasticfilesystem.amazonaws.com%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::111122223333:role/aws-service-role/
elasticfilesystem.amazonaws.com/AWSServiceRoleForAmazonElasticFileSystem",
            "roleId": "111122223333",
            "createDate": "Oct 23, 2019 10:45:41 PM",
            "roleName": "AWSServiceRoleForAmazonElasticFileSystem",
            "path": "/aws-service-role/elasticfilesystem.amazonaws.com/“
        }
```

```
    },
    "requestID": "11111111-2222-3333-4444-abcdef123456",
    "eventID": "11111111-2222-3333-4444-abcdef123456",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

L'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": "20You 19-10-23T22:50:05Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateNetworkInterface",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "elasticfilesystem.amazonaws.com”,
    "userAgent": "elasticfilesystem.amazonaws.com",
    "requestParameters": {
```

```
        "subnetId": "subnet-71e2f83a",
        "description": "EFS mount target for fs-1234567 (fsmt-1234567)",
        "groupSet": {},
        "privateIpAddressesSet": {}
    },
    "responseElements": {
        "requestId": "0708e4ad-03f6-4802-b4ce-4ba987d94b8d",
        "networkInterface": {
            "networkInterfaceId": "eni-0123456789abcdef0",
            "subnetId": "subnet-12345678",
            "vpcId": "vpc-01234567",
            "availabilityZone": "us-east-1b",
            "description": "EFS mount target for fs-1234567 (fsmt-1234567)",
            "ownerId": "666051418590",
            "requesterId": "0123456789ab",
            "requesterManaged": true,
            "status": "pending",
            "macAddress": "00:bb:ee:ff:aa:cc",
            "privateIpAddress": "192.0.2.0",
            "privateDnsName": "ip-192-0-2-0.ec2.internal",
            "sourceDestCheck": true,
            "groupSet": {
                "items": [
                    {
                        "groupId": "sg-c16d65b6",
                        "groupName": "default"
                    }
                ]
            },
            "privateIpAddressesSet": {
                "item": [
                    {
                        "privateIpAddress": "192.0.2.0",
                        "primary": true
                    }
                ]
            },
            "tagSet": {}
        }
    },
    "requestID": "11112222-3333-4444-5555-666666777777",
    "eventID": "aaaabbbb-1111-2222-3333-444444555555",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
```

```
}
```

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 d’IAM pour contrôler l’accès aux données du système 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-aee3-f3429719d460",
    "readOnly": true,
    "resources": [
        {
            "accountId": "0123456789ab",
            "type": "AWS::EFS::FileSystem",
            "ARN": "arn:aws:elasticfilesystem:us-east-2:0123456789ab:file-system/
fs-01234567"
        },
        {
            "accountId": "0123456789ab",
            "type": "AWS::EFS::AccessPoint",
            "ARN": "arn:aws:elasticfilesystem:us-east-2:0123456789ab:access-point/
fsap-0123456789abcdef0"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "0123456789ab",
    "serviceEventDetails": {
        "permissions": {
            "ClientRootAccess": true,
            "ClientMount": true,
            "ClientWrite": true
        },
        "sourceIpAddress": "10.7.3.72"
    }
}
```


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 plus d'informations, consultez Chiffrement des données dans Amazon EFS.

Amazon EFS envoie un 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 chiffrées 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"
```

Performances 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 liés à Amazon EFS : problèmes de performances
- 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'opérations d'entrée/sortie 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 de performance maximale d'E/S présente des latences par opération plus élevées que celui 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	Lecture 1 par système de fichiers	Écriture 1 par système de fichiers	Lecture/écriture par client
Régional	Elasticité	Seulement 250 microsecondes (µs)	Seulement 2,7 millisecondes (ms)	90 000 à 250 000 2	50 000	3 à 20 gigaoctets 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

> **Note**
>
> Notes de bas de page :

1. Le débit de lecture et d'écriture maximal dépend du Région AWS. Un débit supérieur au débit maximal d'un Région AWS nécessite une augmentation du quota de débit. Toute demande de débit supplémentaire est prise en compte 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. Les systèmes de fichiers qui utilisent le débit élastique peuvent générer un maximum de 90 000 IOPS en lecture pour les données rarement consultées et de 250 000 IOPS en lecture pour les données fréquemment consultées. Des recommandations supplémentaires s'appliquent pour atteindre un maximum d'IOPS. Pour plus d'informations, consultez 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 des outils 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 E/S.

- 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 mode Max E/S est un type de performance de génération antérieure conçu pour les charges de travail hautement parallélisées qui peuvent tolérer des latences plus élevées que le mode Usage général. Le mode Max E/S n'est pas pris en charge pour les systèmes de fichiers Zone unique 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 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 plus d'informations, consultez CloudWatch Métriques Amazon 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 Utilisation de CloudWatch métriques pour surveiller les 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 plus d'informations, consultez 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 plus d'informations, consultez 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 plus d'informations, consultez Débit exceptionnel.

Vous pouvez utiliser Amazon CloudWatch pour déterminer le average-to-peak ratio de votre charge de travail en comparant la `MeteredIOBytes` métrique à la `PermittedThroughput` métrique. Pour

plus d'informations sur les métriques de demande Amazon EFS, consultez CloudWatch Métriques Amazon 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**
>
> Le débit élastique n'est disponible que pour les systèmes de fichiers qui utilisent le mode de performance General Purpose.

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 \ Bursting en vigueur à cet égard). Région AWS

Pour plus d'informations sur les limites par RegionProvisioned débit, consultezLes 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 de stockage, 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 MiB × 86 400 secondes = 432 000 MiB), qui peuvent être utilisés MiBps pour atteindre 100 MiB pendant 72 minutes (432 000 MiB ÷ 100 = 72 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 :

Taille d'E/S Moyen

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 faible latence par opération, le débit global augmente généralement avec la taille d'E/S Moyenne, les frais généraux étant amortis sur un plus grand volume 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 de 250 000 IOPS en lecture pour les données fréquemment consultées, le système de fichiers doit utiliser un 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’instance Amazon EC2 avant d’être écrites de manière asynchrone sur Amazon EFS. 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 requête que vous avez choisi fera des compromis en termes de cohérence (si vous utilisez plusieurs instances Amazon EC2) et de vitesse. 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 de Montage supplémentaires.

Lors du Montage de vos systèmes de fichiers sur les instances Amazon EC2, Amazon EFS prend en charge les protocoles Network File System version 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). Les instances Amazon EC2 macOS exécutant macOS Big Sur ne prennent en charge que NFS v4.0.

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 définie `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 liés à Amazon EFS : problèmes de performances

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’instance Amazon EC2 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 entrainant 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 plus d’informations, consultez Gestion des identités et des accès pour Amazon Elastic File System.

Accès refusé aux fichiers autorisés sur le système de fichiers NFS

Lorsqu’un utilisateur auquel sont attribués plus de 16 identifiants de groupe d’accès (GID) tente d’effectuer une opération sur un système de fichiers NFS, il peut se voir refuser l’accès aux fichiers autorisés du système de fichiers. Ce problème se produit car le protocole NFS prend en charge un maximum de 16 GID par utilisateur, et tous les GID supplémentaires sont tronqués 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 (GID) soient attribués à chaque utilisateur.

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 correctement auprès du service Amazon EC2. La console Amazon EFS appelle le service Amazon EC2 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’instance Amazon EC2 se bloque

Une instance Amazon EFS peut se bloquer si vous avez supprimé la cible de montage d’un système de fichiers sans démonter d’abord 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 clients RHEL 6 qui utilisent NFSv4.1, car ces clients NFS sérialisent les opérations d'ouverture et de fermeture NFS. 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 NFSv4.1, notez que le client NFSv4.0 Linux sérialise les demandes d'ouverture et de fermeture par ID d'utilisateur et ID de groupe. Cette sérialisation se produit même si plusieurs processus ou plusieurs threads émettent des requêtes en même temps. Le client envoie uniquement une seule opération d'ouverture ou de fermeture sur un serveur NFS à la fois, lorsque tous les ID correspondent. Pour contourner ces problèmes, vous pouvez effectuer l'une des actions suivantes :

- Vous pouvez exécuter chaque processus à partir d'un ID d'utilisateur différent sur la même instance Amazon EFS.
- Vous pouvez conserver les mêmes ID utilisateur sur toutes les requêtes ouvertes, puis modifier l'ensemble des ID de groupe.
- Vous pouvez exécuter chaque processus à partir d'une instance Amazon EC2 distincte.

Paramètres NFS personnalisés entrainant des délais d’écriture

Vous disposez de paramètres de client NFS personnalisés, et jusqu’à trois secondes sont parfois nécessaires pour qu’une instance Amazon EFS voit une opération d’écriture effectuée sur un système de fichiers depuis une autre instance Amazon EFS.

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 sur l’instance Amazon EFS qui lit des 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 d’attribut dans NFSv4.1 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

Ci-dessous, vous trouverez des informations sur la résolution des problèmes liés à certaines versions d'Amazon Machine Image (AMI) ou de noyau lors de l'utilisation d'Amazon EFS à partir d'une instance Amazon EC2.

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 de vos systèmes de fichiers Amazon EFS

AWS Backup est un moyen simple et économique de protéger vos données en sauvegardant vos systèmes de fichiers Amazon EFS. AWS Backup est un service de sauvegarde unifié conçu pour simplifier la création, la migration, la restauration et la suppression des sauvegardes, tout en fournissant des rapports et des audits améliorés. AWS Backup facilite le développement d'une stratégie de sauvegarde centralisée à des fins de conformité légale, réglementaire et professionnelle. AWS Backup simplifie également la protection AWS de vos volumes de stockage, de vos bases de données et de vos systèmes de fichiers en fournissant un emplacement central où vous pouvez effectuer les opérations suivantes :

- Configurer et auditer les AWS ressources que vous souhaitez sauvegarder
- Automatiser la planification des sauvegardes
- Définir des stratégies de conservation
- Surveiller toutes les activités de sauvegarde et de restauration récentes

Amazon EFS est intégré de manière native à AWS Backup. Vous pouvez utiliser la console EFS, l'API et AWS Command Line Interface (AWS CLI) pour activer les sauvegardes automatiques de votre système de fichiers. Les sauvegardes automatiques utilisent un plan de sauvegarde par défaut avec les paramètres AWS Backup recommandés pour les sauvegardes automatiques. Pour plus d'informations, consultez Sauvegardes automatiques. Vous pouvez également AWS Backup définir manuellement vos propres plans de sauvegarde en spécifiant la fréquence des sauvegardes, le moment de sauvegarde, la durée de conservation des sauvegardes et une politique de cycle de vie pour les sauvegardes. Vous pouvez ensuite attribuer des systèmes de fichiers Amazon EFS ou d'autres ressources AWS à ce plan de sauvegarde.

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 Amazon EFS et les modifier pendant que la 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.

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 1 000 fichiers par seconde ou 300 mégaoctets par seconde (Mbits/s), selon le taux le plus lent.
- Taux de restauration de 500 fichiers par seconde ou 150 Mbits/s, 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 plus d'informations, consultez Quotas pour les systèmes de fichiers Amazon EFS.

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 à l'endroit

où elle s'est arrêtée. Vous pouvez voir le statut de toutes les sauvegardes sur la console de gestion AWS Backup.

Classes de stockage EFS

Vous pouvez l'utiliser AWS Backup pour sauvegarder toutes les données d'un système de fichiers EFS, 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. Pour plus d’informations sur les classes de stockage, consultez Classes de stockage EFS et Gestion du stockage du système de fichiers.

Autorisations IAM pour créer et restaurer des sauvegardes

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 Elastic File System et Utilisation d’IAM pour contrôler l’accès aux données du système de fichiers.

Sauvegardes à la demande

À l’aide d’AWS Backup Management Console ou de l’interface de ligne de commande, 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.

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 les limites de AWS Backup , consultez Limites de AWS Backup dans le Guide du développeur AWS Backup .

Sauvegardes automatiques

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'interface de ligne de commande ou de l'API. 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-fort de sauvegarde EFS par défaut, également créé par EFS en votre nom. Le plan de sauvegarde par défaut et le coffre-fort de sauvegarde ne peuvent pas être supprimés. Vous pouvez modifier les paramètres du plan de sauvegarde par défaut à l'aide de la AWS Backup console. Pour de plus amples informations, consultez Option 3 : Créez des sauvegardes automatiques dans le Guide du développeur AWS Backup . 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. Vous pouvez désactiver les sauvegardes automatiques à tout moment à l'aide de la console Amazon EFS ou de l'interface de ligne de commande, comme indiqué dans la section suivante.

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.

> **Note**
>
> Les sauvegardes automatiques ne sont pas soumises à la configuration AWS Backup de désactivation du service. Pour plus d'informations, consultez Mise en route avec AWS Backup dans le AWS Backup Guide du développeur.

Activation ou désactivation de sauvegardes automatiques pour les systèmes de fichiers existants

Après avoir créé un système de fichiers, vous pouvez activer ou désactiver les sauvegardes automatiques à l'aide de la console, de l'interface de ligne de commande ou de l'API EFS.

Activez ou désactivez les sauvegardes automatiques pour un système de fichiers existant (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.

Activez ou désactivez les sauvegardes automatiques pour un système de fichiers existant (interface de ligne de commande)

- 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"
```

    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"
```

EFS répond avec la nouvelle politique de sauvegarde.

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

Utilisation AWS Backup pour configurer manuellement les sauvegardes

Lorsque vous configurez manuellement AWS Backup les sauvegardes de votre système de fichiers, vous devez d'abord créer un plan de sauvegarde. Le plan de sauvegarde définit le calendrier de sauvegarde, fenêtre de sauvegarde, la stratégie de conservation, la stratégie de cycle de vie et les balises. Vous pouvez créer un plan de sauvegarde à l'aide de la console de AWS Backup gestion AWS CLI, de ou de l' AWS Backup API. Dans le cadre d'un plan de sauvegarde, vous pouvez définir les éléments suivants :

- Planification – Quand la sauvegarde a lieu
- Fenêtre de sauvegarde – Fenêtre de temps au cours de laquelle la sauvegarde doit démarrer
- Cycle de vie – Quand déplacer un point de récupération vers le stockage à froid et quand le supprimer
- Coffre-fort de sauvegarde – Quel coffre-fort utiliser pour organiser les points de récupération créés par la règle de sauvegarde

Une fois le plan de sauvegarde créé, vous devez attribuer les systèmes de fichiers Amazon EFS spécifiques au plan de sauvegarde en utilisant des balises ou l'ID de système de fichiers Amazon EFS. Une fois qu'un plan est affecté, AWS Backup commence automatiquement à sauvegarder le système de fichiers Amazon EFS en votre nom selon le plan de sauvegarde que vous avez défini. Vous pouvez utiliser la AWS Backup console pour gérer les configurations de sauvegarde ou surveiller les activités de sauvegarde. Pour plus d'informations, consultez le Guide du développeur AWS Backup .

> **Note**
>
> Les sockets et les canaux nommés ne sont pas pris en charge, et ne sont pas pris en compte dans les sauvegardes.

Restauration d'un point de récupération

À l'aide de la console AWS Backup ou de l'interface de ligne de commande, vous pouvez restaurer un point de récupération vers un nouveau système de fichiers EFS ou un système de fichiers existant. Vous pouvez effectuer une restauration complète, qui restaure l'ensemble du système de fichiers. Vous pouvez également restaurer des fichiers et des répertoires spécifiques à l'aide d'une restauration partielle. Pour restaurer un fichier ou un répertoire spécifique, vous devez spécifier le chemin relatif lié au point de montage. Par exemple, si le système de fichiers est monté sur `/file1` et que le chemin d'accès au fichier est `/user/home/myname/efs`, saisissez `user/home/myname/efs/file1`. Les chemins sont sensibles à la casse et ne peuvent pas contenir de caractères spéciaux, de caractères génériques ou de chaînes d'expression régulière (regex).

> **Note**
>
> Pour restaurer un point de récupération, les utilisateurs doivent disposer de l'autorisation `backup:StartRestoreJob`.

Lorsque vous effectuez une restauration complète ou partielle, votre point de récupération est restauré dans le répertoire de restauration `aws-backup-restore_`*`timestamp-of-restore`*. Lorsque la restauration est terminée, vous pouvez voir le répertoire de restauration à la racine du système de fichiers. Si vous tentez plusieurs restaurations pour le même chemin d'accès, plusieurs répertoires contenant les éléments restaurés peuvent exister. Si la restauration échoue, vous pouvez voir le répertoire `aws-backup-failed-restore_`*`timestamp-of-restore`*. Vous devez supprimer manuellement les répertoires `restore` et `failed-restore` lorsque vous avez fini de les utiliser.

> **Note**
>
> Pour les restaurations partielles d'un système de fichiers EFS existant, AWS Backup restaure les fichiers et les répertoires dans un nouveau répertoire situé sous le répertoire racine du système de fichiers. La hiérarchie complète des éléments spécifiés est conservée dans le

répertoire de récupération. Par exemple, si le répertoire A contient les sous-répertoires B, C et D, il AWS Backup conserve la structure hiérarchique lorsque A, B, C et D sont restaurés.

Après avoir restauré un point de récupération, les fragments de données qui ne peuvent pas être restaurés dans le répertoire approprié sont placés dans le répertoire `aws-backup-lost+found`. Les fragments peuvent être déplacés vers ce répertoire si des modifications sont apportées au système de fichiers pendant que la sauvegarde est en cours.

Suppression de sauvegardes

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.

Pour supprimer un point de récupération EFS dans AWS Backup

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation de gauche, choisissez Coffres-forts de sauvegarde.
3. Dans la liste Coffres-forts de sauvegarde, choisissez aws/efs/automatic-backup-vault.
4. Sur la page de détails du coffre-fort, choisissez Gérer l'accès dans l'angle supérieur droit de la page. La page Modifier la politique d'accès s'affiche.
5. Pour autoriser toutes les actions sur le coffre-fort de sauvegarde EFS, recherchez la ligne `"Effect": "Deny",` dans l'éditeur JSON et modifiez la ligne `"Effect": "Allow",`.
6. Choisissez Enregistrer la politique pour enregistrer les changements.
7. Sur la page des détails du coffre-fort, allez à la section Sauvegardes et sélectionnez les points de restauration que vous souhaitez supprimer dans la liste des sauvegardes. Ensuite, choisissez Actions, puis Supprimer.

8. Suivez les instructions pour confirmer la suppression. Choisissez ensuite Supprimer les points de récupération.

Répliquer des systèmes de fichiers

Vous pouvez créer une réplique de votre système de fichiers EFS comme vous le Région AWS souhaitez. Lorsque vous activez la réplication sur un système de fichiers EFS, Amazon Elastic File System (Amazon EFS) réplique de manière automatique et 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 jeu, vous pouvez revenir à votre système de fichiers répliqué, puis revenir au système de fichiers principal pour reprendre les opérations. 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 réplication. Pour en savoir plus sur la configuration de réplication d'un système de fichiers, veuillez consulter Configuration de réplication.

Une fois la configuration de réplication créée pour un système de fichiers, Amazon EFS synchronise automatiquement les systèmes de fichiers source et de destination. Les modifications apportées au système de fichiers source ne sont pas transférées vers le système de fichiers de destination de manière point-in-time cohérente, mais sont transférées en fonction de l'heure de dernière synchronisation pour la réplication. 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 plus d'informations, consultez Surveillance des emplacements de réplication.

La réplication est disponible Régions AWS dans tous les pays où EFS est disponible. Pour utiliser la réplication dans une région désactivée par défaut, vous devez d'abord vous inscrire à la région. Pour plus d'informations, consultez Gestion Régions AWS dans le AWS Guide de Référence générale. Si vous vous désabonnez ultérieurement d'une région, Amazon EFS suspend toutes les activités de réplication pour cette région. Pour reprendre les activités de réplication pour la région, vous devez à nouveau vous connecter au Région AWS.

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

Rubriques

- Configuration de réplication
- Créer une configuration de réplication.
- Affichage des configurations de réplication
- Supprimer des configuration de réplication
- Surveillance des emplacements de réplication

Configuration de réplication

Lorsque vous créez la configuration de réplication pour votre système de fichiers, vous choisissez le Région AWS dans lequel créer la réplication et vous devez effectuer la réplication vers un système de fichiers de destination nouveau ou existant.

> **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.

Réplication vers un nouveau système de fichiers

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 le Région AWS système de fichiers de votre choix. Le système de fichiers de destination est créé avec les propriétés suivantes :

- 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 clé AWS Key Management Service (AWS KMS) 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.

- 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 Sauvegardes automatiques.
- 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 Performance Usage général 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 stockage du système de fichiers.

Réplication vers un système de fichiers existant

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, EFS identifie les différences de données entre les systèmes de fichiers et applique ces différences au système de fichiers de destination.

Lors de la réplication vers un système de fichiers existant, les conditions suivantes s'appliquent.

- La protection contre le remplacement par réplication du système de fichiers de destination doit être désactivée. La protection contre le remplacement de la réplication empêche le système de fichiers d'être utilisé comme destination dans une configuration de réplication. Pour plus d'informations sur la désactivation de la protection, consultez Protection du système de fichiers.

  La désactivation de la protection contre le remplacement de la réplication nécessite des autorisations pour l'action elasticfilesystem :. UpdateFileSystemProtection Pour plus d'informations, consultez AWSpolitique gérée : AmazonElasticFileSystemFullAccess.

- 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.

Protection 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 inscriptiole.

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 AWSpolitique gérée : AmazonElasticFileSystemFullAccess.

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 inscriptiole. 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.

Pour désactiver la protection contre le remplacement de la réplication (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.

Autorisations nécessaires

Amazon EFS utilise le rôle lié au service EFS nommé `AWSServiceRoleForAmazonElasticFileSystem` pour synchroniser l'état de la réplication entre les systèmes de fichiers source et de destination. Pour utiliser la réplication EFS, vous devez configurer les autorisations suivantes de manière à permettre à une entité IAM (comme un utilisateur,

groupe ou rôle) de créer un rôle lié à un service, une configuration de réplication et un système de fichiers.

- `elasticfilesystem:CreateReplicationConfiguration`*
- `elasticfilesystem:DeleteReplicationConfiguration`*
- `elasticfilesystem:DescribeFileSystem`
- `elasticfilesystem:DescribeReplicationConfigurations`*
- `elasticfilesystem:CreateFileSystem`*
- `iam:CreateServiceLinkedRole`— consultez l'exemple dansUtilisation des rôles liés à un service pour Amazon EFS.

> **Note**
>
> * Vous pouvez aussi utiliser la politique `AmazonElasticFileSystemFullAccess` gérée pour obtenir automatiquement toutes les autorisations EFS requises. Pour de plus amples informations, veuillez consulter AWSpolitique gérée : AmazonElasticFileSystemFullAccess.

Coûts

Afin de faciliter la réplication, Amazon EFS crée des répertoires cachés et des métadonnées sur le système de fichiers de destination. Cela équivaut à environ 12 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 Mesure : Comment Amazon EFS rapporte les tailles des systèmes de fichiers et des objets.

Performance

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 Surveillance des emplacements 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 plus d'informations, consultez Surveillance des emplacements de réplication.

Montage d'un 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 un système de fichiers de destination, vous devez créer une ou plusieurs cibles de Montage. Pour de plus amples informations, veuillez consulter Utilisation de l'assistant de Montage EFS pour Monter les systèmes de fichiers EFS.

Étant donné qu'un système de fichiers de destination est en lecture seule lorsqu'il est membre d'une configuration de réplication, toutes les opérations d'écriture sur ce système échoueront. Toutefois, vous pouvez utiliser le système de fichiers de destination pour les cas d'utilisation en lecture seule, y compris les tests et le développement.

Basculement et restauration du système de fichiers

En cas de sinistre ou lorsque vous effectuez des exercices le jour du jeu, 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 inscriptiole 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.

Créer une configuration de réplication.

Vous pouvez utiliser la console Amazon EFS, l'API ou le AWS CLI pour répliquer un système de fichiers EFS. Les sections suivantes fournissent des instructions détaillées sur l'utilisation de chacune de ces méthodes.

Pour créer un jeu de configurations (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, puis, dans la section Réplication, sélectionnez Créer une réplication. La page Créer une réplication s'ouvre.
4. Dans la section Paramètres de réplication, définissez les paramètres de réplication :
   a. Pour Configuration de la réplication, choisissez de répliquer le système de fichiers vers un nouveau système de fichiers ou 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.

5. Si vous effectuez une réplication vers un nouveau système de fichiers de destination, 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 plus d'informations, consultez 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, EFS utilise votre clé de service AWS Key Management Service (AWS KMS) pour Amazon EFS (`aws/elasticfilesystem`). Pour utiliser une autre clé KMS, choisissez une clé KMS ou entrez l'ARN d'une clé existante.

      > **Important**
      >
      > Vous ne pouvez pas Modifier ces propriétés après la création de la clé KMS.

6. Si vous effectuez une réplication vers un système de fichiers de destination existant, choisissez Rechercher EFS, puis sélectionnez le système de fichiers. Le chemin d'accès au fichier de destination apparaît dans la zone Destination.

   Si la protection contre le remplacement de la réplication est activée sur le système de fichiers, un avertissement s'affiche, vous invitant à désactiver la protection. Pour désactiver la protection,

choisissez Désactiver la protection, puis désactivez protection contre le remplacement de la réplication. Après avoir désactivé la protection, cliquez sur le bouton Actualiser pour effacer le message.

7. Choisissez Créer une réplication. Si vous effectuez une réplication vers un nouveau système de fichiers, un message s'affiche pour vous demander de confirmer la réplication. Tapez confirmer dans la zone de saisie, puis cliquez sur Créer une réplication.

   La section Réplication apparaît et affiche les détails de la réplication. La valeur État de réplication est initialement Activée, et la Dernière synchronisation est vide. Lorsque l'état Indique Activé, la Dernière synchronisation indique que la Synchronisation initiale est en cours.
8. Pour consulter les informations de configuration du système de fichiers de destination, choisissez l'ID du système de fichiers au-dessus du Système de fichiers de destination. La page Détails du système de fichiers du système de fichiers de destination s'affiche dans un nouvel onglet du navigateur (en fonction des paramètres de votre navigateur).

Pour créer une configuration de réplication (CLI)

Pour créer une configuration de réplication, utilisez la commande CLI `create-replication-configuration`. La commande API équivalente est CreateReplicationConfiguration.

Example : 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*. Cet exemple utilise le `Region` paramètre pour créer un système de fichiers de destination dans le *eu-west-2* Région AWS. Le paramètre `KmsKeyId` spécifie l'ID 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"
}
```

Example : 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*. Cet exemple utilise le paramètre `AvailabilityZoneName` pour créer un système de fichiers de destination dans la Zone de disponibilité *us-west-2a*. 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 pour Amazon EFS (`aws/elasticfilesystem`).

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

Affichage des configurations de réplication

Pour consulter la configuration de réplication d'un système de fichiers, vous pouvez utiliser la console Amazon EFS ou le AWS CLI.

Pour consulter une configuration de réplication (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 un système de fichiers dans la liste.
4. 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’L’État de réplication peut être Activation, Activé, Suppression, Suspension, Suspendu ou Erreur.

  L’État Suspendu se produit lorsque vous vous désactivez de la région source ou de destination après la création de la configuration de réplication. Pour reprendre la réplication du système de fichiers, vous devez à nouveau vous connecter au Région AWS. Pour plus d’informations, consultez Gestion Régions AWS dans le AWS Guide de référence général.

  L’état Réplication se produit après la création d’une réplication, le système de fichiers étant soit le système de fichiers source, soit le système de fichiers de destination.

  L’état Erreur se produit lorsque le système de fichiers source ou de destination (ou les deux) est défaillant et est irrécupérable. Pour de plus amples informations, veuillez consulter Surveillance des emplacements de réplication. Pour effectuer une restauration, vous devez supprimer la configuration de réplication, puis restaurer la sauvegarde la plus récente du système de fichiers défaillant (source ou destination) sur un nouveau système de fichiers.
- 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.

Pour consulter une configuration de réplication (CLI)

Pour créer une configuration de réplication, utilisez la commande CLI `describe-replication-configurations`. 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.

Pour afficher la configuration de réplication d'un système de fichiers, utilisez le paramètre de demande URI `file-system-id`. Vous pouvez spécifier l'ID d'un système de fichiers source ou de destination.

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

```
{
    "Replications": [
        {
            "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:111122223333:file-system/fs-abcdef0123456789a",
            "CreationTime": 1641491892.0,
            "SourceFileSystemRegion": "eu-west-1",
            "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:111122223333:file-system/fs-abcdef0123456789a",
            "SourceFileSystemId": "fs-abcdef0123456789a",
            "Destinations": [
                {
                    "Status": "ENABLED",
                    "FileSystemId": "fs-0123456789abcdef1",
                    "Region": "us-east-1"
                }
            ]
        }
    ]
}
```

Pour afficher toutes les configurations de réplication d'un compte dans un Région AWS, ne spécifiez pas le `file-system-id` paramètre.

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

```
{
    "Replications": [
        {
            "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-0123456789abcdef1",
```

```
            "CreationTime": 1641491892.0,
            "SourceFileSystemRegion": "eu-west-1",
            "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-0123456789abcdef1",
            "SourceFileSystemId": "fs-0123456789abcdef1",
            "Destinations": [
                {
                    "Status": "ENABLED",
                    "FileSystemId": "fs-abcdef0123456789a",
                    "Region": "us-east-1",
                    "LastReplicatedTimestamp": 1641491802.375
                }
            ]
        },
        {
            "SourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-021345abcdef6789a",
            "CreationTime": 1641491822.0,
            "SourceFileSystemRegion": "eu-west-1",
            "OriginalSourceFileSystemArn": "arn:aws:elasticfilesystem:eu-
west-1:555555555555:file-system/fs-021345abcdef6789a",
            "SourceFileSystemId": "fs-021345abcdef6789a",
            "Destinations": [
                {
                    "Status": "ENABLED",
                    "FileSystemId": "fs-012abc3456789def1",
                    "Region": "us-east-1",
                    "LastReplicatedTimestamp": 1641491823.575
                }
            ]
        }
    ]
}
```

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. Une fois que vous avez 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 plus d'informations, consultez Basculement et restauration du système de fichiers.

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, de la CLI ou de l'API.

Pour consulter une configuration de réplication (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.

Pour supprimer une configuration de réplication (CLI)

Pour supprimer une configuration de réplication, utilisez la commande CLI `delete-replication-configuration`. La commande API équivalente est DeleteReplicationConfiguration.

Pour spécifier la configuration de réplication que vous souhaitez supprimer, utilisez le paramètre `source-file-system-id`.

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

```
--source-file-system-id fs-0123456789abcdef1
```

Surveillance des emplacements 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 vérifier à quel moment la dernière réplication s'est terminée avec succès, vous pouvez utiliser la console, la CLI, l'API ou Amazon CloudWatch.

- Dans la console : 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 la CLI ou l'API : la `LastReplicatedTimestamp` propriété de l'objet `Destination` indique l'heure à laquelle la dernière synchronisation réussie s'est terminée. Pour accéder à cette propriété, utilisez la commande `describe-replication-configurations` CLI. DescribeReplicationConfigurationsest 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 plus d'informations, consultez CloudWatch Métriques Amazon pour Amazon EFS.

Vous pouvez également surveiller l'état d'une configuration de réplication à l'aide de la console, de la CLI ou de l'API. 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.

État de réplication	Description
PAUSING	Suite de l’exclusion de la région d’un ou des deux systèmes de fichiers de la configuration de réplication, Amazon EFS est en train d’interrompre la réplication.
PAUSED	La réplication est interrompue suite à l’exclusion de la région pour l’un ou les deux systèmes de fichiers de la configuration de réplication. Pour relancer la réplication, vous devez à nouveau vous connecter à Région AWS. Pour plus d’informations, consultez Gestion Régions AWS dans le AWS Guide de référence général.
ERROR	L’un des systèmes de fichiers de la configuration de réplication (ou les deux) est défaillant et est irrécupérable. Pour accéder aux données du système de fichiers, restaurez une sauvegarde du système de fichiers défaillant sur un nouveau système de fichiers. Pour de plus amples informations, veuillez consulter Restauration d’un point de récupération.

Procédure Amazon Elastic File System

Cette section fournit des procédures que vous pouvez utiliser pour explorer Amazon EFS et tester la configuration de bout en bout.

Rubriques

- Procédure pas à pas : créez un système de fichiers Amazon EFS et montez-le sur une instance Amazon EC2 à l'aide du AWS CLI
- Procédure : Configurer un serveur web Apache et servir des fichiers Amazon EFS
- Procédure : Création de sous-répertoires par utilisateur accessibles en écriture et configuration d'un remontage au redémarrage automatique
- Procédure : Créer et monter un système de fichiers sur site avec AWS Direct Connect et VPN
- Procédure : montage d’un système de fichiers à partir d’un autre VPC
- Procédure : Application du chiffrement sur un système de fichiers Amazon EFS au repos
- Procédure pas à pas : activer le root squashing à l'aide de l'autorisation IAM pour les clients NFS

Procédure pas à pas : créez un système de fichiers Amazon EFS et montez-le sur une instance Amazon EC2 à l'aide du AWS CLI

Cette procédure pas à pas utilise le AWS CLI pour explorer l'API Amazon EFS. Dans ce guide, vous créez un système de fichiers Amazon EFS chiffré, vous le montez sur une instance Amazon EC2 dans votre VPC et vous testez la configuration.

> **Note**
>
> Cette procédure est similaire à l’exercice de mise en route. Dans l’exercice Premiers pas, vous utilisez la console pour créer des ressources EC2 et Amazon EFS. Dans cette procédure pas à pas, vous allez utiliser le AWS CLI pour faire de même, principalement pour vous familiariser avec l'API Amazon EFS.

Dans cette procédure pas à pas, vous allez créer les AWS ressources suivantes dans votre compte :

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

Vous ajoutez des règles à ces groupes de sécurité afin d'autoriser un accès entrant/sortant approprié. Cela permet à votre instance EC2 de se connecter au système de fichiers via la cible de montage à l'aide d'un port TCP NFSv4.1 standard.

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

    Pour monter votre système de fichier sur une instance EC2, 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 plus d'informations, consultez Comment fonctionne Amazon EFS.

Ensuite, vous testez le système de fichiers sur votre instance EC2. L'étape de nettoyage à la fin de la procédure fournit des informations concernant la suppression de ces ressources.

La procédure 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, vos ressources EC2 et vos ressources Amazon EFS, doivent se trouver dans le même Région AWS.

Avant de commencer

- 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 Mise à jour du support 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 Passerelles Internet dans le Amazon VPC Guide de l'utilisateur.
  - 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 Adressage IP dans votre VPC dans le Amazon VPC Guide de l'utilisateur.
  - 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, consultez les rubriques suivantes dans le Guide de l'utilisateur de l'AWS Command Line Interface :

   Configuration à l'aide de l'interface de ligne de AWS commande

   Installation de l'interface AWS de ligne de commande

   Configuration de l'interface AWS de ligne de commande
2. Définissez des profils.

   Vous stockez les informations d'identification de l'utilisateur dans le AWS CLI `config` fichier. Les exemples de commandes CLI dans cette procédure 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 n'indiquez aucune région dans la commande d'interface de ligne de commande, la région us-west-2 est utilisée par défaut.

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 suivante

Étape 1 : Créer les ressources Amazon EC2

Étape 1 : Créer les ressources Amazon EC2

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.
- Lancer une instance EC2. Vous créez et montez un système de fichiers Amazon EFS sur cette instance à l'étape suivante.

Rubriques

- Étape 1.1 : Créer deux groupes de sécurité
- Étape 1.2 : Ajouter des règles aux groupes de sécurité afin d'autoriser un accès entrant/sortant
- Étape 1.3 : Lancer une instance EC2

Étape 1.1 : Créer deux groupes de sécurité

Dans cette section, vous créez des groupes de sécurité dans votre VPC pour votre instance EC2 et la cible de montage Amazon EFS. Plus tard dans la procédure, vous attribuez ces groupes de sécurité à une instance EC2 et une cible de montage Amazon EFS. Pour plus d'informations sur les groupes de sécurité, consultez la section Groupes de sécurité Amazon EC2 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 instance EC2 et fournissez votre ID de 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 Amazon 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 permettre de vous connecter à votre instance EC2.
- Activer le trafic entre une instance EC2 et une cible de montage Amazon EFS (à laquelle vous associez ces groupes de sécurité plus loin dans cette procédure).

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 SSH entrantes au groupe de sécurité pour votre instance EC2 (`efs-walkthrough1-ec2-sg`) afin de pouvoir vous connecter à votre instance EC2 à l'aide de 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-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 instance EC2

Dans cette étape, vous lancez une instance EC2.

Pour lancer une instance EC2

1. Collectez les informations suivantes que vous devez fournir lors du lancement d'une instance EC2 :

- Nom de la paire de clés :
  - Pour des informations de présentation, consultez Configurer pour utiliser Amazon EC2.
  - Pour obtenir des instructions sur la création d'un fichier .pem, consultez la section Créer une paire de clés dans le guide de l'utilisateur Amazon EC2.
- ID de l'Amazon Machine Image (AMI) que vous souhaitez lancer.

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

  > **Note**
  >
  > Vous pouvez utiliser des AMI Linux d'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 HVM Amazon Linux, vous pouvez trouver les ID les plus récents à la section AMI Amazon Linux. Vous choisissez la valeur de l'ID dans le tableau des ID d'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 instance EC2.
- 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 créez une cible de montage dans le même sous-réseau que celui où vous lancez une instance EC2.
- Zone de disponibilité du sous-réseau – Vous avez besoin de cette valeur pour construire le nom DNS de votre cible de montage, laquelle vous permet de monter un système de fichiers sur l'instance EC2.

2. Exécutez la AWS CLI `run-instances` commande suivante pour lancer une instance EC2.

```
$ aws ec2 run-instances \
--image-id AMI ID \
--count 1 \
--instance-type t2.micro \
--associate-public-ip-address \
--key-name key-pair-name \
--security-group-ids ID of the security group created for EC2 instance \
--subnet-id VPC subnet ID \
--region us-west-2 \
--profile adminuser
```

3. Notez l'ID d'instance renvoyé par la commande `run-instances`.
4. L'instance EC2, que vous avez créée doit avoir un nom DNS public que vous utilisez pour vous connecter à l'instance EC2 et monter le système de fichier dessus. 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 sur lequel vous avez lancé l'instance EC2. Pour plus d'informations, consultez Avant de commencer.

5. (Facultatif) Attribuez un nom à l'instance EC2 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 suivante

Étape 2 : Créer les ressources Amazon EFS

Étape 2 : Créer les ressources Amazon EFS

Dans cette étape, vous effectuez les opérations suivantes :

- Créer un système de fichiers EFS
- Activez la gestion du cycle de vie.
- Créez une cible de montage dans la zone de disponibilité où votre instance EC2 a été lancée.

Rubriques

- Étape 2.1 : Créer un système de fichiers Amazon EFS
- Étape 2.2 : Activer la gestion du cycle de vie
- Étape 2.3 : Créer une cible de montage

Étape 2.1 : Créer un système de fichiers Amazon EFS

Dans cette étape, vous créez un système de fichiers Amazon 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 sur votre système de fichiers afin d'utiliser la classe de stockage Accès peu fréquent. Pour en savoir plus, consultez Gestion du stockage du système de fichiers 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

Dans cette étape, vous créez une cible de montage pour votre système de fichiers dans la zone de disponibilité où votre instance EC2 est lancée.

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'instance EC2 à l'étape 1.

Pour cette procédure, vous créez la cible de montage dans le même sous-réseau que celui où vous avez lancé l'instance EC2, vous n'avez donc pas besoin de l'ID de 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 suivante

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

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

Dans cette étape, vous effectuez les opérations suivantes :

Rubriques

- Étape 3.1 : Collecter des informations
- Étape 3.2 : Installer le client NFS sur votre instance EC2
- Étape 3.3 : Monter le système de fichiers sur votre instance EC2 et tester

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 instance EC2 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'instance EC2 sur laquelle vous montez le système de fichiers via la cible de montage peut résoudre le nom DNS du système de fichiers par l'adresse IP de la cible de montage.

> **Note**
>
> Amazon EFS ne nécessite pas que votre instance Amazon EC2 ait une adresse IP publique 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 : Installer le client NFS sur votre instance EC2

Vous pouvez vous connecter à votre instance EC2 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 instance EC2 :

   - Pour vous connecter à votre instance à partir d'un ordinateur exécutant macOS ou Linux, spécifiez le fichier .pem dans votre commande SSH avec l'option `-i` et le chemin d'accès à la clé privée.
   - Pour vous connecter à votre instance depuis un ordinateur exécutant Windows, vous pouvez utiliser l'un MindTerm ou l'autre des systèmes PuTTY. Si vous prévoyez d'utiliser PuTTY, vous devez l'installer et exécuter la procédure suivante pour convertir le fichier .pem en fichier .ppk.

   Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur Amazon EC2 :

   - Connectez-vous à votre instance Linux depuis Windows avec PuTTY
   - Connectez-vous à votre instance Linux depuis Linux ou macOS via SSH

2. Exécutez les commandes suivantes sur l'instance EC2, via la session SSH :

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

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

   Une fois le redémarrage effectué, reconnectez-vous à votre instance EC2.

   b. Installez le client NFS.

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

   > **Note**
   >
   > Si vous choisissez l'AMI Amazon Linux Amazon Linux AMI 2016.03.0 lors du lancement de votre instance Amazon EFS, vous n'avez pas besoin d'installer `nfs-utils`, car il est déjà inclus par défaut dans l'AMI.

Étape 3.3 : Monter le système de fichiers sur votre instance EC2 et tester

À présent, vous montez le système de fichiers sur votre instance EC2.

1. Créez un répertoire ("efs-mount-point").

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

2. Montage d'un système de fichiers Amazon EFS

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

L'instance EC2 peut résoudre le nom DNS de la cible de montage par l'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,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-target-ip:/  ~/efs-mount-point
```

3. Maintenant que le système de fichiers Amazon EFS est monté sur votre instance EC2, 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 un système de fichiers Amazon EFS sur votre instance EC2 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`. Pour plus d'informations, consultez Remontage automatique au redémarrage. Si vous utilisez un groupe Auto Scaling pour lancer des instances EC2, vous pouvez aussi définir des scripts dans une configuration de lancement. Pour obtenir un exemple, consultez Procédure : Configurer un serveur web Apache et servir des fichiers Amazon EFS.

Étape suivante

Étape 4 : Nettoyer

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

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

1. Résiliez l'instance EC2, que vous avez créée pour cette procédure.

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

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

   Pour obtenir des instructions, consultez la section Suppression d'un groupe de sécurité dans le guide de l'utilisateur Amazon EC2.

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
```

Procédure : Configurer un serveur web Apache et servir des fichiers Amazon EFS

Vous pouvez avoir des instances EC2 qui exécutent le serveur web Apache qui distribue les fichiers stockés sur votre système de fichiers Amazon EFS. Il peut s'agir d'une instance EC2, ou si votre application l'exige, de plusieurs instances EC2 qui distribuent les fichiers de votre système de fichiers Amazon EFS. Les procédures suivantes sont décrites.

- Configurer un serveur web Apache sur une instance EC2.
- Configurer un serveur web Apache sur plusieurs instances EC2 en créant un groupe Auto Scaling. Vous pouvez créer plusieurs instances EC2 à l'aide d'Amazon EC2 Auto Scaling, AWS un service qui vous permet d'augmenter ou de diminuer le nombre d'instances EC2 dans un groupe en fonction des besoins de votre application. Lorsque vous avez plusieurs serveurs web, vous avez également besoin d'un équilibreur de charges afin de répartir le trafic sur ces serveurs.

> **Note**
>
> Pour les deux procédures, vous créez toutes les ressources dans la région USA Ouest (Oregon) (`us-west-2`).

instance EC2 unique pour la distribution de fichiers

Suivez les étapes de configuration d'un serveur web Apache sur une instance EC2 pour distribuer les fichiers que vous créez sur votre système de fichiers Amazon EFS.

1. Suivez les étapes de l'exercice de mise en route de manière à disposer d'une configuration opérationnelle composée des éléments suivants :

   - Système de fichiers Amazon EFS
   - instance EC2
   - Système de fichiers monté sur l'instance EC2

   Pour obtenir des instructions, veuillez consulter Débuter avec Amazon Elastic File System Amazon Elastic File System. Lors de l'exécution de ces étapes, notez les informations suivantes :

   - Nom DNS public de l'instance EC2.
   - Nom DNS public de la cible de montage créée dans la zone de disponibilité où vous avez lancé l'instance EC2.
2. (Facultatif) Vous pouvez choisir de démonter le système de fichiers depuis le point de montage que vous avez créé dans l'exercice de mise en route.

   ```
   $ sudo umount  ~/efs-mount-point
   ```

   Dans cette procédure, vous créez un autre point de montage pour le système de fichiers.
3. Sur votre instance EC2, installez le serveur web Apache et configurez-le comme suit :

   a. Connectez-vous à votre instance EC2 et installez le serveur web Apache.

      ```
      $ sudo yum -y install httpd
      ```

   b. Lancez le service .

      ```
      $ sudo service httpd start
      ```

   c. Créez un point de montage.

Tout d'abord notez que `DocumentRoot` dans le fichier `/etc/httpd/conf/httpd.conf` pointe sur `/var/www/html` (`DocumentRoot "/var/www/html"`).

Vous allez monter votre système de fichiers Amazon EFS sur un sous-répertoire sous la racine du document.

Créez un sous-répertoire nommé `efs-mount-point` à utiliser comme point de montage pour votre système de fichiers, sous `/var/www/html`.

```
$ sudo mkdir /var/www/html/efs-mount-point
```

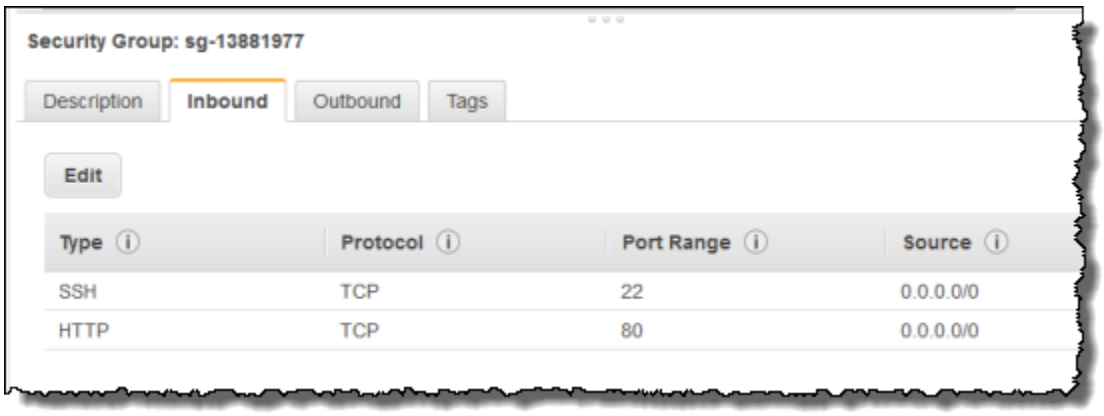
d. Montez votre système de fichiers Amazon EFS à l'aide de la commande suivante. Remplacez `file-system-id` par l'ID de votre système de fichiers.

```
$ sudo mount -t efs file-system-id:/ /var/www/html/efs-mount-point
```

4. Testez la configuration.

a. Ajoutez une règle dans le groupe de sécurité d'instance EC2, que vous avez créé dans l'exercice de mise en route, pour autoriser le trafic HTTP sur le port TCP 80 à partir de n'importe quel emplacement.

Une fois la règle ajoutée, le groupe de sécurité d'instance EC2 aura les règles entrantes suivantes.



Pour obtenir des instructions, veuillez consulter Création d'un groupe de sécurité à l'aide de la console.

b. Créez un exemple de fichier html.

i. Remplacez le répertoire par le point de montage.

```
$ cd /var/www/html/efs-mount-point
```

ii. Créez un sous-répertoire appelé `sampledir` et modifiez la propriété.

```
$  sudo mkdir sampledir
$  sudo chown  ec2-user sampledir
$  sudo chmod -R o+r sampledir
```

Modifiez également le répertoire afin de pouvoir créer des fichiers dans le sous-répertoire `sampledir`.

```
$  cd sampledir
```

iii. Créez un exemple de `hello.html` fichier.

```
$ echo "<html><h1>Hello from Amazon EFS</h1></html>" > hello.html
```

c. Ouvrez une fenêtre de navigateur et entrez l'URL permettant d'accéder au fichier (il s'agit du nom DNS public de l'instance EC2 suivi du nom du fichier). Par exemple :

```
http://EC2-instance-public-DNS/efs-mount-point/sampledir/hello.html
```

Vous distribuez maintenant des pages web stockées sur un système de fichiers Amazon EFS.

> **Note**
>
> Cette configuration ne configure pas l'instance EC2 pour un démarrage automatique de httpd (serveur web) et elle ne monte pas le système de fichiers à l'amorçage. Dans la procédure suivante, vous créez une configuration de lancement pour mettre tout cela en place.

Plusieurs instances EC2 pour la distribution des fichiers

Suivez ces étapes pour distribuer le même contenu sur votre système de fichiers Amazon EFS à partir de plusieurs instances EC2 pour une meilleure capacité de mise à l'échelle ou disponibilité.

1. Suivez les étapes de l'exercice Création rapide d'un système de fichiers doté de paramètres recommandés (console) afin de disposer d'un système de fichiers créé et testé.

   > **Important**
   >
   > Pour cette procédure, vous n'utilisez pas l'instance EC2 que vous avez créée dans l'exercice de mise en route. Au lieu de cela, vous lancez de nouvelles instances EC2.

2. Créez un équilibreur de charge dans votre VPC à l'aide de la procédure suivante.

   a. Définissez un équilibreur de charge

      Dans la section Basic Configuration (Configuration de base), sélectionnez votre VPC dans lequel vous créez également les instances EC2 sur lesquelles vous montez le système de fichiers.

      Dans la section Sélectionner les sous-réseaux, sélectionnez tous les sous-réseaux disponibles. Pour plus d'informations, consultez le script `cloud-config` dans la section suivante.

   b. Attribuez des groupes de sécurité

      Créer un nouveau groupe de sécurité pour l'équilibreur de charge afin d'autoriser l'accès HTTP du port 80 depuis n'importe où, comme illustré ci-après :

      - Type : HTTP
      - Protocole : TCP
      - Plage de ports: 80
      - Source : N'importe où (0.0.0.0/0)

      > **Note**
      >
      > Lorsque tout fonctionne, vous pouvez également mettre à jour l'accès de la règle entrante du groupe de sécurité d'instance EC2 afin d'autoriser le trafic HTTP uniquement à partir de l'équilibreur de charge.

   c. Configurez une vérification de l'état

Définissez la valeur Ping Path (Chemin de ping) sur `/efs-mount-point/test.html`. `efs-mount-point` est le sous-répertoire dans lequel le système de fichiers est monté. Vous y ajouterez la page `test.html` plus loin dans cette procédure.

> **Note**
>
> N"ajoutez aucune instance EC2. Plus tard, vous créerez un groupe Auto Scaling dans lequel vous lancerez l'instance EC2 et indiquerez cet équilibreur de charge.

Pour plus d'informations sur la création d'un équilibreur de charge, consultez Prise en main d'Elastic Load Balancing dans le Guide de l'utilisateur Elastic Load Balancing.

Créez un groupe Auto Scaling avec deux instances EC2. Tout d'abord, vous créez une configuration de lancement décrivant les instances. Ensuite, vous créez un groupe Auto Scaling en spécifiant la configuration de lancement. Les étapes suivantes fournissent des informations de configuration que vous spécifiez pour créer un groupe Auto Scaling à partir de la console Amazon EC2.

1. Choisissez Launch Configurations (Configurations de lancement) sous AUTO SCALING dans le volet de navigation de gauche.
2. Choisissez Créer le groupe Auto Scaling pour lancer l'assistant.
3. Choisissez Créer une configuration du lancement.
4. À partir de Quick Start, sélectionnez la dernière version de l'AMI Amazon Linux 2 Il s'agit de la même AMI que celle que vous avez utilisée à l'Créez votre système de fichiers EFS et lancez votre instance EC2 de l'exercice de mise en route.
5. Dans la section Advanced (Avancé), procédez comme suit :

   - En regard de IP Address Type (Type d'adresse IP), choisissez Assign a public IP address to every instance (Attribuer une adresse IP publique à chaque instance).
   - Copiez/collez le script suivant dans la zone User data (Données utilisateur).

     Vous devez mettre à jour le script en fournissant des valeurs pour *`file-system-id`* et *`aws-region`* (si vous avez suivi l'exercice de mise en route, vous avez créé le système de fichiers dans la région us-west-2).

Dans le script, notez les éléments suivants :

- Le script installe le client NFS et le serveur web Apache.
- La commande echo écrit l'entrée suivante dans le fichier `/etc/fstab` en identifiant le nom DNS du système de fichiers et le sous-répertoire dans lequel le monter. Cette entrée garantit que le fichier est monté après chaque redémarrage du système. Notez que le nom DNS du système de fichiers est créé de manière dynamique. Pour plus d'informations, consultez Montage sur Amazon EC2 avec un nom DNS.

```
file-system-ID.efs.aws-region.amazonaws.com:/ /var/www/html/efs-mount-point
 nfs4   defaults
```

- Créez un sous-répertoire `efs-mount-point` et montez le système de fichiers.
- Créez une page `test.html` pour que la surveillance de l'état ELB puisse trouver le fichier (lors de la création d'un équilibreur de charge, vous avez spécifié ce fichier en tant que le point de ping).

Pour plus d'informations sur les scripts de données utilisateur, consultez la section Métadonnées d'instance et données utilisateur.

```
#cloud-config
package_upgrade: true
packages:
- nfs-utils
- httpd
runcmd:
- echo "$(curl -s http://169.254.169.254/latest/meta-data/placement/availability-
zone).file-system-id.efs.aws-region.amazonaws.com:/    /var/www/html/efs-mount-
point   nfs4    defaults" >> /etc/fstab
- mkdir /var/www/html/efs-mount-point
- mount -a
- touch /var/www/html/efs-mount-point/test.html
- service httpd start
- chkconfig httpd on
```

6. En regard de Assign a security group (Attribuer un groupe de sécurité), choisissez Select an existing security group (Sélectionner un groupe de sécurité existant), puis choisissez le groupe de sécurité que vous avez créé pour l'instance EC2.
7. Maintenant, configurez les détails du groupe de mise à l'échelle automatique en utilisant les informations suivantes.

a. Pour Group size (Taille du groupe), choisissez **`Start with 2 instances`**. Vous allez créer deux instances EC2.

b. Sélectionnez votre VPC dans la liste Network (Réseau).

c. Sélectionnez un sous-réseau dans la même zone de disponibilité que vous avez utilisée lors de l'indication de l'ID cible de montage dans le script de données utilisateur lors de la création de la configuration de lancement à l'étape précédente.

d. Dans la section Détails avancés

i. En regard de Load Balancing (Équilibrage de charges), choisissez Receive traffic from Elastic Load Balancer(s) (Recevoir le trafic des Elastic Load Balancer(s)), puis sélectionnez l'équilibreur de charge que vous avez créé pour cet exercice.

ii. En regard de Health Check Type (Type de vérification de l'état), choisissez ELB.

8. Suivez les instructions pour créer un groupe Auto Scaling dans Configurer une application redimensionnée et à équilibreur de charge dans le Guide de l'utilisateur Amazon EC2 Auto Scaling. Utilisez les informations des tableaux précédents, le cas échéant.

9. Une fois le groupe Auto Scaling créé, vous disposez de deux instances EC2 avec `nfs-utils` et le serveur web Apache installé. Sur chaque instance, vérifiez que vous avez le sous-répertoire `/var/www/html/efs-mount-point` avec votre système de fichiers monté dans ce dernier. Pour obtenir des instructions sur la connexion à une instance EC2, consultez la section Connect to your Linux User Guide d'utilisation d'Amazon EC2.

> **Note**
>
> Si vous choisissez l'AMI Amazon Linux Amazon Linux AMI 2016.03.0 lors du lancement de votre instance Amazon EFS, vous n'avez pas besoin d'installer , car il est déjà inclus par défaut dans l'AMI.

10. Créez un exemple de page (index.html).

a. Changez de répertoire.

```
$ cd /var/www/html/efs-mount-point
```

b. Créez un sous-répertoire `sampledir` et modifiez la propriété. Modifiez également le répertoire afin de pouvoir créer des fichiers dans le sous-répertoire `sampledir`. Si vous

avez suivi la procédure précédente instance EC2 unique pour la distribution de fichiers, vous avez déjà créé le sous-répertoire `sampledir`, vous pouvez donc omettre cette étape.

```
$  sudo mkdir sampledir
$  sudo chown  ec2-user sampledir
$  sudo chmod -R o+r sampledir
$  cd sampledir
```

c. Créez un exemple de `index.html` fichier.

```
$ echo "<html><h1>Hello from Amazon EFS</h1></html>" > index.html
```

11. Vous pouvez maintenant tester la configuration. À l'aide du nom DNS public de l'équilibreur de charge, accédez à la page index.html.

```
http://load balancer public DNS Name/efs-mount-point/sampledir/index.html
```

L'équilibreur de charge envoie une requête à l'une des instances EC2 exécutant le serveur web Apache. Ensuite, le serveur web distribue le fichier qui est stocké sur votre système de fichiers Amazon EFS.

Procédure : Création de sous-répertoires par utilisateur accessibles en écriture et configuration d'un remontage au redémarrage automatique

Une fois que vous avez créé un système de fichiers Amazon EFS et que vous l'avez monté localement sur votre instance EC2, un répertoire vide appelé *racine du système de fichiers s'affiche*. Un cas d'utilisation courant consiste à créer un sous-répertoire « accessibles en écriture » sous la racine de ce système de fichiers pour chaque utilisateur que vous créez sur l'instance EC2 et de le monter dans le répertoire de base de l'utilisateur. Tous les fichiers et sous-répertoires créés par l'utilisateur dans son répertoire de base sont ensuite créés sur le système de fichiers Amazon EFS.

Dans cette procédure, vous commencez par créer un utilisateur « mike » sur votre instance EC2. Vous pouvez ensuite monter un sous-répertoire Amazon EFS dans le répertoire personnel de

l'utilisateur mike. La procédure explique également comment configurer un remontage automatique des sous-répertoires si le système redémarre.

Supposons qu'un système de fichiers Amazon EFS ait été créé et monté dans un répertoire local de votre instance EC2. Appelons-le *EFSroot*.

> **Note**
>
> Vous pouvez suivrePremiers pas cet exercice pour créer et monter un système de fichiers Amazon EFS sur votre instance EC2 vous devez vous connecter à votre instance EC2.

Dans les étapes suivantes, vous allez créer un utilisateur (mike), créer un sous-répertoire pour l'utilisateur (*EFSroot*/mike), faire de l'utilisateur mike le propriétaire du sous-répertoire, lui accorder des autorisations complètes, et enfin monter le sous-répertoire Amazon EFS dans le répertoire personnel de l'utilisateur (/home/mike).

1. Créez l'utilisateur mike :

   - Connectez-vous à votre instance EC2. À l'aide de privilèges racine (dans ce cas, à l'aide de la commande sudo), créez l'utilisateur mike et affectez-lui un mot de passe.

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

     Cette opération crée également un répertoire de base, /home/mike, pour l'utilisateur.

2. Créez un sous-répertoire sous *EFSroot* pour l'utilisateur mike :

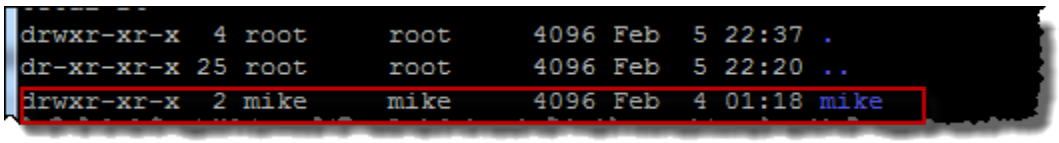
   a. Créez sous-répertoire mike sous *EFSroot*.

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

      Vous n'aurez pas à remplacer *EFSroot* par le nom de votre répertoire local.

   b. L'utilisateur racine et le groupe racine sont les propriétaires du sous-répertoire /mike (vous pouvez le vérifier en utilisant la commande ls -l). Pour activer toutes les autorisations pour l'utilisateur mike sur ce sous-répertoire, accordez à mike la propriété sur le répertoire.

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



3. Utilisez la commande `mount` pour monter le sous-répertoire *EFSroot*/mike dans le répertoire de base de mike.

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

   L'adresse *Mount-Target-DNS* identifie la racine du système de fichiers Amazon EFS distant.

Le répertoire personnel de l'utilisateur mike est désormais un sous-répertoire, inscriptible par mike, dans le système de fichiers Amazon EFS. Si vous démontez cette cible de montage, l'utilisateur ne peut pas accéder à son répertoire EFS sans un remontage, qui exige des autorisations racine.

Remontage automatique au redémarrage

Vous pouvez utiliser le fichier `fstab` pour remonter automatiquement votre système de fichiers après les redémarrages système. Pour plus d'informations, veuillez consulter Montage automatique de votre système de fichiers EFS Amazon.

Procédure : Créer et monter un système de fichiers sur site avec AWS Direct Connect et VPN

Cette procédure pas à pas utilise le AWS Management Console pour créer et monter un système de fichiers sur un client local. Pour ce faire, vous pouvez utiliser une AWS Direct Connect connexion ou une connexion sur un AWS Virtual Private Network (AWS VPN).

> **Note**
>
> L’utilisation d’Amazon EFS avec des clients basés sur Microsoft Windows n’est pas prise en charge.

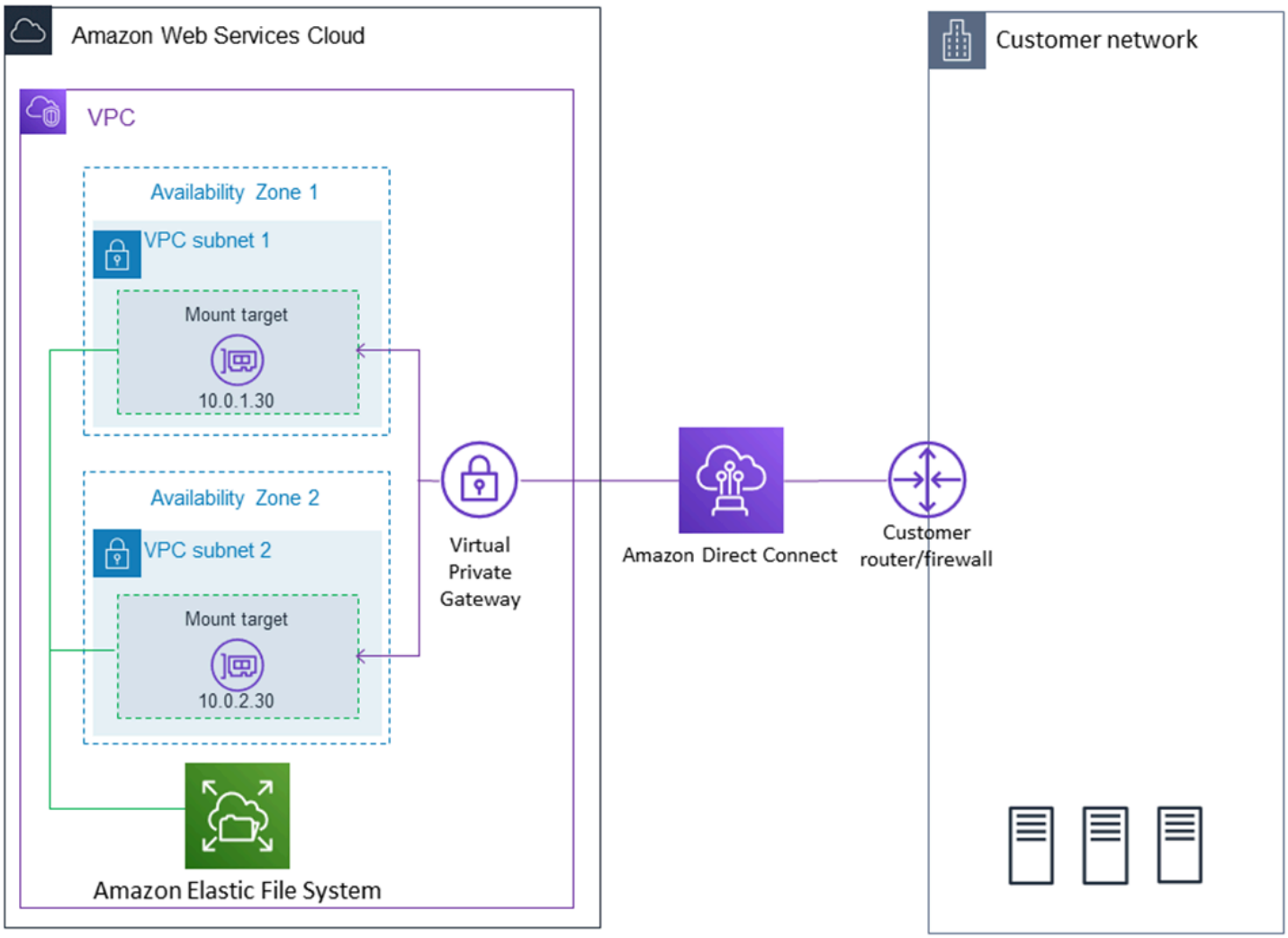
Rubriques

- Avant de commencer
- Étape 1 : créer vos ressources Amazon Elastic File System
- 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

Dans cette procédure pas à pas, nous partons du principe que vous disposez déjà d'une connexion VPN AWS Direct Connect ou d'une connexion VPN. Si ce n’est pas le cas, vous pouvez lancer le processus de connexion maintenant et revenir à cette procédure une fois votre connexion établie. Pour plus d'informations AWS Direct Connect, consultez le guide de AWS Direct Connect l'utilisateur. Pour plus d’informations sur la configuration d’une connexion VPN, consultez Connexions VPN dans le Guide de l’utilisateur Amazon VPC.

Lorsque vous disposez AWS Direct Connect d'une connexion VPN, vous créez un système de fichiers Amazon 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 recommandons la présence de deux clients sur site connectés à votre système de fichiers via différentes zones de disponibilité afin de bénéficier d'une plus grande disponibilité.

Avant de commencer

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, 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 :

- La passerelle Internet est attachée à votre VPC. Pour plus d'informations, consultez Passerelles Internet dans le Amazon VPC Guide de l'utilisateur.
- La table de routage VPC comprend une règle pour l'envoi de tout le trafic Internet entrant vers la passerelle Internet.

Étape 1 : créer vos ressources Amazon Elastic File System

Au cours de cette étape, vous allez créer votre système de fichiers Amazon EFS et monter les cibles.

Pour créer un système de fichiers Amazon EFS

1. Ouvrez la console Amazon EFS 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. Activez les cases à cocher de 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 choisi. Il s'agit de vos cibles de montage. Pour plus d'informations, consultez 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 console Amazon EC2 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 : créer vos ressources Amazon Elastic File System.
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.

   Example

   ```
   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

le terminal comme `ping` sur l'adresse IP de vos instances EC2 dans des zones de disponibilité différentes pour trouver celle avec 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,wsize=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 modifiez la propriété de ce sous-répertoire pour votre utilisateur de l'instance EC2. 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 plus d'informations, consultez Montage automatique de votre système de fichiers EFS Amazon.

> **Warning**
>
> Utilisez l'option `_netdev`, utilisée pour identifier les systèmes de fichiers réseau lors du montage automatique de votre système de fichiers. Si l'option `_netdev` est manquante, votre instance EC2 peut cesser 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 plus d'informations, consultez 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 à l'adresse https://console.aws.amazon.com/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 console Amazon EC2 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 amazon-efs-utils package est une collection open source 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 des outils 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 outil 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.

   Example

   ```
   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 le terminal comme `ping` sur l'adresse IP de vos instances EC2 dans des zones de disponibilité différentes pour trouver celle avec 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
  ```

  Example

  ```
  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.

   Example

   ```
   mkdir ~/efs
   ```

2. Exécutez la commande mount pour monter le système de fichiers.

   Example

   ```
   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 :

   Example

   ```
   sudo mount -t efs -o tls fs-12345678 ~/efs
   ```

Procédure : montage d'un système de fichiers à partir d'un autre VPC

Dans cette procédure, vous allez configurer une instance pour monter un système de fichiers qui se trouve dans un cloud privé virtuel (VPC) différent. 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 des outils 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 de VPC ou une passerelle de transit pour connecter les VPC, les instances Amazon EC2 dans un VPC peuvent accéder aux systèmes de fichiers EFS d'un autre VPC, même si les VPC appartiennent à des comptes différents.

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

Rubriques

- Avant de commencer
- Étape 1 : Déterminer l'ID de zone de disponibilité de la cible de montage EFS
- Étape 2 : Déterminer l'adresse IP de la cible de montage
- Étape 3 : Ajouter une entrée hôte pour la cible de montage
- Étape 4 : Monter votre système de fichiers à l'aide de l'assistant de montage EFS
- Étape 5 : Nettoyer les ressources et protéger votre compte AWS

Avant de commencer

Dans cette procédure, nous supposons que vous disposez déjà des éléments suivants :

- L'ensemble d'outils `amazon-efs-utils` est installé sur l'instance EC2 avant d'utiliser cette procédure. Pour obtenir des instructions sur l'installation de l'ensemble d'outils `amazon-efs-utils`, veuillez consulter Installation des outils Amazon EFS.
- L'un des éléments suivants :
  - Connexion d'appairage de VPC entre le VPC où se trouve le système de fichiers EFS et le VPC où se trouve l'instance EC2. Une connexion d'appairage de VPC est une connexion de mise en réseau entre deux VPC. Ce type de connexion permet d'acheminer le trafic entre ces derniers à l'aide d'adresses IPv4 (Internet Protocol version 4) ou IPv6 (Internet Protocol version 6) privées. Vous pouvez utiliser le peering VPC pour connecter des VPC au sein d'un même Région AWS ou entre eux. Région 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 connectant le VPC où se trouve le système de fichiers EFS et le VPC où se trouve l'instance EC2. Une passerelle de transit est un hub de transit de réseau que vous pouvez utiliser pour relier votre VPC et vos réseaux sur site. Pour en savoir plus, consultez Mise en route avec les passerelles de transit dans le Guide des passerelles de transit Amazon VPC.

Étape 1 : Déterminer l'ID de zone de disponibilité de la cible de montage EFS

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. Cette exigence s'applique en raison des noms de zone de disponibilité qui peuvent différer selon les comptes.

Pour déterminer l'ID de la zone de disponibilité de l'instance EC2

1. Connectez-vous à votre instance EC2 :

   - Pour vous connecter à votre instance à partir d'un ordinateur exécutant macOS ou Linux, spécifiez le fichier .pem dans votre commande SSH. Pour ce faire, utilisez l'option `-i` et le chemin d'accès à votre clé privée.
   - Pour vous connecter à votre instance depuis un ordinateur exécutant Windows, vous pouvez utiliser l'un MindTerm ou l'autre des systèmes PuTTY. Pour utiliser PuTTY, installez-le et convertissez le fichier .pem en fichier .ppk.

   Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur Amazon EC2 :

   - Connectez-vous à votre instance Linux depuis Linux ou macOS via SSH
   - Connectez-vous à votre instance Linux depuis Windows avec PuTTY

2. Déterminez l'ID de la zone de disponibilité dans laquelle se trouve l'instance EC2 à l'aide de la commande d'interface de ligne de commande `describe-availability-zones`, 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`établissement,`use2-az2`.

Étape 2 : Déterminer l'adresse IP de la cible de montage

Maintenant que vous connaissez l'ID de zone de disponibilité de l'instance EC2, vous pouvez récupérer l'adresse IP de la cible de montage qui possède 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 hôte pour la cible de montage

Vous pouvez à présent créer une entrée dans le fichier `/etc/hosts` sur l'instance EC2 qui mappe l'adresse IP de la cible de 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 de la cible de montage dans le fichier `/etc/hosts` de l'instance EC2. 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 pour l'instance EC2 et la cible de montage disposent de règles autorisant l'accès au système EFS, selon les besoins. Pour plus d'informations, consultez Utilisation de groupes de sécurité VPC pour les instances Amazon EC2 et les cibles de montage.

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 commencer par créer un répertoire de montage sur l'instance EC2. Ensuite, à l'aide de l'assistant de montage EFS, vous pouvez monter le système de fichiers avec une autorisation IAM ou un point d'accès EFS. Pour plus d'informations, consultez Utilisation d'IAM pour contrôler l'accès aux données du système de fichiers et Utilisation des points d'accès Amazon EFS.

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 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 ~/mnt/efs
```

2. Créez un sous-répertoire et modifiez la propriété de ce sous-répertoire pour votre utilisateur de l'instance EC2. 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 plus d'informations, consultez Utilisation de `/etc/fstab` avec l'assistant de Montage EFS pour remonter automatiquement les systèmes de fichiers EFS.

> **Warning**
>
> Utilisez l'option `_netdev`, utilisée pour identifier les systèmes de fichiers réseau lors du montage automatique de votre système de fichiers. Si l'option `_netdev` est manquante, votre instance EC2 peut cesser 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 plus d'informations, consultez Le montage automatique échoue et l'instance ne répond pas.

Étape 5 : 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, assurez-vous de suivre les étapes ci-après. Cela nettoie vos ressources et protège 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 à l'adresse https://console.aws.amazon.com/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 console Amazon EC2 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.

Procédure : Application du chiffrement sur un système de fichiers Amazon EFS au repos

Vous trouverez ci-après des informations sur la façon d'appliquer le chiffrement au repos à l'aide d'Amazon CloudWatch etAWS CloudTrail. Cette procédure est basée sur leAWSlivre blancChiffrer les données au repos avec Amazon EFS Encrypted File Systems.

> **Note**
>
> La méthode d'application de la création de systèmes de fichiers Amazon EFS chiffrés au repos décrite dans cette procédure est obsolète. La méthode préférée pour appliquer la création de systèmes de fichiers chiffrés au repos consiste à utiliser`elasticfilesystem:Encrypted`Clé de condition dansAWS Identity and Access ManagementStratégies basées sur l'identité. Pour plus d'informations, consultez Exemple : imposer la création de systèmes de fichiers chiffrés. Vous pouvez utiliser cette procédure pas à pas pour créer des alarmes CloudWatch afin de vérifier que vos stratégies IAM empêchent la création de systèmes de fichiers non chiffrés.

Application du chiffrement au repos

Votre organisation peut exiger le chiffrement au repos de toutes les données qui répondent à une classification spécifique ou qui sont associées à une application, une charge de travail ou un environnement spécifiques. Vous pouvez appliquer des stratégies pour le chiffrement de données au repos pour les systèmes de fichiers Amazon EFS à l'aide de contrôles de détection. Ces contrôles détectent la création d'un système de fichiers et vérifient que le chiffrement au repos est activé.

Si un système de fichiers qui ne possède pas de chiffrement au repos est détecté, vous pouvez répondre d'un certain nombre de façons. Celles-ci vont de la suppression du système de fichiers et des cibles de montage à la notification d'un administrateur.

Si vous souhaitez supprimer un système de fichiers au repos non chiffré, mais que vous souhaitez conserver les données, vous devez d'abord créer un nouveau système de fichiers chiffrés au repos. Ensuite, copiez les données vers le nouveau système de fichiers chiffrés au repos. Une fois que les données sont copiées, vous pouvez supprimer le système de fichiers non chiffrés au repos.

Détection de systèmes de fichiers non chiffrés au repos

Vous pouvez créer une alarme CloudWatch pour surveiller les journaux CloudTrail pour`CreateFileSystem`event. Vous pouvez ensuite déclencher l'alarme pour informer un administrateur si le système de fichiers qui a été créé a été chiffré au repos.

Créer un filtre de métrique

Pour créer une alarme CloudWatch qui se déclenche lorsqu'un système de fichiers Amazon EFS non chiffrés est créé, utilisez la procédure suivante.

Avant de commencer, vous devez avoir créé un journal d'activité qui envoie les journaux CloudTrail à un groupe de journaux CloudWatch Logs. Pour de plus amples informations, veuillez consulterEnvoi d'événements à CloudWatch Logsdans leAWS CloudTrailGuide de l'utilisateur.

Pour créer un filtre de métrique

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Logs (Journaux).
3. Dans la liste des groupes de journaux, choisissez le groupe de journaux que vous avez créé pour les événements de journaux CloudTrail.

4. Choisissez Create Metric Filter.
5. Sur la page Define Logs Metric Filter (Définir le filtre des métriques de journaux), choisissez Filter Pattern (Modèle de filtre), puis saisissez ce qui suit :

```
{ ($.eventName = CreateFileSystem) && ($.responseElements.encrypted IS FALSE) }
```

6. Choisissez Assign Metric (Affecter une métrique).
7. Pour Nom du filtre, tapez **`UnencryptedFileSystemCreated`**.
8. Dans Metric Namespace (Espace de noms de la métrique), saisissez **`CloudTrailMetrics`**.
9. Dans Metric Name (Nom de la métrique), saisissez **`UnencryptedFileSystemCreatedEventCount`**.
10. Choisissez Show advanced metric settings.
11. Dans Valeur de métriques, tapez **`1`**.
12. Choisissez Create Filter (Créer un filtre).

Créer une alarme

Une fois que vous avez créé le filtre de métrique, suivez cette procédure pour créer une alarme.

Pour créer une alarme

1. Sous Filtres pour la page Log_Group_Name, à côté du nom du filtre UnencryptedFileSystemCreated, choisissez Créer une alarme.
2. Sur la page Créer une alarme, définissez les paramètres suivants :
   - Pour Nom, tapez **`Unencrypted File System Created`**
   - Pour Lorsque :, procédez comme suit :
     - Définissez est sur *`> =1`*.
     - Définissez for: (pour :) sur *`1`* période consécutive.
   - Pour Traiter les données manquantes comme, choisissez correctes (seuil non dépassé).
   - Pour Actions, procédez comme suit :
     - Pour Whenever this alarm (Chaque fois que cette alarme), sélectionnez State is ALARM (L'état est ALARME).
     - Pour Envoyer les notifications à, choisissez NotifyMe, choisissez Nouvelle liste, puis tapez un nom de rubrique unique pour la liste.

- Dans Liste des adresses e-mail, saisissez l'adresse e-mail où vous souhaitez que les notifications soient envoyées. Vous recevrez un e-mail à cette adresse afin de confirmer que vous avez créé cette alarme.
- Pour Aperçu de l'alarme, procédez comme suit :
  - Pour Période, choisissez 1 Minute.
  - Pour Statistiques, choisissez Standard et Somme.

3. Choisissez Create Alarm (Créer l'alarme).

Test de l'alarme pour la création de systèmes de fichiers non chiffrés

Vous pouvez tester l'alarme en créant un système de fichiers au repos non chiffrés, comme suit.

Pour tester l'alarme en créant un système de fichiers au repos non chiffrés

1. Connectez-vous àAWS Management Consoleet ouvrez la console Amazon EFS à l'adressehttps://console.aws.amazon.com/efs/.
2. ChoisissezCréez un système de fichierspour afficherCréez un système de fichiersboîte de dialogue.
3. Pour créer un système de fichiers non chiffré au repos, choisissezPersonnaliser l'pour afficherParamètres du système de fichiers.
4. PourGénéral, entrez ce qui suit.
   a. (Facultatif) Entrez unNompour le système de fichiers.
   b. KeepGestion des cycles de vie,Mode de performances, etMode de débitDéfinissez les valeurs par défaut.
   c. DésactiverChiffrementpar dédouanementActivation du chiffrement de données au repos.
5. ChoisissezSuivantpour continuer àAccès réseauétape du processus de configuration.
6. Choisissez la valeur par défautVirtual Private Cloud (VPC).
7. PourFixation de cibles, choisissez la valeur par défautGroupes de sécuritéPour chaque cible de montage.
8. ChoisissezSuivantpour afficherStratégie de système de fichiers.
9. ChoisissezSuivantpour continuer àVérifier et créer.
10. Passez en revue le système de fichiers et choisissezCréerpour créer votre système de fichiers et revenir à la pageSystèmes de fichiers.

Votre journal de suivi consigne`CreateFileSystem`et transmet l'événement à votre groupe de journaux CloudWatch Logs. L'événement déclenche votre alarme de métrique et CloudWatch Logs vous envoie une notification à propos de la modification.

Procédure pas à pas : activer le root squashing à l'aide de l'autorisation IAM pour les clients NFS

Dans cette procédure pas à pas, vous allez configurer Amazon EFS pour empêcher l'accès root à votre système de fichiers Amazon EFS pour tous lesAWS principaux utilisateurs, à l'exception d'un seul poste de gestion. Pour ce faire, configurez l'autorisationAWS Identity and Access Management (IAM) pour les clients NFS (Network File System). Pour plus d'informations sur l'autorisation IAM pour les clients NFS dans EFS, consultez Utilisation d'IAM pour contrôler l'accès aux données du système de fichiers.

Pour ce faire, vous devez configurer deux politiques d'autorisations IAM, comme suit :

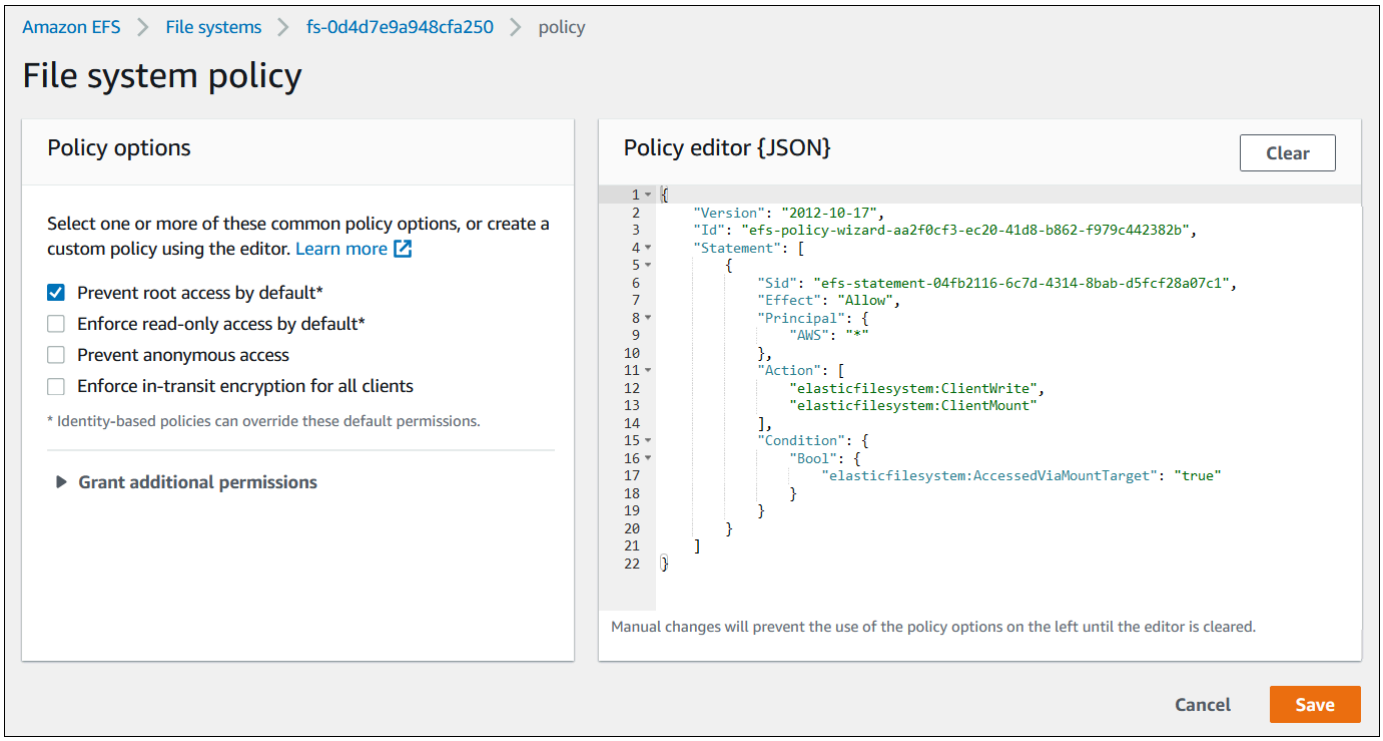
- Créez une stratégie de système de fichiers EFS qui autorise explicitement l'accès en lecture et en écriture au système de fichiers et qui refuse implicitement l'accès racine.
- Attribuez une identité IAM à la station de travail de gestion Amazon EC2 qui nécessite un accès root au système de fichiers à l'aide d'un profil d'instance Amazon EC2. Pour plus d'informations sur les profils d'instance Amazon EC2, consultez la section Utilisation des profils d'instance dans le guide deAWS Identity and Access Management l'utilisateur.
- Attribuez la stratégie gérée par AWS `AmazonElasticFileSystemClientFullAccess` au rôle IAM de la station de travail de gestion. Pour plus d'informations sur les politiquesAWS gérées pour EFS, consultezGestion des identités et des accès pour Amazon Elastic File System.

Pour activer l'écrasement racine à l'aide de l'autorisation IAM pour les clients NFS, procédez comme suit.

Pour empêcher l'accès root au système de fichiers

1. Ouvrez la console Amazon Elastic File System à l'adresse https://console.aws.amazon.com/efs/.
2. Choisissez Filesystems.
3. Sélectionnez le système de fichiers sur lequel vous souhaitez activer l'écrasement racine sur la page Systèmes de fichiers.

4. Sur la page de détails du système de fichiers, choisissez Politique du système de fichiers, puis choisissez Modifier. La page File system policy (Stratégie du système de fichiers) s'affiche.



5. Choisissez Empêcher l'accès root par défaut* sous Options de politique. L'objet JSON de stratégie apparaît dans l'éditeur de politiques.
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 politique`AmazonElasticFileSystemClientFullAccess` gérée au rôle du poste de travail, IAM accorde un accès root au poste de travail en fonction de sa politique 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. création d'un rôle pour Amazon EC2 appelé`EFS-client-root-access`. IAM crée un profil d'instance portant le même nom que le rôle EC2 que vous avez créé.
3. Affectez la stratégie géré par AWS `AmazonElasticFileSystemClientFullAccess` au rôle EC2 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'instance EC2 que vous utilisez comme station de travail de gestion, comme décrit ci-dessous. Pour plus d'informations, veuillez consulter les informations relatives à l'attachement d'un rôle IAM à une instance dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

   a. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.

   b. Dans le panneau de navigation, sélectionnez 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, consultezInstallation des outils 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'instance Amazon EC2 pour monter automatiquement le système de fichiers avec une autorisation IAM. Pour plus d'informations sur le montage d'un système de fichiers EFS avec une autorisation IAM, consultezMontage avec autorisation IAM.

Sécurité 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.
- 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 140-2 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 (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

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 Name (Nom). Cela inclut lorsque vous travaillez avec EFS ou d'autres entités à Services

AWS l'aide de la console, de l'API ou des AWS kits de développement logiciel. 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 Elastic File System
- Utilisation d'IAM pour contrôler l'accès aux données du système de fichiers
- Contrôle de l'accès réseau aux systèmes de fichiers Amazon EFS pour les clients NFS
- Utilisation des utilisateurs, des groupes et des autorisations au niveau du système de fichiers réseau (NFS)
- Utilisation des points d'accès Amazon EFS
- Blocage de l'accès public aux systèmes de fichiers Amazon 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 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 (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.

Chiffrement de données au repos

Vous pouvez créer des systèmes de fichiers chiffrés à l'aide du AWS Management Console AWS CLI, du ou par programmation via l'API Amazon EFS ou l'un des SDK. AWS 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 Amazon 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 (SCP) 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. La procédure suivante décrit comment activer le chiffrement pour un nouveau système de fichiers lorsque vous le créez à partir de la console.

> **Note**
>
> Le chiffrement au repos n’est pas activé par défaut lors de la création d’un nouveau système de fichiers à l’aide de AWS CLI, l’API et des SDK. Pour plus d’informations, consultez Création d'un système de fichiers (AWS CLI).

Pour chiffrer un nouveau système de fichiers à l’aide de la console EFS

1. Ouvrez la console Amazon Elastic File System 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 :

   - Le chiffrement des données au repos est activé à l'aide de votre option par défaut AWS KMS key pour Amazon EFS (`aws/elasticfilesystem`).
   - Sauvegardes automatiques activées - Pour plus d’informations, consultez Sauvegarde de vos systèmes de fichiers Amazon EFS.
   - Cibles de montage : Amazon EFS crée des cibles de montage avec les paramètres suivants :
     - Situé dans chaque zone de disponibilité dans Région AWS laquelle le système de fichiers est créé.
     - Situé dans les sous-réseaux par défaut du VPC que vous avez sélectionné.
     - Utiliser le groupe de sécurité par défaut du VPC. Vous pouvez gérer les groupes de sécurité une fois le système de fichiers créé.

   Pour plus d’informations, consultez Gestion de l’accessibilité réseau du système de fichiers.

- Mode performance à usage général — Pour plus d'informations, consultez Modes de performances.
- Débit élastique – Pour plus d'informations, consultez Modes de débit.
- Gestion du cycle de vie activée avec une stratégie à 30 jours — Pour plus d'informations, consultez Gestion du stockage du système de fichiers.

6. 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.

Vous disposez désormais d'un nouveau système de encrypted-at-rest fichiers.

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 de plus amples informations, consultez Principes de base du chiffrement dans le AWS Key Management Service Guide du développeur.

Comment Amazon EFS utilise 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 Amazon EFS Clé gérée par AWS pour chiffrer et déchiffrer les métadonnées du système de fichiers (c'est-à-dire les noms de fichiers, les noms de répertoire et le contenu des répertoires). `aws/elasticfilesystem`
- 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 plus d'informations, consultez Gestion de l'accès à la clé KMS pour un système de fichiers.

> **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 identifiants de AWS compte spécifiques à Amazon EFS apparaissent dans vos AWS CloudTrail journaux relatifs aux AWS KMS actions. Pour plus d'informations, consultez 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 KMSdans le AWS Key Management Service Guide du développeur. La liste suivante décrit toutes les autorisations AWS KMS associées 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 : GenerateData KeyWithout Plaintext — (Obligatoire) Renvoie une clé de chiffrement des données chiffrée sous une clé gérée par le client. Cette autorisation est incluse dans la politique de clé par défaut sous kms : GenerateData Key*.
- 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 octrois, consultez Utilisation d'octrois dans le AWS Key Management Service Guide du 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) Répertorie 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 des données en transit

L'activation du chiffrement des données en transit pour votre système de fichiers Amazon EFS s'effectue en activant le protocole TLS (Transport Layer Security) lors du montage de votre système de fichiers à l'aide de l'assistant de montage Amazon EFS. Pour plus d'informations, consultez Utilisation de l'assistant de Montage EFS pour Monter les systèmes de fichiers 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.

Pour monter votre système de fichiers Amazon EFS avec l’assistant de montage en ayant préalablement activé le chiffrement des données en transit

1. Accédez au terminal pour votre instance via SSH (Secure Shell) et connectez-vous avec le nom d’utilisateur approprié. Pour plus d'informations sur la procédure à suivre, voir Se connecter à votre instance Linux depuis Linux ou macOS à l'aide de SSH.
2. Exécutez la commande suivante pour Monter votre système de fichiers.

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

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 Amazon 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 Amazon EFS à l'aide de TLS échoue.
>
> Après avoir installé le amazon-efs-utils package, pour mettre à niveau la version de Stunnel de votre système, consultezMise 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,wsize=1048576,namlen=255,hard,proto=tcp,port=20127,timeo=6
```

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 connaître l'ID du système de fichiers Amazon EFS correspondant au 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 chaque processus stunnel de montage est en cours d'exécution et arrête le stunnel lorsque le système de fichiers Amazon 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
- Impossible de créer le système de ncrypted-at-rest fichiers E
- 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 plus d'informations, consultez 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 plus d'informations, consultez 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.

Impossible de créer le système de ncrypted-at-rest fichiers E

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 Elastic File System

AWS Identity and Access Management (IAM) est un Service AWS qui aide un administrateur à contrôler en toute sécurité l'accès aux ressources AWS. 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 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 Elastic File System
- Politiques gérées par AWS pour Amazon EFS
- Utilisation de 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

Votre utilisation de AWS Identity and Access Management (IAM) diffère selon la tâche que vous accomplissez 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 souhaiterez 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 correspond au processus par lequel vous vous connectez à AWS avec vos informations d'identification. Vous devez vous authentifier (être connecté à AWS) en tant qu'Utilisateur racine d'un compte AWS, en tant qu'utilisateur IAM ou en endossant un rôle IAM.

Vous pouvez vous connecter à AWS en tant qu'identité fédérée à l'aide des 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 en utilisant la fédération, vous endossez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter à la AWS Management Console ou au portail d'accès AWS. Pour plus d'informations sur la connexion à AWS, consultez Connexion à votre Compte AWSdans le Guide de l'utilisateurConnexion à AWS.

Si vous accédez à AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes en utilisant vos informations d'identification. Si vous n'utilisez pas les outils AWS, vous devez signer les requêtes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez Signature des demandes d'API AWS 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, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Utilisateur root Compte AWS

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée utilisateur root du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide de l'adresse électronique et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

Demandez aux utilisateurs humains, et notamment aux utilisateurs qui nécessitent un accès administrateur, d'appliquer la bonne pratique consistant à utiliser une fédération avec fournisseur d'identité pour accéder à Services AWS en utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, l'AWS Directory Service, l'annuaire Identity Centerou tout utilisateur qui accède à Services AWS en utilisant des informations d'identification fournies via une source d'identité. Quand des identités fédérées accèdent à Comptes AWS, elles endossent des rôles, ces derniers fournissant 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 connecter et vous synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité pour une utilisation sur l'ensemble de vos applications et de vos Comptes AWS. 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 dans votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou 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 tels que les 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 de faire pivoter les 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des 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 en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une entité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un rôle IAM dans la AWS Management Console en changeant de rôle. Vous pouvez obtenir un rôle en appelant une opération d'API AWS CLI ou AWS à l'aide d'une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM 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, certains Services AWS vous permettent d'attacher une politique directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès interservices : 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, une fonction de service ou un rôle lié au service.
  - Sessions de transmission d'accès (FAS) : lorsque vous vous servez d'un utilisateur ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un principal. 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 un Service AWS, associées au Service AWS demandeur pour adresser des demandes aux services situés en aval. Les demandes FAS ne sont formulées que lorsqu'un service reçoit une demande qui, pour aboutir, a besoin d'interagir avec d'autres ressources ou Services AWS. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

- Fonction du 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 une fonction du 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 au service – Un rôle lié au service est un type de fonction du service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications s'exécutant sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant des demandes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez les accès dans AWS en créant des politiques et en les attachant à des identités AWS ou à des ressources. Une politique est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit les autorisations de ces dernières. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou séance de rôle) envoie une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont

stockées dans AWS en tant que documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Présentation des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques JSON AWS 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 avec cette politique peut obtenir des informations utilisateur à partir de la AWS Management Console, de la AWS CLI ou de l'API AWS.

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 Création de politiques IAM 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 attacher à plusieurs utilisateurs, groupes et rôles dans votre Compte AWS. Les politiques gérées incluent les politiques gérées par AWS 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. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. 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 des Services AWS.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques gérées AWS depuis IAM dans une politique basée sur une ressource.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3, AWS WAF et Amazon VPC sont des exemples de services prenant en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes 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 courantes. 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 qui en résultent 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 remplace 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 (SCP) - les SCP sont des politiques JSON qui spécifient le nombre maximal d'autorisations pour une organisation ou une unité d'organisation (OU) dans AWS

Organizations. AWS Organizations est un service qui vous permet de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. La SCP limite les autorisations pour les entités dans les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations.

- 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 la séance obtenue 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 remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de stratégies, veuillez consulter Logique d'évaluation de stratégies 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

Fonctionnalité IAM	Support Amazon EFS
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Amazon EFS et d'autres services AWS fonctionnent avec IAM, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Amazon EFS

Prend en charge les politiques basées sur une 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 Groupes d'utilisateurs IAM 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 Création de politiques IAM 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 IAM 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 une ressource	Oui

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. 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 des 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 entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Quand le principal et la ressource se trouvent dans des Comptes AWS différents, un administrateur IAM dans le compte approuvé doit également accorder à l'entité principal (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 Différence entre les rôles IAM et les politiques basées sur une ressource 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 d'IAM pour contrôler l'accès aux données du système

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 Elastic File System.

Actions de politique pour Amazon EFS

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS 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 politique possèdent généralement le même nom que l'opération d'API AWS 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 politique 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 JSON AWS 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 afficher la liste des types de ressources Amazon EFS et de leurs ARN, consultez Ressources définies par Amazon Elastic File System dans la Référence de l'autorisation de service. 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

Prise en charge des clés de condition de stratégie spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS 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 opération `OR` 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 à un service. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globale AWS 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.

ACL dans Amazon EFS

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès 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)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés étiquettes. Vous pouvez attacher des étiquettes à des entités IAM (utilisateurs ou rôles), ainsi qu'à de nombreuses ressources AWS. 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 balises, vous devez fournir les informations de balise 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 l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (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 quand vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les Services AWS qui fonctionnent avec des informations d'identification temporaires, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires quand vous vous connectez à la AWS Management Console en utilisant toute méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS en utilisant le lien d'authentification unique (SSO) de votre société, 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 Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide d'AWS CLI ou de l'API AWS. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder à AWS. AWS recommande de générer des informations d'identification temporaires de façon dynamique 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 transmissions de sessions d'accès (FAS)	Oui

Lorsque vous vous servez d'un utilisateur IAM ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un principal. Lorsque vous utilisez certains services, l'action que vous effectuez est susceptible de lancer une autre action dans un autre service. FAS utilise les autorisations du principal appelant un Service AWS, associées au Service AWS demandeur pour adresser des demandes aux services situés en aval. Les demandes FAS ne sont formulées que lorsqu'un service reçoit une demande qui, pour aboutir, a besoin d'interagir avec d'autres ressources ou Services AWS. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives à l'envoi de demandes FAS, consultez Transférer les sessions d'accès.

Fonctions du service pour Amazon EFS

Prend en charge les fonctions du service	Oui

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du 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 à un service.	Oui

Un rôle lié à un service est un type de fonction du service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le 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 exécuter des tâches à l'aide de la AWS Management Console, de l'AWS Command Line Interface (AWS CLI) ou de l'API AWS. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM doit 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 dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Amazon EFS, y compris le format des ARN pour chacun des types de ressources, consultez Actions, ressources et clés de condition pour Amazon Elastic File System dans la Référence de l'autorisation de service.

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 :

- Démarrer avec AWS gérées et évoluez vers les autorisations de moindre privilège - Pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les politiques gérées AWS qui accordent des autorisations dans de nombreux cas d'utilisation courants. Elles sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client AWS qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder 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.
- Utiliser 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 via un Service AWS spécifique, comme

AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer 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 politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Authentification multifactorielle (MFA) nécessaire : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root dans votre Compte AWS, activez l'authentification multifactorielle pour une sécurité renforcée. Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par 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 consulter des informations sur les ressources Amazon EFS dans votre Compte AWS. Si vous créez une stratégie 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 stratégie.

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des appels uniquement à AWS CLI ou à l'API AWS. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour vous assurer que les utilisateurs et les rôles peuvent continuer à utiliser la console Amazon SNS, attachez également la politique Amazon SNS ou la politique gérée par Amazon EFS `AmazonElasticFileSystemReadOnlyAccess` AWS 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 Politiques gérées par AWS 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 nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou de l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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 AWS Management Console, AWS CLI, ou API AWS 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 AWS Management Console, AWS CLI, ou API AWS 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 services (SCP) AWS Organizations. Pour plus d'informations sur les politiques de contrôle des services dans AWS Organizations, consultez Politiques de contrôle des services dans le AWS OrganizationsGuide de l'utilisateur.

Exemples de politiques basées sur les ressources pour Amazon Elastic File System

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 rôle AWS spécifique
- Exemple : Accorder l'accès en lecture seule
- Exemple : Accorder l'accès à un point d'accès EFS

Exemple : accorder un accès en lecture et en écriture à un rôle AWS 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 Procédure pas à pas : activer le root squashing à l'aide de l'autorisation IAM pour les clients NFS.

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 Amazon EFS.

```
{
```

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

Politiques gérées par AWS pour Amazon EFS

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS 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.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont spécifiques à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWSpolitique gérée : AmazonElasticFileSystemFullAccess

Vous pouvez associer la politique `AmazonElasticFileSystemFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent à un d'accéder pleinement à Amazon EFS et aux services AWS 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 de AWS Backup.
- `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 (VPC) et les attributs VPC associés à un système de fichiers Amazon 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricData",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs",
                "ec2:ModifyNetworkInterfaceAttribute",
                "elasticfilesystem:Backup",
```

```
                "elasticfilesystem:CreateFileSystem",
                "elasticfilesystem:CreateMountTarget",
                "elasticfilesystem:CreateTags",
                "elasticfilesystem:CreateAccessPoint",
                "elasticfilesystem:CreateReplicationConfiguration",
                "elasticfilesystem:DeleteFileSystem",
                "elasticfilesystem:DeleteMountTarget",
                "elasticfilesystem:DeleteTags",
                "elasticfilesystem:DeleteAccessPoint",
                "elasticfilesystem:DeleteFileSystemPolicy",
                "elasticfilesystem:DeleteReplicationConfiguration",
                "elasticfilesystem:DescribeAccountPreferences",
                "elasticfilesystem:DescribeBackupPolicy",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeFileSystemPolicy",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeMountTargetSecurityGroups",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticfilesystem:DescribeTags",
                "elasticfilesystem:DescribeAccessPoints",
                "elasticfilesystem:ModifyMountTargetSecurityGroups",
                "elasticfilesystem:PutAccountPreferences",
                "elasticfilesystem:PutBackupPolicy",
                "elasticfilesystem:PutLifecycleConfiguration",
                "elasticfilesystem:PutFileSystemPolicy",
                "elasticfilesystem:UpdateFileSystem",
                "elasticfilesystem:UpdateFileSystemProtection",
                "elasticfilesystem:TagResource",
                "elasticfilesystem:UntagResource",
                "elasticfilesystem:ListTagsForResource",
                "elasticfilesystem:Restore",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],

            "Sid": "ElasticFileSystemFullAccess",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Sid": "CreateServiceLinkedRoleForEFS",
            "Effect": "Allow",
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "elasticfilesystem.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

AWSpolitique gérée : AmazonElasticFileSystemReadOnlyAccess

Vous pouvez associer la politique `AmazonElasticFileSystemReadOnlyAccess` à vos identités IAM.

Cette politique accorde un accès en lecture seule à Amazon EFS via 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, les VPC et leurs attributs dans la console Amazon EFS.
- `kms` – Permet aux mandants de répertorier les alias des clés AWS KMS dans la console Amazon EFS.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricData",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs",
                "elasticfilesystem:DescribeAccountPreferences",
                "elasticfilesystem:DescribeBackupPolicy",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeFileSystemPolicy",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeMountTargetSecurityGroups",
                "elasticfilesystem:DescribeTags",
                "elasticfilesystem:DescribeAccessPoints",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticfilesystem:ListTagsForResource",
                "kms:ListAliases"
            ],

            "Resource": "*"
        }
    ]
}
```

AWSpolitique gérée : AmazonElasticFileSystemClientReadWrite Accès

Vous pouvez attacher la politique `AmazonElasticFileSystemClientReadWriteAccess` à une entité IAM.

Cette politique accorde aux clients un accès en lecture et en écriture à un système de fichiers Amazon EFS. Cette politique permet aux clients NFS de monter, de lire et d'écrire sur les systèmes de fichiers Amazon EFS.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:DescribeMountTargets"
            ],
            "Resource": "*"
        }
    ]
}
```

Mises à jour Amazon EFS pour les politiques gérées par AWS

Affichez les détails des mises à jour des politiques gérées par AWS pour Amazon EFS depuis que ce service a commencé à assurer le suivi des 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	Politique : AmazonElasticFileSystemFullAccess Amazon EFS a ajouté une nouvelle autorisat ion 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
Mise à jour d'une stratégie existante	Politique : AmazonElasticFileSystemServiceRolePo licy Amazon EFS a ajouté de nouvelles autorisations pour permettre aux principaux de créer, de décrire et de supprimer des réplications Amazon EFS, ainsi que de créer des systèmes de fichiers Amazon EFS. Les autorisations sont requises pour permettre à Amazon EFS de gérer les configura	25 janvier 2022

Modification	Description	Date
	tions de réplication des systèmes de fichiers au nom de l'utilisateur.	
Mise à jour d'une stratégie existante	Politique : AmazonElasticFileSystemReadOnlyAccess Amazon EFS a ajouté une nouvelle autorisation permettant aux principaux de décrire les réplications Amazon EFS. Les autorisations sont requises pour permettre aux utilisateurs de visualiser les configura tions de réplication des systèmes de fichiers.	25 janvier 2022
Mise à jour d'une stratégie existante	Politique : AmazonElasticFileSystemFullAccess Amazon EFS a ajouté de nouvelles autorisations pour permettre aux principaux de créer, de décrire et de supprimer des réplications Amazon EFS. Les autorisations sont requises pour permettre aux utilisateurs de gérer les configurations de réplication des systèmes de fichiers.	25 janvier 2022
Démarrage de la politique de suivi	Politique : AmazonElasticFileSystemClientReadWriteAccès Accorde des privilèges de lecture et d'écriture sur les systèmes de fichiers Amazon EFS aux clients NFS.	3 janvier 2022
Démarrage de la politique de suivi	Politique : AmazonElasticFileSystemServiceRolePolicy Autorisations du rôle lié à un service pour Amazon EFS.	8 octobre 2021

Modification	Description	Date
Mise à jour d'une stratégie existante	Politique : 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 paramètre s des préférences du compte dans la console Amazon EFS.	7 mai 2021
Mise à jour d'une stratégie existante	Politique : AmazonElasticFileSystemRead OnlyAccess Amazon EFS a ajouté de nouvelles autorisat ions 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 modificat ions apportées à ses politiques gérées par AWS	7 mai 2021

Utilisation de 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, reportez-vous à :

- Balisage des ressources Amazon EFS
- Contrôle de l'accès basé sur les balises d'une ressource
- À quoi sert ABACAWS ? dans le guide de l'utilisateur IAM

> **Note**
>
> La réplication Amazon EFS ne prend pas en charge l'utilisation de balises pour le contrôle d'accès basé sur les attributs (ABAC).

Pour appliquer des balises aux ressources Amazon EFS lors de leur création, les utilisateurs doivent disposer de certaines autorisationsAWS Identity and Access Management (IAM).

Octroi d'autorisations pour labéliser les ressources lors de la création

Les actions d'API Amazon EFS de création de balises vous permettent de spécifier des balises lorsque vous créez la ressource.

- `CreateAccessPoint`
- `CreateFileSystem`

Pour permettre aux utilisateurs de baliser les ressources lors de leur création, ils doivent être autorisés à utiliser l'action qui crée les ressources, telle que`elasticfilesystem:CreateAccessPoint` ou`elasticfilesystem:CreateFileSystem`. Si les balises sont spécifiées dans l'action de création de ressources,AWS effectue une autorisation supplémentaire sur l'`elasticfilesystem:TagResource`action 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.

Example politique : autoriser l'ajout de balises aux systèmes de fichiers uniquement au moment de la création

L'exemple de stratégie suivant permet aux utilisateurs de créer des systèmes de fichiers et de leur appliquer des balises uniquement 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"
          }
       }
    }
  ]
}
```

Utilisation de balises pour contrôler l'accès à vos ressources Amazon EFS

Pour contrôler l'accès aux ressources et aux actions Amazon EFS, vous pouvez utiliser des politiques IAM basées sur des balises. Vous pouvez effectuer ce contrôle de deux manières :

- Vous pouvez contrôler l'accès aux ressources Amazon EFS basé sur les balises de ces ressources.
- Vous pouvez contrôler quelles balises peuvent être transmises dans une condition de requête IAM.

Pour plus d'informations sur l'utilisation des balises pour contrôler l'accès auxAWS ressources, consultez la section Contrôle de l'accès à l'aide de balises dans le Guide de l'utilisateur IAM.

Contrôle de l'accès basé sur les balises d'une ressource

Pour contrôler les actions qu'un utilisateur ou un rôle peut effectuer sur une ressource Amazon EFS, vous pouvez utiliser des balises sur la ressource. Par exemple, vous souhaiterez peut-être 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.

Example 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"
        }
    }
}
```

Example politique : Supprimer les systèmes de fichiers avec des 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 serviceAWS Identity and Access Management (IAM). Le rôle lié à un service Amazon EFS est un type unique de rôle IAM lié directement à Amazon EFS. Le rôle lié à un service Amazon EFS comprend les autorisations requises par le service pour appeler d'autresServices AWS en votre 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 son rôle lié à un service et seul Amazon EFS peut endosser son rôle. 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 la suppression préalable du rôle lié à un service Amazon EFS uniquement après la suppression préalable du rôle lié au service Amazon EFS. Vos ressources Amazon EFS sont ainsi protégées, car vous ne pouvez pas supprimer involontairement l'autorisation d'accéder aux ressources.

Les rôles liés à un service permettent aussi que tous les appels d'API soient visibles via AWS CloudTrail. Cela facilite le suivi et les exigences d'audit, car vous pouvez suivre toutes les actions exécutées par Amazon EFS en votre nom. Pour plus d'informations, veuillez consulter Entrées de journal pour les rôles liés à un service EFS.

Autorisations du rôle lié à un service pour Amazon EFS

Amazon EFS utilise le rôle lié au service nomméAWSServiceRoleForAmazonElasticFileSystem pour permettre à Amazon EFS d'appeler et de gérerAWS des ressources pour le compte de vos systèmes de fichiers EFS.

Le rôle lié à un service AWSServiceRoleForAmazonElasticFileSystem approuve les services suivants pour endosser le rôle :

- `elasticfilesystem.amazonaws.com`

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"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Vous devez configurer manuellement les autorisations IAMAWS KMS lors de la création d'un nouveau système de fichiers Amazon EFS chiffré au repos. Pour en savoir plus, consultez Chiffrement de données au repos.

Création d'un rôle lié à un service pour Amazon EFS

Vous devez configurer les autorisations de manière à permettre à une entité IAM (telle qu'un utilisateur, groupe ou rôle) de créer un rôle lié à un service. Pour ce faire, ajoutez l'`iam:CreateServiceLinkedRole`autorisation à une entité IAM, comme illustré dans l'exemple suivant.

```
{
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": [
                "elasticfilesystem.amazonaws.com"
            ]
        }
    }
}
```

Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Vous n'avez pas besoin 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 laAWS Management ConsoleAWS CLI, ou l'AWSAPI, Amazon EFS crée automatiquement le rôle lié au service.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure 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 recrée automatiquement le rôle lié au service.

Modification d'un rôle lié à un service pour Amazon EFS

Amazon EFS ne vous permet pas de modifier le rôle`AWSServiceRoleForAmazonElasticFileSystem` lié à un service. 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, consultez Editing a Service-Linked Role (Modification d'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.

> **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.

Pour supprimer les ressources Amazon EFS utilisées par`AWSServiceRoleForAmazonElasticFileSystem`

Procédez comme suit pour supprimer les ressources Amazon EFS utilisées par`AWSServiceRoleForAmazonElasticFileSystem`. Pour la procédure détaillée, reportez-vous à la section Nettoyez les ressources et protégez votre AWS compte.

1. Sur votre instance Amazon EC2, démontez le système de fichiers Amazon EFS.
2. Supprimez le système de fichiers Amazon EFS.
3. Supprimez le groupe de sécurité personnalisé du système de fichiers.

> **Warning**
>
> Si vous avez utilisé le groupe de sécurité par défaut pour votre Virtual Private Cloud (VPC), ne le supprimez pas.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForAmazonElasticFileSystem. Pour plus d'informations, veuillez consulter Deleting a Service-Linked Role (Suppression d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

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 veux autoriser des personnes extérieures à mon 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 encore besoin d'aide, contactez votre administrateur AWS. Votre administrateur vous a fourni vos informations 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 vous permettent de transmettre un rôle existant à ce service, au lieu de créer une nouvelle fonction du service ou 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 une fonction du 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 encore besoin d'aide, contactez votre administrateur AWS. Votre administrateur vous a fourni vos informations de connexion.

Je veux autoriser des personnes extérieures à mon 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 (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, 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 octroyer l'accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, consultez la section Fournir l'accès à un utilisateur IAM dans un autre Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment octroyer l'accès à vos ressources à des tiers Comptes AWS, consultez Fournir l'accès aux Comptes AWS appartenant à 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 découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation d'IAM pour contrôler l'accès aux données du système 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, consultezJournalisation des appels d'API Amazon EFS avec AWS CloudTrail.

> **Important**
>
> Vous devez utiliser l'assistant de montage EFS pour monter vos systèmes de fichiers Amazon EFS afin d'utiliser l'autorisation IAM pour contrôler l'accès par les clients. Pour plus d'informations, consultez 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
`elasticfilesystem:ClientMount`	Fournit un accès en lecture seule à un système de fichiers.
`elasticfilesystem:ClientWrite`	Fournit les droits d'écriture sur un système de fichiers.
`elasticfilesystem:ClientRootAccess`	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
`aws:SecureTransport`	Utilisez cette clé pour exiger que les clients utilisent TLS lors de la connexion à un système de fichiers EFS.	Booléen
`aws:SourceIp`	Adresse IP privée du client accédant à un système de fichiers EFS.	Chaîne
`elasticfilesystem:AccessPointArn`	ARN du point d'accès EFS auquel le client se connecte.	Chaîne
`elasticfilesystem:AccessedViaMountTarget`	Utilisez cette clé pour empêcher les clients qui n'utilisent pas de cibles de montage de systèmes de fichiers d'accéder à un système de fichiers EFS.	Booléen

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 Elastic File System.

Contrôle de l'accès réseau aux systèmes de fichiers Amazon 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 avec Amazon EC2, tels que les règles de groupe de sécurité VPC et les listes ACL réseau. 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 pour les instances Amazon EC2 et les cibles de montage
- Ports source à utiliser avec EFS
- Considérations relatives à la sécurité pour l’accès réseau
- Utilisation des points de terminaison VPC d'interface dans Amazon EFS

Utilisation de groupes de sécurité VPC pour les instances Amazon EC2 et les cibles de montage

Lorsque vous utilisez Amazon EFS, vous spécifiez des groupes de sécurité Amazon EC2 pour vos instances EC2 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 de mise en route, vous avez créé un groupe de sécurité lors du lancement de l’instance EC2. 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 de mise en route. Toutefois, pour un système de production, vous devez configurer des groupes de sécurité avec des autorisations minimales pour une utilisation avec EFS.

Vous pouvez autoriser l’accès entrant et sortant à votre système de fichiers EFS. Pour ce faire, vous devez ajouter des règles qui autorisent votre instance EC2 à se connecter à votre système de fichiers Amazon EFS via la cible de montage en utilisant le port Network File System (NFS). Pour créer et mettre à jour vos groupes de sécurité, procédez comme indiqué ci-après.

Pour créer des groupes de sécurité pour les instances EC2 et les cibles de montage

1. Créez deux groupes de sécurité dans votre VPC.

   Pour plus d’informations, consultez la procédure Pour créer un groupe de sécurité dans un Guide de l’utilisateur Amazon VPC.
2. Ouvrez la console de gestion Amazon VPC à l’adresse https://console.aws.amazon.com/vpc/ et vérifiez les règles par défaut pour ces groupes de sécurité. Les deux groupes de sécurité doivent avoir uniquement une règle sortante qui autorise le trafic en sortie.

Pour mettre à jour l’accès nécessaire pour vos groupes de sécurité

1. Ouvrez la console Amazon VPC à l’adresse https://console.aws.amazon.com/vpc/.

2. Ajoutez une règle pour votre groupe de sécurité EC2 afin d'autoriser l'accès entrant avec SSH (Secure Shell) depuis n'importe quel hôte. Vous pouvez éventuellement limiter l'adresse Source.

   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 la connexion TCP sur le port NFS, en identifiant le groupe de sécurité de la cible de montage en tant que destination.

   Pour plus d'informations, consultez Ajout et suppression de règles dans le Guide de l'utilisateur Amazon VPC.

3. Création de règles entrantes et sortantes pour la cible de montage.

   - Ajoutez une règle de réception pour le groupe de sécurité cible de montage afin d'autoriser l'accès entrant à partir du groupe de sécurité EC2. Identifier le groupe de sécurité EC2 comme source.
   - Ajoutez une règle de sortie pour ouvrir la connexion TCP sur tous les ports NFS. Identifie le groupe de sécurité EC2 comme destination.

   Pour plus d'informations, consultez Ajout et suppression de règles dans le Guide de l'utilisateur Amazon VPC.

4. Vérifiez que les deux groupes de sécurité autorisent maintenant l'accès entrant et sortant.

Pour plus d'informations sur les groupes de sécurité, consultez la section Groupes de sécurité Amazon EC2 pour les instances Linux.

Ports source à utiliser avec 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 vers le port NFS (TCP port 2049) de l'une des cibles de montage du système de fichiers. De même, un client NFSv4.1 ne peut faire valoir un ID de groupe et un ID d'utilisateur 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 :
  - Instances Amazon EC2 dans le VPC Amazon local
  - instances EC2 des VPC connectés
  - Serveurs sur site connectés à un Amazon VPC à AWS Direct Connect l'aide d' AWS Virtual Private Network un (VPN)
- ACL réseau des sous-réseaux VPC du client et des cibles de montage pour l'accès depuis l'extérieur des sous-réseaux d'une cible de montage – Pour monter le système de fichiers, le client doit pouvoir établir une connexion TCP sur le port NFS d'une cible de montage et recevoir le trafic en retour.
- Règles des groupes de sécurité VPC du client et des cibles de montage, pour tous les accès – Pour qu'une instance EC2 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 plus d’informations, consultez Gérer des cibles de Montage.

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 Points de terminaison VPC 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 d'autres VPC à l'aide AWS VPN de l'appairage VPC. AWS Direct Connect Pour en savoir plus, consultez la section Accès aux services via AWS PrivateLink le guide de l'utilisateur Amazon VPC.

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 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 la section Création d'un point de terminaison 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, veuillez consulter Contrôle de l'accès aux services avec des points de terminaison d'un VPC dans le Amazon VPC Guide de l'utilisateur.

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": "*"
        }
    ]
}
```

Pour plus d'informations, veuillez consulter Utilisation des politiques de point de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Utilisation des utilisateurs, des groupes et des 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 plus d'informations, consultez Utilisation des points d'accès Amazon EFS.

Les objets du système de fichiers Amazon EFS ont un mode de style Unix qui leur est associé. 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 mappées 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 les identifiants numériques mappés 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 identifiants de groupe (GID) par utilisateur et tous les GID supplémentaires sont tronqués à partir des demandes des clients NFS. Pour plus d'informations, consultez 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
- Exemple de cas d'utilisation et d'autorisations du système de fichiers Amazon 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 de type Unix sur la base de l'ID utilisateur et de l'ID de groupe déclarés par le client NFSv4.1 de montage, sauf s'ils sont remplacés par un point d'accès EFS. Pour plus d'informations, consultez Utilisation des utilisateurs, des groupes et des autorisations au niveau du système de fichiers réseau (NFS).

> **Note**
>
> Par défaut, cette couche de contrôle d'accès varie selon l'approbation du client NFSv4.1 dans sa déclaration de l'ID utilisateur et de l'ID de 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 d'IAM pour contrôler l'accès aux données du système 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 fichier du répertoire partagé `/share`.

Exemple de cas d'utilisation et d'autorisations du système de fichiers Amazon EFS

Une fois que vous avez créé un système de fichiers Amazon EFS et des cibles de montage pour le système de fichiers dans votre VPC, vous pouvez monter le système de fichiers éloigné en local sur

votre instance Amazon EFS. 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,wsize=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, voirProcédure : Création de sous-répertoires par utilisateur accessibles en écriture et configuration d'un remontage au redémarrage automatique.
- Autoriser des utilisateurs à écrire à la racine de système de fichiers Amazon EFS. Un utilisateur avec des privilèges racine peut accorder à d'autres utilisateurs l'accès au système de fichiers.
  - Pour transférer la propriété du système de fichiers Amazon EFS à un utilisateur et un groupe non racine, utilisez la commande suivante :

    ```
    $ 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 instances EC2 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 répertoires d'un système de fichiers Amazon EFS prennent en charge les autorisations lecture, écriture et exécution de type Unix sur la base de l'ID utilisateur et des ID de groupe. 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. Les points d'accès EFS peuvent être utilisés pour remplacer l'ID utilisateur et les ID de groupe utilisés par le client NFS. Lorsque les utilisateurs essaient d'accéder aux fichiers et aux répertoires, Amazon EFS vérifie leurs identifiants d'utilisateur et de groupe pour s'assurer que chaque utilisateur a le droit d'accéder aux objets. Amazon EFS utilise également ces ID 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 instance EC2, vous pouvez lui affecter un ID utilisateur (UID) et un ID de groupe (GID) numériques. Les ID d'utilisateur numériques sont définis dans le fichier `/etc/passwd` sur les systèmes Linux. Les ID de groupe numériques se trouvent dans le fichier `/etc/group`. Ces fichiers définissent les mappings entre les noms et les ID. En dehors de l'instance EC2, Amazon EFS n'effectue aucune authentification de ces ID, y compris de l'ID racine 0.

Si un utilisateur accède à un système de fichiers Amazon EFS à partir de deux instances EC2 différentes, selon que l'UID de l'utilisateur est le même ou différent sur ces instances, vous constatez un comportement différent, comme suit :

- Si les ID d'utilisateur sont identiques sur les deux instances EC2, Amazon EFS estime qu'ils indiquent le même utilisateur, quelle que soit l'instance EC2 utilisée. L'expérience utilisateur lors de l'accès au système de fichiers est la même depuis les deux instances EC2.

- Si les ID d’utilisateur ne sont pas les mêmes sur les deux instances EC2, Amazon EFS considère les utilisateurs comme étant des utilisateurs différents. L’expérience utilisateur est différente lors de l’accès au système de fichiers Amazon EFS à partir de deux instances EC2 différentes.
- Si deux utilisateurs différents sur différentes instances EC2 partagent un ID, Amazon EFS estime qu’il s’agit du même utilisateur.

Vous pouvez envisager de gérer les mappings d’ID utilisateur sur les instances EC2 de manière cohérente. 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 outil de mappage d’ID qui gère le mapping entre les noms d’utilisateur et les ID. Dans Amazon Linux, ce démon est appelé `rpc.idmapd` et sur Ubuntu il est appelé `idmapd`. Il convertit les ID utilisateur et ID de groupe en noms et inversement. Toutefois, Amazon EFS gère uniquement les ID numériques. Nous vous recommandons de désactiver ce processus sur vos instances EC2. 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 ressources AWS Identity and Access Management (AWS IAM) n'autorise pas l'accès à l'`ClientRootAccess`action. Lorsque l’écrasement racine est activé, l’utilisateur racine est converti en utilisateur disposant d’autorisations limitées sur le serveur NFS.

Pour plus d'informations, consultez Utilisation d'IAM pour contrôler l'accès aux données du système de fichiers et Procédure pas à pas : activer le root squashing à l'aide de l'autorisation IAM pour les clients NFS.

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 Amazon EFS.

Utilisation des points d'accès Amazon EFS

Les points d'accès Amazon EFS sont des points d'entrée spécifiques à l'application dans un système de fichiers EFS, lesquels facilitent la gestion de l'accès des applications aux jeux 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.

Pour plus d'informations sur la création d'un point d'accès, consultez Création de points d'accès.

Rubriques

- Création d'un point d'accès
- Montage d'un système de fichiers à l'aide d'un point d'accès
- 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

Création d'un point d'accès

Vous pouvez créer des points d'accès pour un système de fichiers Amazon EFS existant à l' AWS Management Console aide des API, the AWS Command Line Interface (AWS CLI) et EFS. Un système de fichiers Amazon EFS peut avoir 1 000 points d'accès maximum. 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, voirCréation de points d'accès.

Montage d'un système de fichiers à l'aide d'un point 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.

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.
- ID de groupe secondaire : liste facultative d'ID de groupe secondaire.

Lorsque l'application utilisateur forcée est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS 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.
- EFS prend en compte l'ID utilisateur, l'ID de groupe et les ID de groupe secondaire du point d'accès lors de l'évaluation des autorisations du système de fichiers. EFS ignore les ID du client NFS.

> **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 Utilisation des utilisateurs, des groupes et des autorisations au niveau du système de fichiers réseau (NFS).

Amazon EFS crée un répertoire racine de point d'accès uniquement si le nom OwnUid, 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 OwnerUid 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 de répertoire racine est en place, EFS ne divulgue pas les descripteurs de fichiers pour les fichiers qui se trouvent 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 à l'aide d'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 Amazon EFS

La fonctionnalité de blocage de l’accès public Amazon EFS fournit des paramètres qui vous permettent de gérer l’accès public aux systèmes de fichiers Amazon EFS. Par défaut, les nouveaux systèmes de fichiers Amazon 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, les 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 afin d'accéder à votre système de fichiers, contactez AWS le 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 CIDR (Classless Inter-Domain Routing) utilisant `aws:SourceIp`. Pour plus d’informations sur CIDR, consultez RFC 4632 sur le site web RFC Editor.
- 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 EFS `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 :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- 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 (AZ). Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec AzS,

vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement entre les zones sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

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 d'autres zones de disponibilité, 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 plus d'informations, consultez Utiliser Amazon EFS 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.

Vous pouvez appeler ces opérations d’API à partir de n’importe quel emplacement sur le réseau, mais Amazon EFS prend bel et bien en charge les stratégies d’accès basées sur les ressources, ce qui peut inclure des restrictions en fonction de l’adresse IP source. Vous pouvez également utiliser des politiques Amazon EFS pour contrôler l’accès à partir de points de terminaison Amazon Virtual Private Cloud (Amazon VPC) ou de VPC spécifiques. 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 NFSv4.0 et 4.1 non prises en charge
- Considérations supplémentaires
- Résolution des erreurs de traitement de fichiers

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 toutes les valeurs limites Amazon EFS et demander une augmentation du quota pour le nombre de systèmes de fichiers EFS dans un Région AWS.

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.
- Quota de débit élastique par système de fichiers régional pour tous les clients connectés dans un Région AWS.
- Quota de débit alloué par système de fichiers régional pour tous les clients connectés dans un. Région AWS

Le tableau suivant répertorie les quotas pour chaque ressource .

Nombre de systèmes de fichiers par compte client

Ressource	Quota par défaut
Nombre de systèmes de fichiers pour chaque compte client dans un Région AWS	1 000

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) Région USA Est (Virginie du Nord) Région USA Ouest (Oregon) Région Asie-Pacifique (Tokyo) Région Europe (Irlande)	20 gibioctets par seconde () GiBps	5 GiBps
Tous les autres Régions AWS	3 GiBps	1 GiBps

Systèmes de fichiers régionaux — Débit total provisionné par défaut par système de fichiers pour tous les clients connectés dans chaque système de fichiers Région AWS

Région AWS	Débit de lecture maximal	Débit d'écriture maximal (débit mesuré)
Région US East (Ohio) Région USA Est (Virginie du Nord) Région USA Ouest (Oregon)	10 GiBps	3,33 GiBps

Région AWS	Débit de lecture maximal	Débit d'écriture maximal (débit mesuré)
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 points d'accès ou 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

Les tableaux suivants répertorient les quotas de ressources généraux, les limites de débit du système de fichiers One Zone et les limites de débit Bursting qui ne peuvent pas être modifiées.

Quotas de ressources généraux qui ne peuvent pas être Modifiés

Ressource	Quota
Nombre de points d'accès pour chaque système de fichiers	1 000
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 VPC 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 plus d'informations, consultez Montage de systèmes de fichiers EFS à partir d'un autre système Compte AWS ou d'un VPC.

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

Systèmes de fichiers régionaux et à zone unique : débit total en rafale par système de fichiers pour tous les clients connectés de chaque système Région AWS

Région AWS	Débit de lecture maximal	Débit d'écriture maximal
Région US East (Ohio) Région USA Est (Virginie du Nord) Région USA Ouest (Oregon) Région Asie-Pacifique (Sydney) Région Europe (Irlande)	5 GiBps	3 GiBps
Tous les autres Régions AWS	3 GiBps	1 GiBps

Quotas pour les clients NFS

Les quotas suivants s'appliquent aux clients NFS en supposant un client Linux NFSv4.1 :

- 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 identifiants de groupe (GID) par utilisateur et tous les GID supplémentaires 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
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 NFSv4.0 et 4.1 non prises en charge

Bien qu'Amazon EFS ne prenne pas en charge NFSv2 ou NFSv3, il prend en charge à la fois NFSv4.1 et NFSv4.0, à l'exception des fonctionnalités suivantes :

- pNFS
- 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 (ACL)
- 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
- Conservation des données NFSv4.1

- SetUID sur les répertoires
- Types de fichier non pris en charge lors de l'utilisation de l'opération CREATE : périphériques de stockage en mode bloc (NF4BLK), périphérique 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, FATTR4_MIMETYPE, FATTR4_QUOTA_AVAIL_HARD, FATTR4_QUOTA_AVAIL_SOFT, FATTR4_QUOTA_USED, FATTR4_TIME_BACKUP et FATTR4_ACL.

  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 Références générales AWS.
- 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 Montage avec des clients sur site.

Résolution des erreurs de traitement de fichiers

Lorsque vous accédez aux systèmes de fichiers Amazon 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 le client et sur les fichiers dans Amazon EFS consultez Quotas pour les clients NFS. 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 plus d’informations, consultez 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 de l'API Amazon EFS spécifique à la régionRégion 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 correspond une demande donnée est déterminée par la combinaison de la méthode de la demande (GET, PUT, POST ou DELETE) et du modèle auquel correspond son URI de demande parmi les différents modèles. Si l'opération est PUT ou POST, Amazon EFS extrait les arguments d'appel du segment de chemin Request-URI, des paramètres de requête et de l'objet JSON dans le corps de la requête.

> **Note**
>
> Bien que les noms d'opération, tels que `CreateFileSystem`, n'apparaissent pas dans le transfert, ces noms ont une signification dans les stratégies AWS Identity and Access Management (IAM). Pour plus d'informations, veuillez consulter Gestion des identités et des accès pour Amazon Elastic File System.
> Le nom de l'opération est également utilisé pour nommer les commandes dans les outils de ligne de commande et les éléments des API duAWS SDK. Par exemple, une commande de l'AWS CLI nommée `create-file-system` est mappée à l'opération `CreateFileSystem`.
> Le nom de l'opération apparaît également dansAWS CloudTrail les journaux des appels d'API Amazon EFS.

Point de terminaison d'API

Le point de terminaison API est le nom DNS utilisé en tant que hôte dans l'URI HTTP pour les appels d'API. Ces points de terminaison d'API sont spécifiques àRégions AWS et prennent la forme suivante.

```
elasticfilesystem.aws-region.amazonaws.com
```

Par exemple, le point de terminaison d'API Amazon EFS pour la région USA Ouest (Oregon) est le suivant.

```
elasticfilesystem.us-west-2.amazonaws.com
```

Pour obtenir laRégion AWS liste des systèmes pris en charge par Amazon EFS (où vous pouvez créer et gérer des systèmes de fichiers), consultez Amazon Elastic File System dans le Références générales AWS.

Le point de terminaison d'API spécifique à la région définit l'étendue des ressources Amazon EFS accessibles lorsque vous effectuez un appel d'API. Par exemple, lorsque vous appelez l'`DescribeFileSystems`opération à l'aide du point de terminaison précédent, vous obtenez une liste des systèmes de fichiers de la région USA Ouest (Oregon) qui ont été créés dans votre compte.

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 de 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 Elastic File System
- Actions
- Types de données

Utilisation du taux de demandes de l'API de requête pour Amazon EFS

Les demandes d'API Amazon EFS sont limitées pour chaqueCompte AWS région afin d'améliorer les performances du service. Tous les appels d'API Amazon EFS combinés, qu'ils proviennent d'une application, de laAWS CLI console Amazon EFS ou de la console Amazon EFS, ne doivent pas dépasser le taux de demandes d'API maximum autorisé. Le taux maximal de demandes d'API peut varier d'un endroit à l'autreRégions AWS. Les demandes d'API effectuées sont attribuées au sous-jacentCompte 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.

Réessais ou traitement par lots

Il se peut que votre application doive réessayer une demande d'API en cas d'échec, ou pour traiter plusieurs ressources (par exemple, tous 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 sommeil

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 Error Retries and Exponential BackoffAWS 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. 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 approche de la limitation de 1 000 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 : chaîne

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 : 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

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"
      }
   ]
}
```

Eléments 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 : chaîne

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 : chaîne

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 : chaîne

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 : 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})$`

LifeCycleState

Identifie la phase du cycle de vie du point d'accès.

Type : chaîne

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 : chaîne

OwnerId

Identifie Compte AWS le propriétaire de la ressource du point d'accès.

Type : chaîne

Contraintes de longueur : longueur maximale de 14.

Modèle : `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

PosixUser

Identité POSIX complète, y compris l'ID utilisateur, l'ID de groupe et les ID de groupe secondaire, sur le point d'accès utilisé pour toutes les opérations de fichiers effectuées 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, consultezhttps://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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 des instances EC2 dans 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 : chaîne

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 partout Régions AWS 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 : chaîne

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 CreateFileSystem:Encrypted sur true.

> **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 : chaîne

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 performance `generalPurpose` 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 : chaîne

Valeurs valides : `generalPurpose | maxIO`

Obligatoire : non

ProvisionedThroughputInMibps

Débit, mesuré en mébioctets 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 AWS 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 : chaîne

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"
}
```

Eléments 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 : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

FileSystemId

ID du système de fichiers, attribué par Amazon EFS.

Type : 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})$`

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 : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

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` définit 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 instances EC2 à l'aide de la cible de montage.

Vous pouvez créer une cible de montage dans chaque Zone de disponibilité de votre VPC. Toutes les instances EC2 d'un VPC dans une Zone de disponibilité donnée partagent une seule cible de montage pour un système de fichiers donné. Si vous disposez de plusieurs sous-réseaux dans une Zone de disponibilité, vous pouvez créer une cible de montage dans l'un de ces sous-réseaux. Pour accéder à leur système de fichiers, les instances EC2 n'ont pas besoin de partager le même sous-réseau que la cible de montage.

Vous ne pouvez créer qu'une seule cible de montage pour un système de fichiers Zone unique. Vous devez créer cette cible de montage dans la même Zone de disponibilité que celle où se trouve le système de fichiers. Utilisez `AvailabilityZoneName` propriétés `AvailabiltyZoneId` et de l'objet de réponse DescribeFileSystems pour obtenir ces informations. Utilisez la Zone de disponibilité `subnetId` associée au système de fichiers lors de la création de la cible de montage.

Pour plus d'informations, consultez Fonctionnement d'Amazon EFS.

Pour créer une cible de montage pour un système de fichiers, l'état du cycle de vie du système de fichiers doit être `available`. Pour plus d'informations, consultez DescribeFileSystems.

Dans la demande, fournissez les éléments suivants :

- L'ID du système de fichiers pour lequel vous créez la cible de montage.
- Un ID de sous-réseau, qui détermine les éléments suivants :
  - Le VPC dans lequel Amazon EFS crée la cible de montage
  - La Zone de disponibilité dans laquelle Amazon EFS crée la cible de montage
  - La plage d'adresses IP à partir de laquelle Amazon EFS sélectionne l'adresse IP de la cible de montage (si vous ne spécifiez pas d'adresse IP dans la demande)

Une fois la cible de montage créée, Amazon EFS retourne une réponse qui inclut un `MountTargetId` et une `IpAddress`. Vous utilisez cette adresse IP lors du montage du système de fichiers dans une instance EC2. Vous pouvez également utiliser le nom DNS de la cible de montage lors du montage du système de fichiers. L'instance EC2 sur laquelle vous montez le système de fichiers via la cible de montage peut convertir le nom DNS de la cible de montage en son adresse IP. Pour plus d'informations, consultez Fonctionnement de la présentation de la mise en place.

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. En d'autres termes, si le système de fichiers possède déjà une ou plusieurs cibles de montage créées pour ce dernier, le sous-réseau spécifié dans la demande d'ajout d'une autre cible de montage doit répondre aux exigences suivantes :

- Il doit appartenir au même VPC que les sous-réseaux des cibles de montage existantes
- Il ne doit pas se trouver dans la même Zone de disponibilité que les sous-réseaux des cibles de montage existantes

Si la demande répond aux exigences, Amazon EFS procède comme suit :

- Il crée une cible de montage dans le sous-réseau spécifié.
- Il crée également une interface réseau dans le sous-réseau comme suit :
  - Si la demande fournit une `IpAddress`, Amazon EFS attribue cette adresse IP à l'interface réseau. Sinon, Amazon EFS attribue une adresse gratuite au sous-réseau (de la même manière que l'appel `CreateNetworkInterface` Amazon EC2 lorsqu'une demande ne spécifie pas d'adresse IP privée principale).
  - Si la demande fournit des `SecurityGroups`, cette interface réseau est associée à ces groupes de sécurité. Sinon, elle appartient au groupe de sécurité par défaut pour le VPC du sous-réseau.
  - Attribue la description `Mount target` *`fsmt-id`* `for file system` *`fs-id`* dans laquelle *`fsmt-id`* est l'ID de la cible de montage et *`fs-id`* est le `FileSystemId`.
  - Définit la propriété `requesterManaged` de l'interface réseau sur `true` et la valeur `requesterId` sur `EFS`.

  Chaque cible de montage Amazon EFS dispose d'une interface réseau EC2 gérée par demandeur correspondante. Une fois l'interface réseau créée, Amazon EFS définit le champ `NetworkInterfaceId` dans la description de la cible de montage sur l'ID d'interface réseau et le champ `IpAddress` 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.

Nous vous recommandons de créer une cible de Montage dans chacune des Zones de disponibilité. L'utilisation d'un système de fichiers dans une Zone de disponibilité via une cible de montage créée dans une autre Zone de disponibilité implique un certain coût. Pour plus d'informations, consultez 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. En cas de défaillance de la Zone de disponibilité dans laquelle la cible de montage est créée, vous ne pouvez pas accéder à votre système de fichiers via cette cible de montage.

Cette opération exige des autorisations pour l'action suivante sur le système de fichiers :

- `elasticfilesystem:CreateMountTarget`

Cette opération exige également des autorisations pour les actions Amazon EC2 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",
   "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 : 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

IpAddress

Adresse IPv4 valide dans la plage d'adresses du sous-réseau spécifié.

Type : chaîne

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

SecurityGroups

Cinq ID de groupe de sécurité VPC maximum au format `sg-xxxxxxxx`. Ils sont destinés au même VPC que le sous-réseau spécifié.

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.

Type : chaîne

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",
   "LifeCycleState": "string",
   "MountTargetId": "string",
   "NetworkInterfaceId": "string",
   "OwnerId": "string",
   "SubnetId": "string",
   "VpcId": "string"
}
```

Eléments 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 : chaîne

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 la zone `us-east-1a` de disponibilité de votre région ne soit pas la même que celle `us-east-1a` d'une autre Compte AWS.

Type : chaîne

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 : 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})$`

IpAddress

Adresse à laquelle le système de fichiers peut être monté à l'aide de la cible de montage.

Type : chaîne

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}$`

LifeCycleState

État du cycle de vie de la cible de montage.

Type : chaîne

Valeurs valides : `creating | available | updating | deleting | deleted | error`

MountTargetId

ID de cible de montage attribué par le système.

Type : chaîne

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 : chaîne

OwnerId

Compte AWS ID propriétaire de la ressource.

Type : chaîne

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 : chaîne

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 : chaîne

Erreurs

AvailabilityZonesMismatch

Renvoie si la Zone de disponibilité spécifiée pour une cible de montage est différente de la Zone de disponibilité spécifiée pour le stockage Zone unique. 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 en spécifie un `IpAddress` qui est déjà utilisé 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

Renvoie si ce `IpAddress` n’est pas spécifié dans la demande et s’il n’y a aucune adresse IP libre dans le sous-réseau.

Code d’état HTTP : 409

SecurityGroupLimitExceeded

Renvoyé si la taille de `SecurityGroups` spécifiée dans la demande est supérieure à cinq.

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

Ajouter une cible de montage à un système de fichiers

La demande suivante crée une cible de montage pour un système de fichiers. La demande spécifie des valeurs uniquement pour les `FileSystemId` paramètres et les paramètres `SubnetId` requis. La demande ne fournit pas les options `IpAddress` et les paramètres `SecurityGroups`. Pour

`IpAddress`, l'opération utilise l'une des adresses IP disponibles dans le sous-réseau spécifié. De plus, l'opération utilise le groupe de sécurité par défaut associé au VPC pour `SecurityGroups`.

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

{
    "MountTargetId": "fsmt-55a4413c",
    "NetworkInterfaceId": "eni-01234567",
    "FileSystemId": "fs-01234567",
    "LifeCycleState": "available",
    "SubnetId": "subnet-01234567",
    "OwnerId": "231243201240",
    "IpAddress": "172.31.22.183"
}
```

Ajouter une cible de montage à un système de fichiers

La demande suivante spécifie tous les paramètres de demande pour créer une 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"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateReplicationConfiguration

Crée une configuration de réplication qui réplique un système de fichiers EFS existant vers un nouveau système de fichiers en lecture seule. 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 – Le système de fichiers EFS que vous souhaitez répliquer. Le système de fichiers source ne peut pas être un système de fichiers de destination dans une configuration de réplication existante.
- Région AWS — Le système de fichiers Région AWS dans lequel le système de fichiers de destination est créé. La réplication Amazon EFS est disponible Régions AWS dans tous les pays où EFS est disponible. La région doit être activé. Pour plus d'informations, consultez la section Gestion Régions AWS dans le Guide de référence AWS général.
- Configuration du système de fichiers de destination – Configuration du système de fichiers de destination vers lequel le système de fichiers source sera répliqué. Il ne peut y avoir qu'un seul système de fichiers de destination dans une configuration de réplication.

  Les paramètres de configuration de réplication incluent :

  - ID du système de fichiers – ID du système de fichiers de destination pour la réplication. Si aucun identifiant n'est fourni, EFS crée un nouveau système de fichiers avec les paramètres par défaut. Pour les systèmes de fichiers existants, la protection contre le remplacement par réplication du système de fichiers doit être désactivée. Pour en savoir plus, consultez la section Réplication vers un système de fichiers existant.
  - Zone de disponibilité – Si vous souhaitez que le système de fichiers de destination utilise le stockage Zone unique, vous devez spécifier la Zone de disponibilité dans laquelle créer le système de fichiers. Pour plus d'informations, consultez les types de systèmes de fichiers EFS dans le Guide de l'utilisateur Amazon EFS.
  - Chiffrement – Tous les systèmes de fichiers de destination sont créés avec le chiffrement au repos activé. Vous pouvez spécifier la clé AWS Key Management Service (AWS KMS) 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.

    > **Note**
    >
    > Vous ne pouvez pas modifier ces propriétés après la création de la clé KMS.

Pour les nouveaux systèmes de fichiers de destination, les propriétés suivantes sont définies par défaut :

- 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 EFS Zone unique. Dans ce cas, le mode Performance Usage général 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 de débit.

- 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 activer la gestion du cycle de vie.
- Sauvegardes automatiques – Les sauvegardes quotidiennes automatiques sont activées sur le système de fichiers de destination. Une fois le système de fichiers créé, vous pouvez modifier ce paramètre.

Pour plus d'informations, consultez la Réplication Amazon EFS 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"
      }
   ]
}
```

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,
```

```
            "Region": "string",
            "Status": "string"
        }
    ],
    "OriginalSourceFileSystemArn": "string",
    "SourceFileSystemArn": "string",
    "SourceFileSystemId": "string",
    "SourceFileSystemRegion": "string"
}
```

Eléments 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 : chaîne

SourceFileSystemArn

Amazon Resource Name (ARN) du système de fichiers source actuel dans la configuration de réplication.

Type : chaîne

SourceFileSystemId

ID du système de fichiers Amazon EFS source qui est répliqué.

Type : 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})$`

SourceFileSystemRegion

Région AWS Dans lequel se trouve le système de fichiers EFS source.

Type : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 instance EC2 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 actif`deleting`. 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'action Amazon EC2 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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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"
}
```

Eléments 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 : chaîne

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" ]
   }
}
```

Eléments 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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"
   }
}
```

Eléments 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 la politique de système de fichiers EFS par défaut est appliquée au système de fichiers EFS spécifié.

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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"
}
```

Eléments 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 : 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})$`

Policy

Le JSON formaté `FileSystemPolicy` pour le système de fichiers EFS.

Type : chaîne

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 la politique de système de fichiers EFS par défaut est appliquée au système de fichiers EFS spécifié.

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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"
}
```

Eléments 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 : chaîne

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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLifecycleConfiguration

Renvoie l'objet actuel `LifecycleConfiguration` pour le système de fichiers Amazon 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"
      }
   ]
}
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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`.

Syntaxe de la demande

```
GET /2015-02-01/mount-targets?
AccessPointId=AccessPointId&FileSystemId=FileSystemId&Marker=Marker&MaxItems=MaxItems&MountTarg
 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",
            "LifeCycleState": "string",
            "MountTargetId": "string",
            "NetworkInterfaceId": "string",
            "OwnerId": "string",
            "SubnetId": "string",
            "VpcId": "string"
        }
    ],
    "NextMarker": "string"
}
```

Eléments 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 : chaîne

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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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" ]
}
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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.

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,
               "Region": "string",
               "Status": "string"
            }
         ],
         "OriginalSourceFileSystemArn": "string",
         "SourceFileSystemArn": "string",
         "SourceFileSystemId": "string",
         "SourceFileSystemRegion": "string"
      }
   ]
}
```

Eléments 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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"
      }
   ]
}
```

Eléments 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 : chaîne

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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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"
      }
   ]
}
```

Eléments 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 plus d'informations, consultez 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 tableau comprenant jusqu'à cinq ID de groupes de sécurité VPC.

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
```

Eléments 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 la taille de `SecurityGroups` spécifiée dans la demande est supérieure à cinq.

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutAccountPreferences

Utilisez cette opération pour définir la préférence de Région AWS actuelle afin d'utiliser des identifiants de ressource longs de 17 caractères (63 bits) ou courts de 8 caractères (32 bits) pour le nouveau système de fichiers EFS et de monter les ressources cibles. Tous les identifiants de ressources existants ne sont pas affectés par les modifications que vous apportez. Vous pouvez définir la préférence d'identification pendant la période d'inscription à mesure que l'EFS passe à des identifiants de ressource longs. Pour en savoir plus, consultez Gestion des identifiants de ressources Amazon EFS.

> **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 que vous devez utiliser des identifiants courts pour le système de fichiers et les 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 que vous devez utiliser des identifiants courts pour le système de fichiers et les ressources cibles de montage.

Type : chaîne

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" ]
   }
}
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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"
   }
}
```

Eléments 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 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 ressource 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 : chaîne

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"
}
```

Eléments 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 : 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})$`

Policy

Le JSON formaté `FileSystemPolicy` pour le système de fichiers EFS.

Type : chaîne

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-1:111122233334444:file-
system/fs-01234567"
        }
    ]
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 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.

> **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"
      }
   ]
}
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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
```

Eléments 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 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 AWS 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 : chaîne

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"
}
```

Eléments 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 : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

FileSystemId

ID du système de fichiers, attribué par Amazon EFS.

Type : 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})$`

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 : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

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` définit 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 : chaîne

Valeurs valides : `ENABLED | DISABLED | REPLICATING`

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "ReplicationOverwriteProtection": "string"
}
```

Eléments 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 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 : chaîne

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 : chaîne

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 : chaîne

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 : 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 : non

LifeCycleState

Identifie la phase du cycle de vie du point d’accès.

Type : chaîne

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 : chaîne

Contraintes de longueur : longueur maximale de 14.

Modèle : `^(\d{12})|(\d{4}-\d{4}-\d{4})$`

Obligatoire : non

PosixUser

Identité POSIX complète, y compris l'ID utilisateur, l'ID de groupe et les ID de groupe secondaire, sur le point d'accès utilisé pour toutes les opérations de fichiers effectuées 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : chaîne

Valeurs valides : `ENABLED | ENABLING | DISABLED | DISABLING`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 les ID POSIX 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : 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

Region

Le système de fichiers Région AWS dans lequel se trouve le système de fichiers de destination.

Type : chaîne

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 du système de fichiers EFS de destination.

- L'état `Paused` se produit lorsque vous vous désactivez de la région source ou de destination après la création de la configuration de réplication. Pour reprendre la réplication du système de fichiers, vous devez à nouveau vous connecter au Région AWS. Pour plus d'informations, consultez la section Gestion Régions AWS dans le Guide de référence AWS général.
- L'état `Error` se produit lorsque le système de fichiers source ou de destination (ou les deux) est défaillant et est irrécupérable. Pour plus d'informations, consultez Surveillance de l'état de la réplication dans le Guide de l'utilisateur d'Amazon EFS. Vous devez supprimer la configuration de réplication, puis restaurer la sauvegarde la plus récente du système de fichiers défaillant (soit la source, soit la destination) sur un nouveau système de fichiers.

Type : chaîne

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

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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.

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 : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `.+`

Obligatoire : non

FileSystemId

ID du système de fichiers à utiliser pour la cible. La réplication de l'écrasement du système de fichiers doit être désactivée. Si vous ne fournissez pas d'ID, EFS crée un nouveau système de fichiers pour la destination de réplication.

Type : 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 : 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 - 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 - L'ARN pour un alias de clé, par exemple `arn:aws:kms:us-west-2:444455556666:alias/projectKey1`.

Type : chaîne

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

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.

Type : chaîne

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

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : chaîne

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 : 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

LifeCycleState

Phase du cycle de vie du système de fichiers.

Type : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

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 : chaîne

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` définit 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 : chaîne

Valeurs valides : `bursting | provisioned | elastic`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : chaîne

Valeurs valides : `ENABLED | DISABLED | REPLICATING`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : chaîne

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 : chaîne

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 replacer 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 : chaîne

Valeurs valides : `AFTER_1_ACCESS`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : 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

LifeCycleState

État du cycle de vie de la cible de montage.

Type : chaîne

Valeurs valides : `creating | available | updating | deleting | deleted | error`

Obligatoire : oui

MountTargetId

ID de cible de montage attribué par le système.

Type : chaîne

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 : chaîne

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 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 : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : `.+`

Obligatoire : non

IpAddress

Adresse à laquelle le système de fichiers peut être monté à l’aide de la cible de montage.

Type : chaîne

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

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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

PosixUser

Identité POSIX complète, y compris l'ID utilisateur, l'ID de groupe et tout ID de groupe secondaire, sur le point d'accès utilisé pour toutes les opérations de 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

ID de groupe POSIX secondaire utilisés pour toutes les opérations de 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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : chaîne

Obligatoire : oui

SourceFileSystemArn

Amazon Resource Name (ARN) du système de fichiers source actuel dans la configuration de réplication.

Type : chaîne

Obligatoire : oui

SourceFileSystemId

ID du système de fichiers Amazon EFS source qui est répliqué.

Type : 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

SourceFileSystemRegion

Région AWS Dans lequel se trouve le système de fichiers EFS source.

Type : chaîne

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

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 les ID POSIX et les autorisations à appliquer au `RootDirectory` du point 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 : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^(\/|(\/(?!\.)+[^$#<>;`|&?{}^*/\n]+){1,4})$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : chaîne

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 : chaîne

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 AWS SDK spécifiques au langage, consultez les pages suivantes :

- 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 : 15 mai 2024

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
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 mises 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 réplicati on a été ajoutée aux systèmes de fichiers et est activée par défaut. La protection empêche l'utilisation des système de fichiers comme destination dans une configuration de réplication. Pour plus d'informa tions, 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 Mac EC2 exécutées 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 FIFO.	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 de cibles de montage se voient désormais attribuer des ID à 17 caractères. 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	A compter du 1er octobre 2021, Amazon EFS passe d'ID à 8 caractères à des ID à 17 caractères pour les systèmes de fichiers et les cibles de montage. Au cours de cette transition, vous pouvez vous inscrire et commencer à utiliser des identifiants de ressource à 17 caractères par an Région AWS . Pour de plus amples informations, veuillez consulter ID de ressource.	5 mai 2021
Ajout de la prise en charge du montage de systèmes de fichiers One Zone depuis une autre zone de disponibilité à l'aide de l'assistant de montage Amazon EFS	Vous pouvez désormais recourir à l'assistant de montage EFS pour monter un système de fichiers Amazon EFS qui utilise les classes de stockage One Zone sur une instance EC2 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'informations, consultez Montage de systèmes de fichiers avec des classes de stockage One Zone.	6 avril 2021

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 nécessite nt 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

Ajout de la prise en charge des instances macOS Amazon EC2 exécutant macOS Big Sur	Vous pouvez désormais monter votre système de fichiers Amazon EFS à partir d'instances macOS EC2 qui exécutent 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 `MeteredIOBytes`	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 CloudWatchmétriques 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 peur 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 instances EC2. 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 %	EFS prend désormais en charge jusqu'à 500 Mo/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 la section 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, consultez le système de fichiers CreateyYour Amazon 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 la section 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 nécessair es. 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 Acess (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 instance EC2.	Vous pouvez désormais configurer de nouvelles instances Amazon EC2 pour monter vos systèmes de fichiers EFS au lancement dans l'assistant de lancement d'instance EC2. Pour de plus amples informations, consultez l'Étape 2. Créez vos ressources EC2 et lancez votre instance EC2.	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 transféré s dans la classe de stockage économique d'accès peu fréquent. Pour plus d'informa tions, 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 CreateFileSystème et création d'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 la section relative au montage à partir d'un autre compte ou VPC et au fonctionnement d'Amazon EFS avec Direct Connect et les VPN.	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
Support mathématique CloudWatch métrique ajouté	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 plus d'informations, consultez Utilisation des maths de métriques avec Amazon EFS.	4 avril 2018
Ajout de l'ensemble d'outils `amazon-efs-utils` open-source et ajout du chiffrement in 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 plus d'informations, consultez Installation des outils 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 plus d'informations, consultez 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 plus d'informations, consultez Les quotas de ressources Amazon EFS que vous ne pouvez pas Modifier.	15 mars 2018
Région AWS Support	Amazon EFS est désormais disponible pour tous les utilisateurs de l'ouest des États-Unis (Californie du Nord) Région AWS.	14 mars 2018

Modification	Description	Date de modification
supplémentaire ajouté		
Chiffrement de données au repos	Amazon ES prend désormais en charge le chiffrement des données au repos. Pour plus d'informations, consultez 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 résolu par l'adresse IP de la cible de montage dans la zone de disponibilité de l'instance Amazon EC2 en cours de connexion. Pour plus d'informations, consultez Montage sur Amazon EC2 avec un nom DNS.	20 décembre 2016
Meilleure prise en charge des balise 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 Balisage des ressources Amazon 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
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

Modification	Description	Date de modification
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.