aws

Guide de l'utilisateur de Lustre

FSx pour Lustre

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

FSx pour Lustre: Guide de l'utilisateur de Lustre

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Qu'est-ce qu'Amazon FSx for Lustre ? 1
Plusieurs options de déploiement et classes de stockage 2
FSx pour Lustre et les référentiels de données 2
FSx pour l'intégration du référentiel de données Lustre S3 3
FSx pour Lustre et les référentiels de données sur site 3
Accès aux systèmes de fichiers 3
Intégrations avec les services AWS 4
Conformité et sécurité 5
Hypothèses 5
Tarification d'Amazon FSx pour Lustre 6
Forums Amazon FSx pour Lustre 6
Utilisez-vous Amazon FSx for Lustre pour la première fois ? 6
Configuration 7
S'inscrire à Amazon Web Services 7
Inscrivez-vous pour un Compte AWS 7
Création d’un utilisateur doté d’un accès administratif 8
Ajouter des autorisations pour utiliser les référentiels de données dans Amazon S3 9
Comment FSx Lustre vérifie l'accès aux compartiments S3 11
Étape suivante 12
Premiers pas 13
Prérequis 13
Étape 1 : Créez votre système de fichiers FSx for Lustre 14
Installez le Lustre client 19
Étape 3 : monter le système de fichiers 20
Étape 4 : Exécutez votre flux de travail 22
Étape 5 : Nettoyer les ressources 22
Options de déploiement et de classe de stockage 24
Systèmes de fichiers persistants 24
Type de déploiement persistant 2 25
Type de déploiement persistant 1 25
Systèmes de fichiers Scratch 25
Adresses IP 26
FSx pour les classes de stockage Lustre 28
Comment la classe de stockage Intelligent-Tiering hiérarchise les données 29

Disponibilité du type de déploiement 30
Utilisation de référentiels de données 33
Vue d'ensemble des référentiels de données 34
Support des régions et des comptes pour les compartiments S3 liés 36
Support des métadonnées POSIX 36
Exportation de liens physiques 38
Associer des autorisations POSIX à un compartiment S3 39
Lier votre système de fichiers à un compartiment S3 42
Création d'un lien vers un compartiment S3 45
Mise à jour des paramètres d'association du référentiel de données 48
Supprimer une association vers un compartiment S3 50
Afficher les détails des associations de référentiels de données 51
État du cycle de vie des associations au référentiel de données 52
Utilisation de compartiments Amazon S3 chiffrés côté serveur 53
Importation de modifications depuis votre référentiel de données 56
Importez automatiquement des mises à jour depuis votre compartiment S3 58
Utilisation des tâches du référentiel de données pour importer des modifications 64
Préchargement de fichiers dans votre système de fichiers 66
Exportation des modifications vers le référentiel de données 69
Exportez automatiquement les mises à jour vers votre compartiment S3 70
Utilisation des tâches du référentiel de données pour exporter les modifications 74
Exportation de fichiers à l'aide de commandes HSM 76
Tâches du référentiel de données 77
Types de tâches liées au référentiel de données 78
État et détails de la tâche 79
Utilisation des tâches du référentiel de données 80
Utilisation des rapports d'achèvement des tâches 88
Résolution des échecs de tâches 89
Publication de fichiers 95
Utilisation des tâches du référentiel de données pour publier des fichiers 97
Utilisation d'Amazon FSx avec vos données sur site 99
Journaux d'événements du référentiel de données 100
Importer des événements 101
Exporter des événements 110
Événements de restauration HSM 118
Utilisation d'anciens types de déploiement 121

Liez votre système de fichiers à un compartiment Amazon S3 121
Importez automatiquement des mises à jour depuis votre compartiment S3 130
Performance 136
Présentation de 136
Comment fonctionnent FSx les systèmes de fichiers Lustre 136
Performances des métadonnées du système de fichiers 138
Débit vers les instances clientes individuelles 139
Disposition du stockage du système de fichiers 140
Regrouper les données dans votre système de fichiers 141
Modification de votre configuration de striping 142
Mises en page de fichiers progressives 144
Surveillance des performances et de l'utilisation 145
Classes de stockage SSD et HDD 146
Exemple : base de référence agrégée et débit en rafale 150
Classe de stockage à hiérarchisation intelligente 150
Performances du système de fichiers pour la hiérarchisation intelligente 152
Conseils sur les performances 154
Conseils relatifs à la hiérarchisation intelligente des performances 156
Accès aux systèmes de fichiers 158
Lustrecompatibilité entre le système de fichiers et le noyau client 158
Installation du Lustre client 163
Amazon Linux 163
CentOS, Rocky Linux et Red Hat 166
Ubuntu avec taille de page par défaut (4 Ko) 177
Ubuntu avec une taille de page de 64 Ko 179
SUSE Linux 181
Montage depuis Amazon EC2 184
Configuration des clients EFA 186
Étape 1 : Installation des pilotes requis 186
Étape 2 : Configuration de l'EFA pour le client Lustre 188
Étape 3 : interfaces EFA 189
Montage depuis Amazon ECS 191
Montage à partir d'une instance Amazon EC2 hébergeant des tâches Amazon ECS 192
Montage à partir d'un conteneur Docker 193
Montage à partir d'un VPC sur site ou d'un autre VPC 194
Montage FSx automatique d'Amazon 196

Montage automatique à l'aide de /etc/fstab 196
Montage de jeux de fichiers spécifiques 200
Démontage des systèmes de fichiers 201
Utilisation d'instances Spot EC2 202
Gestion des interruptions des instances Amazon EC2 Spot 203
Administration des systèmes de fichiers 206
Systèmes de fichiers compatibles avec EFA 206
Considérations relatives à l'utilisation de systèmes de fichiers compatibles EFA 207
Conditions préalables à l'utilisation de systèmes de fichiers compatibles avec EFA 208
Création d'un système de fichiers compatible EFA 209
Quotas de stockage 210
Application des quotas 210
Types de quotas 210
Limites de quotas et délais de grâce 211
Définition et affichage des quotas 212
Quotas et compartiments liés à Amazon S3 216
Quotas et restauration des sauvegardes 217
Capacité de stockage 218
Considérations relatives à l'augmentation de la capacité de stockage 219
Quand augmenter la capacité de stockage 219
Comment le dimensionnement du stockage et les demandes de sauvegarde simultanés sont gérés 220
Augmenter la capacité de stockage 220
Surveillance de l'augmentation de la capacité de stockage 222
Caches de lecture SSD 225
Considérations relatives à la mise à jour du cache de lecture SSD 228
Mettre à jour le cache de lecture d'un SSD provisionné 228
Surveillance des mises à jour du cache de lecture du SSD 230
Gérez les performances des métadonnées 232
Lustreconfiguration des performances des métadonnées 233
Considérations relatives à l'amélioration des performances des métadonnées 234
Quand améliorer les performances des métadonnées 235
Améliorer les performances des métadonnées 235
Modification du mode de configuration des métadonnées 237
Surveillance des mises à jour de configuration des métadonnées 238
Capacité de débit 241

Considérations relatives à la mise à jour de la capacité de débit 242
Quand modifier la capacité de débit 243
Modification de la capacité de débit 243
Surveillance des variations de capacité de débit 246
Compression des données 248
Gestion de la compression des données 249
Compression de fichiers déjà écrits 252
Affichage de la taille des fichiers 252
Utilisation de CloudWatch métriques 253
Courge racine 253
Comment fonctionne le courge-racine 254
Gérer les courges-racines 255
État du système de fichiers 259
Baliser vos ressources 260
Principes de base des étiquettes 261
Balisage de vos ressources 262
Restrictions liées aux étiquettes 262
Autorisations et étiquette 263
Maintenance 263
Versions lustrées 265
Bonnes pratiques pour les mises à niveau de la version Lustre 265
Exécution de la mise à niveau 266
Suppression d’un système de fichiers 268
Sauvegardes 269
Support de sauvegarde FSx pour Lustre 270
Utilisation de sauvegardes quotidiennes automatiques 271
Utilisation de sauvegardes initiées par l'utilisateur 271
Création de sauvegardes initiées par l'utilisateur 272
Utilisation AWS Backup avec Amazon FSx 272
Copie de sauvegardes 273
Limites relatives à la copie de sauvegarde 274
Autorisations pour les copies de sauvegarde interrégionales 275
Copies complètes et incrémentielles 276
Copier des sauvegardes au sein d'un même Compte AWS 276
Restauration des sauvegardes 277
Suppression de sauvegardes 279

Surveillance des systèmes de fichiers 280
Surveillance avec CloudWatch 281
Utilisation de CloudWatch métriques 283
Accès aux CloudWatch métriques 287
Métriques et dimensions 289
Avertissements et recommandations en matière de performances 311
Création d' CloudWatch alarmes 314
Journalisation à l'aide de CloudWatch journaux 317
Aperçu de la journalisation 317
Destinations des journaux 318
Gestion de la journalisation 319
Affichage des journaux 321
Se connecter avec AWS CloudTrail 322
Informations sur Amazon FSx for Lustre dans CloudTrail 322
Comprendre les entrées du fichier journal Amazon FSx for Lustre 323
Migration vers FSx for Lustre 326
Migration de fichiers avec AWS DataSync 326
Conditions préalables 326
DataSync étapes de base de la migration 327
Sécurité 328
Protection des données 329
Chiffrement des données 330
Confidentialité du trafic inter-réseau 333
Gestion des identités et des accès 334
Public ciblé 335
Authentification par des identités 335
Gestion de l’accès à l’aide de politiques 337
FSx pour Lustre et IAM 338
Exemples de politiques basées sur l’identité 344
AWS politiques gérées 347
Résolution des problèmes 364
Utiliser des tags avec Amazon FSx 366
Utilisation des rôles liés à un service 373
Contrôle d'accès au système de fichiers avec Amazon VPC 380
Groupes de sécurité Amazon VPC 380
Lustre règles du groupe de sécurité VPC client 384

Réseau Amazon VPC ACLs 387
Validation de la conformité 387
Points de terminaison de VPC d'Interface 388
Considérations relatives aux points de terminaison FSx VPC de l'interface Amazon 388
Création d'un point de terminaison VPC d'interface pour Amazon API FSx 389
Création d'une politique de point de terminaison VPC pour Amazon FSx 389
Quotas de service 391
Les quotas que vous pouvez augmenter 391
Quotas de ressources pour chaque système de fichiers 394
Considérations supplémentaires 394
Résolution des problèmes 396
La création d'un système de fichiers échoue 396
Impossible de créer un système de fichiers compatible EFA en raison d'un groupe de sécurité mal configuré 396
Impossible de créer un système de fichiers en raison d'un groupe de sécurité mal configuré 397
Impossible de créer un système de fichiers en raison d'erreurs liées à une capacité insuffisante 397
Impossible de créer un système de fichiers lié à un compartiment S3 398
Le montage du système de fichiers échoue 398
Le montage du système de fichiers échoue immédiatement 398
Le montage du système de fichiers se bloque, puis échoue avec une erreur de dépassement de délai d'attente 399
Le montage automatique échoue et l'instance ne répond pas 399
Le montage du système de fichiers échoue lors du démarrage du système 400
Le montage du système de fichiers à l'aide du nom DNS échoue 400
Vous ne pouvez pas accéder à votre système de fichiers 401
L'adresse IP élastique attachée à l'interface Elastic Network du système de fichiers a été supprimée 401
L'interface Elastic Network du système de fichiers a été modifiée ou supprimée 402
La création d'un DRA échoue 402
Le changement de nom des répertoires prend beaucoup de temps 403
Compartiment S3 lié mal configuré 403
Problèmes de stockage 405
Erreur d'écriture due à l'absence d'espace sur la cible de stockage 405
Stockage déséquilibré sur OSTs 406

Problèmes liés au pilote CSI 409
Informations supplémentaires 410
Configuration d'un calendrier de sauvegarde personnalisé 410
Présentation de l’architecture 411
CloudFormation modèle 412
Déploiement automatique 412
Options supplémentaires 414
Historique de la documentation 416
..... cdxliv

Qu'est-ce qu'Amazon FSx for Lustre ?

FSx for Lustre permet de lancer et d'exécuter facilement et à moindre coût le système de Lustre fichiers populaire et performant. Vous utilisez Lustre pour les charges de travail où la rapidité est importante, telles que l'apprentissage automatique, le calcul haute performance (HPC), le traitement vidéo et la modélisation financière.

Le système de Lustre fichiers est conçu pour les applications qui nécessitent un stockage rapide, lorsque vous souhaitez que votre stockage suive le rythme de vos calculs. Lustrea été conçu pour résoudre le problème du traitement rapide et économique des ensembles de données mondiaux toujours plus nombreux. Il s'agit d'un système de fichiers largement utilisé conçu pour les ordinateurs les plus rapides du monde. Il fournit des latences inférieures à la milliseconde, un débit pouvant atteindre un multiple et TBps des millions d'IOPS. Pour plus d'informationsLustre, consultez le Lustresite Web.

En tant que service entièrement géré, Amazon vous FSx permet de l'utiliser Lustre plus facilement pour les charges de travail où la vitesse de stockage est importante. FSx for Lustre élimine la complexité traditionnelle liée à la configuration et à la gestion des systèmes de Lustre fichiers, vous permettant de créer et d'exécuter un système de fichiers performant éprouvé en quelques minutes. Il propose également plusieurs options de déploiement et classes de stockage afin que vous puissiez optimiser les coûts en fonction de vos besoins.

FSx for Lustre est compatible POSIX, vous pouvez donc utiliser vos applications Linux actuelles sans avoir à apporter de modifications. FSx for Lustre fournit une interface de système de fichiers native et fonctionne comme n'importe quel système de fichiers avec votre système d'exploitation Linux. Il assure également read-after-write la cohérence et prend en charge le verrouillage des fichiers.

Rubriques

- Plusieurs options de déploiement et classes de stockage
- FSx pour Lustre et les référentiels de données
- Accès FSx aux systèmes de fichiers Lustre
- Intégrations avec les services AWS
- Conformité et sécurité
- Hypothèses
- Tarification d'Amazon FSx pour Lustre
- Forums Amazon FSx pour Lustre

- Utilisez-vous Amazon FSx for Lustre pour la première fois ?

Plusieurs options de déploiement et classes de stockage

Amazon FSx for Lustre propose un choix de systèmes de fichiers temporaires et persistants pour répondre aux différents besoins en matière de traitement des données. Les systèmes de fichiers temporaires constituent l'alternative parfaite pour le stockage et le traitement de données sur le court terme. Les données ne sont ni répliquées ni conservées si l'exécution d'un serveur échoue. Les systèmes de fichiers persistants sont idéaux pour le stockage à long terme et les charges de travail axées sur le débit. Dans les systèmes de fichiers persistants, les données sont répliquées et les serveurs de fichiers sont remplacés en cas de défaillance. Pour de plus amples informations, veuillez consulter Options de classe de déploiement et de stockage FSx pour les systèmes de fichiers Lustre.

Amazon FSx for Lustre propose des classes de stockage sur disque SSD (Solid State Drive), Intelligent-Tiering et sur disque dur (HDD) optimisées pour répondre aux différentes exigences en matière de traitement des données :

- La classe de stockage SSD est optimisée pour les charges de travail comportant de petites opérations de fichiers aléatoires et nécessitant un débit allant jusqu'à TBps Il fournit un accès constant avec une latence inférieure à la milliseconde à l'ensemble de données complet.
- La classe de stockage Intelligent-Tiering convient et est recommandée pour la plupart des charges de travail qui ne nécessitent pas une faible latence constante sur l'ensemble de données complet. Il fournit un stockage entièrement élastique et rentable, un débit pouvant atteindre plusieurs fois et un accès avec TBps une latence inférieure à une milliseconde aux données fréquemment consultées grâce à un cache de lecture SSD en option.
- La classe de stockage HDD peut être utilisée avec des charges de travail qui nécessitent une latence constante à un chiffre en ms et un débit pouvant atteindre des dizaines pour GBps l'ensemble de données complet. Vous pouvez éventuellement provisionner un cache de lecture SSD dont la taille correspond à 20 % de la capacité de stockage de votre disque dur.

Pour de plus amples informations, veuillez consulter FSx pour les classes de stockage Lustre.

FSx pour Lustre et les référentiels de données

Vous pouvez lier FSx les systèmes de fichiers Lustre à des référentiels de données sur Amazon S3 ou à des magasins de données sur site.

FSx pour l'intégration du référentiel de données Lustre S3

FSx for Lustre s'intègre à Amazon S3, ce qui vous permet de traiter plus facilement les ensembles de données dans le cloud à l'aide d'un système de fichiers Lustre performant. Lorsqu'il est lié à un compartiment Amazon S3, un système de fichiers FSx for Lustre présente de manière transparente les objets S3 sous forme de fichiers. Amazon FSx importe les listes de tous les fichiers existants dans votre compartiment S3 lors de la création du système de fichiers. Amazon FSx peut également importer des listes de fichiers ajoutés au référentiel de données après la création du système de fichiers. Vous pouvez définir les préférences d'importation en fonction de vos besoins en matière de flux de travail. Le système de fichiers vous permet également de réécrire les données du système de fichiers dans S3. Les tâches de dépôt de données simplifient le transfert de données et de métadonnées entre votre système de fichiers FSx for Lustre et son référentiel de données durable sur Amazon S3. Pour plus d'informations, consultez Utilisation de référentiels de données avec Amazon FSx for Lustre et Tâches du référentiel de données.

FSx pour Lustre et les référentiels de données sur site

Avec Amazon FSx for Lustre, vous pouvez transférer vos charges de travail de traitement de données sur site vers le AWS Cloud en important des données à l'aide Direct Connect de ou. Site-to-Site VPN Pour de plus amples informations, veuillez consulter Utilisation d'Amazon FSx avec vos données sur site.

Accès FSx aux systèmes de fichiers Lustre

Vous pouvez associer les types d'instances de calcul et les images Linux Amazon Machine (AMIs) connectées à un seul système de fichiers FSx pour Lustre.

Les systèmes de fichiers Amazon FSx for Lustre sont accessibles depuis des charges de travail de calcul exécutées sur des instances Amazon Elastic Compute Cloud (Amazon EC2), sur des conteneurs Docker Amazon Elastic Container Service (Amazon ECS) et des conteneurs exécutés sur Amazon Elastic Kubernetes Service (Amazon EKS).

- Amazon EC2 — Vous accédez à votre système de fichiers depuis vos instances de calcul Amazon EC2 à l'aide du client open source. Lustre Les instances Amazon EC2 peuvent accéder à votre système de fichiers depuis d'autres zones de disponibilité au sein du même Amazon Virtual Private Cloud (Amazon VPC), à condition que votre configuration réseau permette l'accès à travers les sous-réseaux du VPC. Une fois votre système de fichiers Amazon FSx for Lustre monté, vous

pouvez travailler avec ses fichiers et répertoires comme vous le feriez avec un système de fichiers local.

- Amazon EKS — Vous accédez à Amazon FSx for Lustre à partir de conteneurs exécutés sur Amazon EKS à l'aide du pilote open source FSx pour Lustre CSI, comme décrit dans le guide de l'utilisateur Amazon EKS. Vos conteneurs exécutés sur Amazon EKS peuvent utiliser des volumes persistants à hautes performances (PVs) soutenus par Amazon FSx for Lustre.
- Amazon ECS — Vous accédez à Amazon FSx for Lustre à partir de conteneurs Docker Amazon ECS sur des instances Amazon EC2. Pour de plus amples informations, veuillez consulter Montage depuis Amazon Elastic Container Service.

Amazon FSx for Lustre est compatible avec les systèmes Linux les plus populaires, AMIs notamment Amazon Linux 2023 et Amazon Linux 2, Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu et SUSE Linux. Le Lustre client est inclus dans Amazon Linux 2023 et Amazon Linux 2. Pour RHEL, CentOS et Ubuntu, AWS Lustre un référentiel client fournit des clients compatibles avec ces systèmes d'exploitation.

Avec FSx for Lustre, vous pouvez transférer vos charges de travail gourmandes en ressources informatiques du local vers le AWS Cloud en important des données sur ou. Direct Connect AWS Virtual Private Network Vous pouvez accéder à votre système de FSx fichiers Amazon sur site, copier des données dans votre système de fichiers selon vos besoins et exécuter des charges de travail intensives sur des instances dans le cloud.

Pour plus d'informations sur les clients, les instances de calcul et les environnements à partir desquels vous pouvez accéder FSx aux systèmes de fichiers Lustre, consultezAccès aux systèmes de fichiers.

Intégrations avec les services AWS

Amazon FSx for Lustre s'intègre à Amazon SageMaker AI en tant que source de données d'entrée. Lorsque vous utilisez SageMaker AI with FSx for Lustre, vos tâches de formation au machine learning sont accélérées en éliminant l'étape initiale de téléchargement depuis Amazon S3. En outre, votre coût total de possession (TCO) est réduit en évitant le téléchargement répétitif d'objets courants pour des tâches itératives sur le même ensemble de données, tout en économisant sur les coûts liés aux requêtes S3. Pour plus d'informations, voir Qu'est-ce que SageMaker l'IA ? dans le manuel Amazon SageMaker AI Developer Guide. Pour découvrir comment utiliser Amazon for Lustre comme source de données FSx pour l' SageMaker IA, consultez Accélérer la formation sur Amazon SageMaker AI

à l'aide des systèmes de fichiers Amazon FSx for Lustre et Amazon EFS sur le blog AWS Machine Learning.

FSx for Lustre s'intègre à AWS Batch l'utilisation de modèles de lancement EC2. AWS Batch vous permet d'exécuter des charges de travail de calcul par lots sur le AWS Cloud, notamment le calcul haute performance (HPC), l'apprentissage automatique (ML) et d'autres charges de travail asynchrones. AWS Batch redimensionne automatiquement et dynamiquement les instances en fonction des besoins en ressources du travail. Pour plus d'informations, voir Qu'est-ce que c'est AWS Batch ? dans le guide de AWS Batch l'utilisateur.

FSx for Lustre s'intègre à AWS ParallelCluster. AWS ParallelCluster est un outil de gestion de clusters open source AWS pris en charge et utilisé pour déployer et gérer des clusters HPC. Il peut créer automatiquement FSx pour les systèmes de fichiers Lustre ou utiliser des systèmes de fichiers existants pendant le processus de création du cluster.

Conformité et sécurité

FSx car les systèmes de fichiers Lustre prennent en charge le chiffrement au repos et en transit. Amazon chiffre FSx automatiquement les données du système de fichiers au repos à l'aide de clés gérées dans AWS Key Management Service (AWS KMS). Les données en transit sont également automatiquement chiffrées sur les systèmes de fichiers dans certains Régions AWS cas lorsqu'elles sont accessibles à partir d'instances Amazon EC2 prises en charge. Pour plus d'informations sur le chiffrement des données dans FSx Lustre, notamment sur les Régions AWS cas où le chiffrement des données en transit est pris en charge, voirChiffrement des données dans Amazon FSx for Lustre. Amazon FSx a été évalué comme étant conforme aux certifications ISO, PCI-DSS et SOC, et est éligible à la loi HIPAA. Pour de plus amples informations, veuillez consulter La sécurité dans Amazon FSx pour Lustre.

Hypothèses

Dans ce guide, nous formulons les hypothèses suivantes :

- Si vous utilisez Amazon Elastic Compute Cloud (Amazon EC2), nous supposons que vous connaissez ce service. Pour plus d'informations sur l'utilisation d'Amazon EC2, consultez la documentation Amazon EC2.
- Nous supposons que vous êtes habitué à utiliser Amazon Virtual Private Cloud (Amazon VPC). Pour plus d'informations sur l'utilisation d'Amazon VPC, consultez le guide de l'utilisateur Amazon VPC.

- Nous partons du principe que vous n'avez pas modifié les règles du groupe de sécurité par défaut de votre VPC sur la base du service Amazon VPC. Si c'est le cas, assurez-vous d'ajouter les règles nécessaires pour autoriser le trafic réseau de votre instance Amazon EC2 vers votre système de fichiers Amazon FSx for Lustre. Pour en savoir plus, consultez Contrôle d'accès au système de fichiers avec Amazon VPC.

Tarification d'Amazon FSx pour Lustre

Avec Amazon FSx for Lustre, il n'y a aucun coût initial de matériel ou de logiciel. Vous ne payez que pour les ressources utilisées, sans engagement minimum, frais d'installation ou frais supplémentaires. Pour plus d'informations sur les prix et les frais associés à ce service, consultez Amazon FSx for Lustre Pricing.

Forums Amazon FSx pour Lustre

Si vous rencontrez des problèmes lors de l'utilisation d'Amazon FSx pour Lustre, consultez les forums.

Utilisez-vous Amazon FSx for Lustre pour la première fois ?

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

1. Si vous êtes prêt à créer votre premier système de fichiers Amazon FSx for Lustre, essayezCommencer à utiliser Amazon FSx pour Lustre.
2. Pour plus d'informations sur les performances, consultez Amazon FSx pour les performances de Lustre.
3. Pour plus d'informations sur la liaison de votre système de fichiers à un référentiel de données de compartiment Amazon S3, consultezUtilisation de référentiels de données avec Amazon FSx for Lustre.
4. Pour plus d'informations sur FSx la sécurité d'Amazon for Lustre, consultezLa sécurité dans Amazon FSx pour Lustre.
5. Pour plus d'informations sur les limites d'évolutivité d'Amazon FSx for Lustre, notamment le débit et la taille du système de fichiers, consultez. Quotas de service pour Amazon FSx pour Lustre
6. Pour plus d'informations sur l'API Amazon FSx for Lustre, consultez le manuel Amazon FSx for Lustre API Reference.

Configuration de Amazon FSx for Lustre

Avant d'utiliser Amazon FSx pour Lustre pour la première fois, effectuez les tâches décrites dans la S'inscrire à Amazon Web Services section. Pour terminer le didacticiel de démarrage, assurez-vous que le compartiment Amazon S3 que vous allez lier à votre système de fichiers possède les autorisations répertoriéesAjouter des autorisations pour utiliser les référentiels de données dans Amazon S3.

Rubriques

- S'inscrire à Amazon Web Services
- Ajouter des autorisations pour utiliser les référentiels de données dans Amazon S3
- Comment FSx Lustre vérifie l'accès aux compartiments S3 liés
- Étape suivante

S'inscrire à Amazon Web Services

Pour configurer AWS, effectuez les tâches suivantes :

1. Inscrivez-vous pour un Compte AWS
2. Création d’un utilisateur doté d’un accès administratif

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d’inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l’utilisateur racine a accès à l’ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un

utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Ajouter des autorisations pour utiliser les référentiels de données dans Amazon S3

Amazon FSx for Lustre est profondément intégré à Amazon S3. Cette intégration signifie que les applications qui accèdent à votre système de fichiers FSx for Lustre peuvent également accéder facilement aux objets stockés dans votre compartiment Amazon S3 associé. Pour de plus amples informations, veuillez consulter Utilisation de référentiels de données avec Amazon FSx for Lustre.

Pour utiliser les référentiels de données, vous devez d'abord accorder à Amazon FSx for Lustre certaines autorisations IAM dans un rôle associé au compte de votre utilisateur administrateur.

Pour intégrer une politique intégrée pour un rôle à l'aide de la console

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau de navigation, choisissez Rôles.

3. Dans la liste, sélectionnez le nom du rôle auquel intégrer une stratégie.
4. Sélectionnez l’onglet Autorisations.
5. Faites défiler jusqu'en bas de la page et choisissez Add inline policy (Ajouter une stratégie en ligne).

> **Note**
>
> Vous ne pouvez pas intégrer de politique intégrée dans un rôle lié à un service dans IAM. Comme le service lié définit si vous pouvez modifier les autorisations du rôle, vous pourrez peut-être ajouter des politiques depuis la console de service, l'API ou l’interface AWS CLI. Pour consulter la documentation relative aux rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et choisissez Oui dans la colonne Rôle lié au service correspondant à votre service.

6. Choisissez Créer des politiques avec l'éditeur visuel
7. Ajoutez la déclaration de politique d'autorisation suivante.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:CreateServiceLinkedRole",
            "iam:AttachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/*"
    }
}
```

Une fois que vous avez créé une stratégie en ligne, elle est automatiquement intégrée à votre rôle. Pour plus d’informations sur les rôles liés à un service, consultez Utilisation de rôles liés à un service pour Amazon FSx.

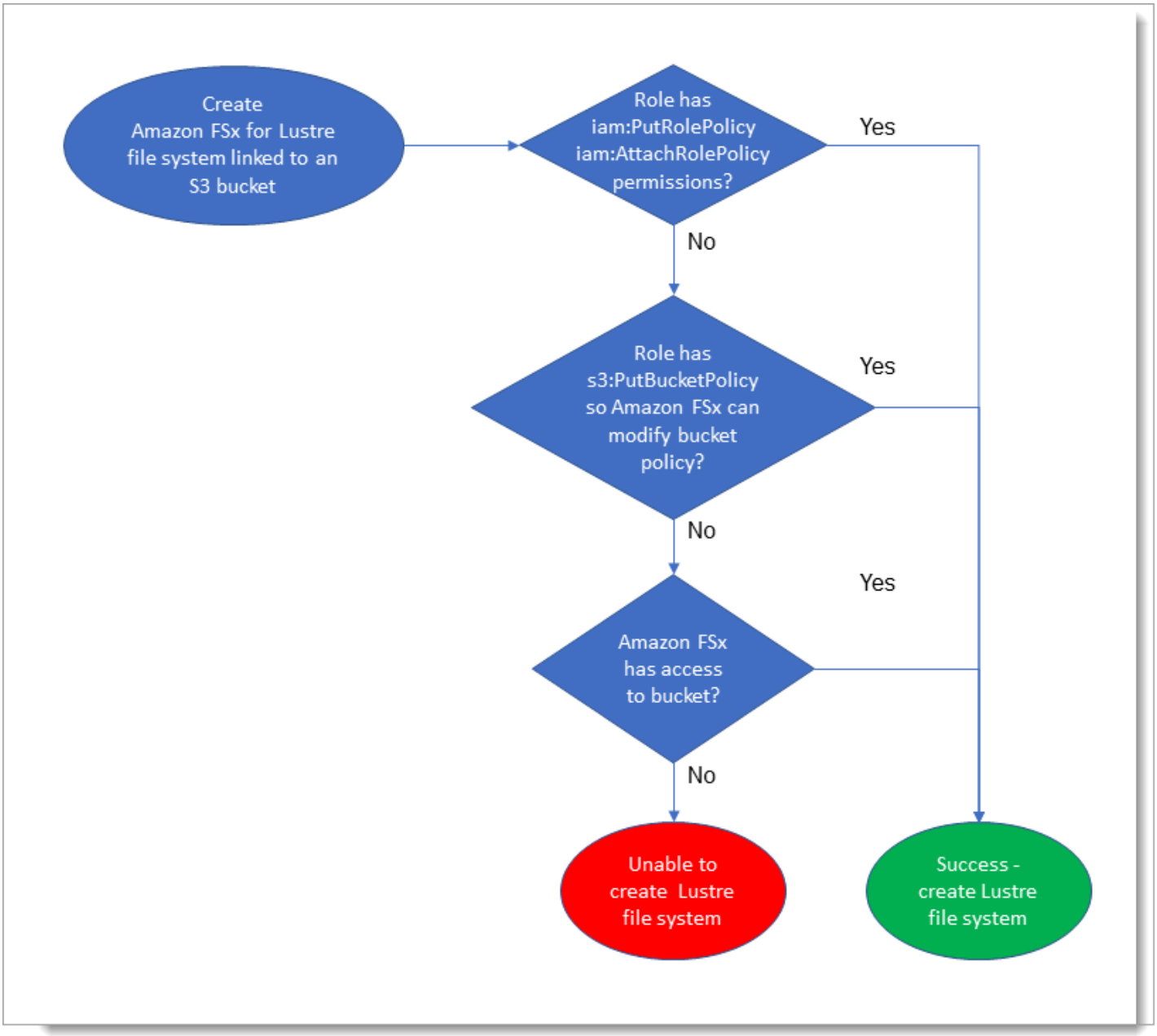
Comment FSx Lustre vérifie l'accès aux compartiments S3 liés

Si le rôle IAM que vous utilisez pour créer le système de fichiers FSx for Lustre ne dispose pas des `iam:PutRolePolicy` autorisations `iam:AttachRolePolicy` et, Amazon FSx vérifie s'il peut mettre à jour votre politique de compartiment S3. Amazon FSx peut mettre à jour votre politique de compartiment si l'`s3:PutBucketPolicy`autorisation est incluse dans votre rôle IAM afin de permettre au système de FSx fichiers Amazon d'importer ou d'exporter des données vers votre compartiment S3. S'il est autorisé à modifier la politique de compartiment, Amazon FSx ajoute les autorisations suivantes à la politique de compartiment :

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:PutObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutBucketPolicy`
- `s3:DeleteBucketPolicy`

Si Amazon ne FSx peut pas modifier la politique de compartiment, il vérifie ensuite si la politique de compartiment existante autorise Amazon à FSx accéder au compartiment.

Si toutes ces options échouent, la demande de création du système de fichiers échoue. Le schéma suivant illustre les contrôles effectués par Amazon FSx pour déterminer si un système de fichiers peut accéder au compartiment S3 auquel il sera lié.



Étape suivante

Pour commencer à utiliserFSx for Lustre, consultez Commencer à utiliser Amazon FSx pour Lustre les instructions pour créer vos ressources Amazon FSx for Lustre.

Commencer à utiliser Amazon FSx pour Lustre

Vous découvrirez ci-dessous comment commencer à utiliser Amazon FSx pour Lustre. Ces étapes vous guident dans la création d'un système de fichiers Amazon FSx for Lustre et l'accès à celui-ci depuis vos instances de calcul. Ils montrent éventuellement comment utiliser votre système de fichiers Amazon FSx for Lustre pour traiter les données de votre compartiment Amazon S3 avec vos applications basées sur des fichiers.

Cet exercice de mise en route comprend les étapes suivantes.

Rubriques

- Prérequis
- Étape 1 : Créez votre système de fichiers FSx for Lustre
- Étape 2 : Installation et configuration du Lustre client
- Étape 3 : monter le système de fichiers
- Étape 4 : Exécutez votre flux de travail
- Étape 5 : Nettoyer les ressources

Prérequis

Pour effectuer cet exercice de mise en route, vous avez besoin des éléments suivants :

- Un AWS compte disposant des autorisations nécessaires pour créer un système de fichiers Amazon FSx for Lustre et une EC2 instance Amazon. Pour de plus amples informations, veuillez consulter Configuration de Amazon FSx for Lustre.
- Créez un groupe de sécurité Amazon VPC à associer à votre système de fichiers FSx for Lustre, et ne le modifiez pas après la création du système de fichiers. Pour plus d'informations, consultez Pour créer un groupe de sécurité pour votre système de FSx fichiers Amazon.
- Une EC2 instance Amazon exécutant une version Linux prise en charge dans votre cloud privé virtuel (VPC) sur la base du service Amazon VPC. Pour cet exercice de mise en route, nous vous recommandons d'utiliser Amazon Linux 2023. Vous allez installer le Lustre client sur cette EC2 instance, puis monter votre système de fichiers FSx for Lustre sur l' EC2 instance. Pour plus d'informations sur la création d'une EC2 instance, consultez Getting started : Launch an instance ou Launch your instance dans le guide de EC2 l'utilisateur Amazon.

Outre Amazon Linux 2023, le Lustre client prend en charge les systèmes d'exploitation Amazon Linux 2, Red Hat Enterprise Linux (RHEL), CentOS, Rocky Linux, SUSE Linux Enterprise Server et Ubuntu. Pour de plus amples informations, veuillez consulter Lustrecompatibilité entre le système de fichiers et le noyau client.

- Lorsque vous créez votre EC2 instance Amazon pour cet exercice de mise en route, gardez à l'esprit les points suivants :
  - Nous vous recommandons de créer votre instance dans votre VPC par défaut.
  - Nous vous recommandons d'utiliser le groupe de sécurité par défaut lors de la création de votre EC2 instance.
- Déterminez le type de système de fichiers Amazon FSx for Lustre que vous souhaitez créer, à gratter ou à conserver. Pour de plus amples informations, veuillez consulter Options de classe de déploiement et de stockage FSx pour les systèmes de fichiers Lustre.
- Chaque système de fichiers FSx pour Lustre nécessite une adresse IP pour chaque serveur de métadonnées (MDS) et une adresse IP pour chaque serveur de stockage (OSS). Pour de plus amples informations, veuillez consulter Adresses IP pour les systèmes de fichiers.
- Un compartiment Amazon S3 stockant les données à traiter par votre charge de travail. Le compartiment S3 sera le référentiel de données durable lié à votre système de fichiers FSx for Lustre.

Étape 1 : Créez votre système de fichiers FSx for Lustre

Vous créez votre système de fichiers dans la FSx console Amazon. Notez que tous les systèmes de fichiers FSx pour Lustre sont basés sur la Lustre version 2.15 lorsqu'ils sont créés à l'aide de la FSx console Amazon.

Pour créer votre système de fichiers .

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord, choisissez Créer un système de fichiers pour démarrer l'assistant de création de système de fichiers.
3. Choisissez FSx for Lustrepuis cliquez sur Suivant pour afficher la page Créer un système de fichiers.

   Commencez votre configuration par la section Détails du système de fichiers.

4. Pour Nom du système de fichiers facultatif, indiquez le nom de votre système de fichiers. Vous pouvez utiliser jusqu'à 256 lettres Unicode, espaces blancs et chiffres, ainsi que les caractères spéciaux + - =. _ :/.
5. Pour Déploiement et classe de stockage, choisissez l'une des options suivantes :

   - Choisissez un SSD persistant pour le stockage à long terme et pour les charges de travail sensibles à la latence. Avec le stockage SSD, la quantité de stockage que vous fournissez vous est facturée.

     Vous pouvez également choisir d'activer EFA pour activer la prise en charge d'Elastic Fabric Adapter (EFA) pour le système de fichiers. Pour plus d'informations sur l'EFA, consultezUtilisation de systèmes de fichiers compatibles avec EFA.
   - Optez pour une hiérarchisation persistante et intelligente pour un stockage à long terme. La classe de stockage Intelligent-Tiering fournit un stockage entièrement élastique et économique adapté à la plupart des charges de travail, ainsi qu'un cache de lecture SSD en option qui fournit des latences SSD pour la lecture des données fréquemment consultées. Avec Intelligent-Tiering, vous êtes facturé pour les données que vous stockez, en fonction de la taille de votre ensemble de données, et il n'est pas nécessaire de spécifier la taille du système de fichiers.

     Vous pouvez également choisir d'activer EFA pour activer la prise en charge d'Elastic Fabric Adapter (EFA) pour le système de fichiers.
   - Choisissez Scratch, le déploiement de SSD pour le stockage temporaire et le traitement des données à court terme. Avec le stockage SSD, la quantité de stockage que vous fournissez vous est facturée.
6. Choisissez le débit de votre système de fichiers. Vous payez le débit que vous allouez.

   - Pour le stockage SSD persistant, choisissez une valeur de débit par unité de stockage. Le débit par unité de stockage est le débit de lecture et d'écriture pour chaque tebioctet (TiB) de stockage provisionné.
   - Pour le stockage SSD Scratch, choisissez une valeur de débit par unité de stockage.
   - Pour le stockage à hiérarchisation intelligente, choisissez une valeur de capacité de débit.
7. Pour Capacité de stockage (classe de stockage SSD uniquement), définissez la capacité de stockage de votre système de fichiers, en To :

   - Pour un type de déploiement SSD persistant, définissez-le sur une valeur de 1,2 TiB, 2,4 TiB ou par incréments de 2,4 TiB.

- Pour un type de déploiement SSD persistant compatible EFA, définissez cette valeur par incréments de 4,8 TiB, 9,6 TiB, 19,2 TiB et 38,4 TiB pour les niveaux de débit de 1 000, 500, 250 et 125 /TiB, respectivement. MBps

Vous pouvez augmenter la capacité de stockage selon vos besoins après avoir créé le système de fichiers. Pour de plus amples informations, veuillez consulter Gestion de la capacité de stockage.

8. Pour la configuration des métadonnées, choisissez l'une des options suivantes pour définir le nombre d'IOPS de métadonnées pour votre système de fichiers :

   - Choisissez Automatique (classe de stockage SSD uniquement) si vous souhaitez qu'Amazon FSx for Lustre provisionne et adapte automatiquement les IOPS de métadonnées sur votre système de fichiers en fonction de la capacité de stockage de ce dernier.
   - Choisissez Provisioned par l'utilisateur si vous souhaitez spécifier le nombre d'IOPS de métadonnées à provisionner pour votre système de fichiers avec une classe de stockage SSD ou Intelligent-Tiering. Les valeurs valides sont les suivantes :
     - Pour les systèmes de fichiers SSD, les valeurs valides sont `15003000`,`6000`,`12000`, et des multiples `12000` allant jusqu'à un maximum de`192000`.
     - Pour les systèmes de fichiers à hiérarchisation intelligente, les valeurs valides sont et. `6000` `12000`

   Pour plus d'informations sur les IOPS des métadonnées, consultezLustreconfiguration des performances des métadonnées.

9. Pour le cache de lecture SSD (hiérarchisation intelligente uniquement), sélectionnez Automatique (proportionnel à la capacité de débit) ou Personnalisé (provisionné par l'utilisateur). Avec l'option Automatique, Amazon FSx for Lustre choisit automatiquement une taille de cache de lecture en fonction du débit que vous avez configuré. Si vous connaissez la taille approximative de votre ensemble de données de travail actif, vous pouvez sélectionner Personnalisé pour personnaliser la taille du cache de lecture SSD. Pour de plus amples informations, veuillez consulter Gestion du cache de lecture SSD provisionné.
10. Pour le type de compression des données, choisissez AUCUN pour désactiver la compression des données ou choisissez LZ4d'activer la compression des données avec l' LZ4 algorithme. Pour de plus amples informations, veuillez consulter Lustrecompression de données.
11. Dans la section Réseau et sécurité, fournissez les informations suivantes sur le réseau et le groupe de sécurité :

- Pour Virtual Private Cloud (VPC), choisissez le VPC que vous souhaitez associer à votre système de fichiers. Pour cet exercice de mise en route, choisissez le même VPC que celui que vous avez choisi pour votre instance Amazon EC2 .
- Pour les groupes de sécurité VPC, l'ID du groupe de sécurité par défaut de votre VPC doit déjà être ajouté.

  Si vous n'utilisez pas le groupe de sécurité par défaut, assurez-vous que la règle entrante suivante est ajoutée au groupe de sécurité que vous utilisez pour cet exercice de démarrage.

Type	Protocole	Plage de ports	Source	Description
Tous les TCP	TCP	0-65535	Personnalisé *the_ID_of_this_security_group*	Règle relative au Lustre trafic entrant

> **Important**
>
> - Assurez-vous que le groupe de sécurité que vous utilisez suit les instructions de configuration fournies dansContrôle d'accès au système de fichiers avec Amazon VPC. Vous devez configurer le groupe de sécurité pour autoriser le trafic entrant sur les ports 988 et 1018-1023 à partir du groupe de sécurité lui-même ou du CIDR du sous-réseau complet, qui est nécessaire pour permettre aux hôtes du système de fichiers de communiquer entre eux.
> - Si vous créez un système de fichiers compatible EFA, assurez-vous de spécifier un groupe de sécurité compatible EFA.

- Pour Sous-réseau, choisissez une valeur dans la liste des sous-réseaux disponibles.

12. Pour la section Chiffrement, les options disponibles varient en fonction du type de système de fichiers que vous créez :

    - Dans le cas d'un système de fichiers persistant, vous pouvez choisir une clé de chiffrement AWS Key Management Service (AWS KMS) pour chiffrer les données de votre système de fichiers au repos.

- Dans le cas d'un système de fichiers scratch, les données au repos sont chiffrées à l'aide de clés gérées par AWS.
- Pour les systèmes de fichiers Scratch 2 et persistants, les données en transit sont chiffrées automatiquement lorsque le système de fichiers est accessible à partir d'un type d' EC2 instance Amazon compatible. Pour de plus amples informations, veuillez consulter chiffrement des données en transit.

13. Pour la section facultative Import/Export de référentiels de données, la liaison de votre système de fichiers aux référentiels de données Amazon S3 est désactivée par défaut. Pour plus d'informations sur l'activation de cette option et la création d'une association de référentiel de données à un compartiment S3 existant, consultezPour lier un compartiment S3 lors de la création d'un système de fichiers (console).

> ⚠ Important
>
> - La sélection de cette option désactive également les sauvegardes et vous ne pourrez pas les activer lors de la création du système de fichiers.
> - Si vous liez un ou plusieurs systèmes de fichiers Amazon FSx for Lustre à un compartiment Amazon S3, ne supprimez pas le compartiment Amazon S3 tant que tous les systèmes de fichiers liés n'ont pas été supprimés.
> - Les systèmes de fichiers à hiérarchisation intelligente ne prennent pas en charge les liens vers les référentiels de données Amazon S3.

14. Pour la journalisation facultative, la journalisation est activée par défaut. Lorsque cette option est activée, les défaillances et les avertissements relatifs à l'activité du référentiel de données sur votre système de fichiers sont enregistrés dans Amazon CloudWatch Logs. Pour plus d'informations sur la configuration de la journalisation, consultezGestion de la journalisation.
15. Dans Backup and maintenance optional, vous pouvez effectuer les opérations suivantes.

- Désactivez la sauvegarde automatique quotidienne. Cette option est activée par défaut, sauf si vous avez activé Import/Export du référentiel de données.
- Définissez l'heure de début de la fenêtre de sauvegarde automatique quotidienne.
- Définissez la période de conservation automatique des sauvegardes, comprise entre 1 et 35 jours.
- Définissez l'heure de début de la fenêtre de maintenance hebdomadaire ou conservez-la sur la valeur par défaut Aucune préférence.

Pour plus d'informations, consultez Protection de vos données grâce à des sauvegardes et Fenêtres FSx de maintenance Amazon pour Lustre.

16. Pour Root Squash (facultatif), le root squash est désactivé par défaut. Pour plus d'informations sur l'activation et la configuration de Root Squash, consultezPour activer Root Squash lors de la création d'un système de fichiers (console).
17. Créez les balises que vous souhaitez appliquer à votre système de fichiers.
18. Choisissez Suivant pour afficher la page récapitulative de la création d'un système de fichiers.
19. Vérifiez les paramètres de votre système de fichiers Amazon FSx for Lustre, puis choisissez Create file system.

Maintenant que vous avez créé votre système de fichiers, notez son nom de domaine complet et son nom de montage pour une étape ultérieure. Vous pouvez trouver le nom de domaine complet et le nom de montage d'un système de fichiers en choisissant le nom du système de fichiers dans le tableau de bord des systèmes de fichiers, puis en choisissant Attacher.

Étape 2 : Installation et configuration du Lustre client

Avant de pouvoir accéder à votre système de fichiers Amazon FSx for Lustre depuis votre EC2 instance Amazon, vous devez effectuer les opérations suivantes :

- Vérifiez que votre EC2 instance répond aux exigences minimales du noyau.
- Mettez à jour le noyau si nécessaire.
- Téléchargez et installez le Lustre client.

Pour vérifier la version du noyau et télécharger le Lustre client

1. Ouvrez une fenêtre de terminal sur votre EC2 instance.
2. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance de calcul en exécutant la commande suivante.

```
uname -r
```

3. Effectuez l'une des actions suivantes :

- Si la commande est renvoyée `6.1.79-99.167.amzn2023.x86_64` pour les EC2 instances basées sur x86, `6.1.79-99.167.amzn2023.aarch64` ou supérieures pour les instances basées sur Graviton2, téléchargez et installez le EC2 client à l'aide de la Lustre commande suivante.

  ```
  sudo dnf install -y lustre-client
  ```

- Si la commande renvoie un résultat inférieur à celui `6.1.79-99.167.amzn2023.x86_64` des EC2 instances basées sur x86, ou inférieur `6.1.79-99.167.amzn2023.aarch64` à celui des instances basées sur Graviton2 EC2 , mettez à jour le noyau et redémarrez votre EC2 instance Amazon en exécutant la commande suivante.

  ```
  sudo dnf -y update kernel && sudo reboot
  ```

  Vérifiez que le noyau a été mis à jour à l'aide de la uname -r commande. Téléchargez et installez ensuite le Lustre client comme décrit ci-dessus.

Pour plus d'informations sur l'installation du Lustre client sur d'autres distributions Linux, consultezInstallation du Lustre client.

Étape 3 : monter le système de fichiers

Pour monter votre système de fichiers, vous allez créer un répertoire de montage, ou point de montage, puis monter le système de fichiers sur votre client et vérifier que celui-ci peut accéder au système de fichiers.

Pour monter votre système de fichiers

1. Créez un répertoire pour le montage point à l'aide de la commande suivante.

   ```
   sudo mkdir -p /mnt/fsx
   ```

2. Montez le système de fichiers Amazon FSx for Lustre dans le répertoire que vous avez créé. Utilisez la commande suivante et remplacez les éléments suivants :

   - Remplacez *`file_system_dns_name`* par le nom du système de noms de domaine (DNS) actuel du système de fichiers.

- *mountname*Remplacez-le par le nom de montage du système de fichiers, que vous pouvez obtenir en exécutant la describe-file-systems AWS CLI commande ou en exécutant l'opération DescribeFileSystemsAPI.

```
sudo mount -t lustre -o relatime,flock file_system_dns_name@tcp:/mountname /mnt/fsx
```

Cette commande permet de monter votre système de fichiers avec deux options, `-o relatime` et `flock` :

- `relatime`— Bien que l'`atime`option conserve `atime` (temps d'accès aux inodes) les données pour chaque accès à un fichier, elle conserve également les `relatime` `atime` données, mais pas pour chaque accès à un fichier. Lorsque l'`relatime`option est activée, les `atime` données sont écrites sur le disque uniquement si le fichier a été modifié depuis la dernière mise à jour des `atime` données (`mtime`), ou si le dernier accès au fichier remonte à un certain temps (6 heures par défaut). L'utilisation de l'`atime`option `relatime` ou optimisera les processus de publication des fichiers.

  > **Note**
  >
  > Si votre charge de travail nécessite un temps d'accès précis, vous pouvez utiliser l'option de `atime` montage. Cela peut toutefois avoir un impact sur les performances de la charge de travail en augmentant le trafic réseau requis pour maintenir des valeurs de temps d'accès précises.
  > Si votre charge de travail ne nécessite pas de temps d'accès aux métadonnées, l'utilisation de l'option de `noatime` montage pour désactiver les mises à jour du temps d'accès peut apporter un gain de performances. Sachez que les processus `atime` ciblés tels que la publication de fichiers ou la publication de la validité des données seront inexacts lors de leur publication.

- `flock`— Active le verrouillage des fichiers pour votre système de fichiers. Si vous ne souhaitez pas activer le verrouillage des fichiers, utilisez la `mount` commande sans`flock`.

3. Vérifiez que la commande mount a réussi en répertoriant le contenu du répertoire dans lequel vous avez monté le système de fichiers`/mnt/fsx`, à l'aide de la commande suivante.

```
ls /mnt/fsx
import-path  lustre
```

```
$
```

Vous pouvez également utiliser la `df` commande suivante.

```
df
Filesystem                      1K-blocks    Used  Available Use% Mounted on
devtmpf                          1001808       0    1001808   0% /dev
tmpfs                            1019760       0    1019760   0% /dev/shm
tmpfs                            1019760     392    1019368   1% /run
tmpfs                            1019760       0    1019760   0% /sys/fs/cgroup
/dev/xvda1                       8376300 1263180    7113120  16% /
123.456.789.0@tcp:/mountname  3547698816   13824 3547678848   1% /mnt/fsx
tmpfs                             203956       0     203956   0% /run/user/1000
```

Les résultats indiquent que le système de FSx fichiers Amazon est montéon /mnt/fsx.

Étape 4 : Exécutez votre flux de travail

Maintenant que votre système de fichiers a été créé et monté sur une instance de calcul, vous pouvez l'utiliser pour exécuter votre charge de travail de calcul à hautes performances.

Vous pouvez créer une association de référentiel de données pour lier votre système de fichiers à un référentiel de données Amazon S3. Pour plus d'informations, consultezLier votre système de fichiers à un compartiment Amazon S3.

Après avoir lié votre système de fichiers à un référentiel de données Amazon S3, vous pouvez à tout moment exporter les données que vous avez écrites dans votre système de fichiers vers votre compartiment Amazon S3. Depuis un terminal sur l'une de vos instances de calcul, exécutez la commande suivante pour exporter un fichier vers votre compartiment Amazon S3.

```
sudo lfs hsm_archive file_name
```

Pour plus d'informations sur la façon d'exécuter rapidement cette commande sur un dossier ou une grande collection de fichiers, consultezExportation de fichiers à l'aide de commandes HSM.

Étape 5 : Nettoyer les ressources

Une fois cet exercice terminé, vous devez suivre ces étapes pour nettoyer vos ressources et protéger votre AWS compte.

Pour nettoyer des ressources

1. Si vous souhaitez effectuer une exportation finale, exécutez la commande suivante.

   ```
   nohup find /mnt/fsx -type f -print0 | xargs -0 -n 1 sudo lfs hsm_archive &
   ```

2. Sur la EC2 console Amazon, mettez fin à votre instance. Pour plus d'informations, consultez Résilier votre instance dans le guide de EC2 l'utilisateur Amazon.
3. Sur la console Amazon FSx for Lustre, supprimez votre système de fichiers en suivant la procédure suivante :

   a. Dans le volet de navigation, sélectionnez Systèmes de fichiers.
   b. Choisissez le système de fichiers que vous souhaitez supprimer dans la liste des systèmes de fichiers du tableau de bord.
   c. Dans Actions, choisissez Supprimer le système de fichiers.
   d. Dans la boîte de dialogue qui apparaît, indiquez si vous souhaitez effectuer une sauvegarde finale du système de fichiers. Indiquez ensuite l'ID du système de fichiers pour confirmer la suppression. Choisissez Supprimer le système de fichiers.
4. Si vous avez créé un compartiment Amazon S3 pour cet exercice, et si vous ne souhaitez pas conserver les données que vous avez exportées, vous pouvez désormais le supprimer. Pour plus d'informations, consultez Supprimer un compartiment dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Options de classe de déploiement et de stockage FSx pour les systèmes de fichiers Lustre

Amazon FSx for Lustre propose deux options de déploiement de systèmes de fichiers : persistant et scratch. Il propose trois classes de stockage : SSD (disque SSD), Intelligent-Tiering et HDD (disque dur).

Vous choisissez le type de déploiement du système de fichiers et la classe de stockage lorsque vous créez un nouveau système de fichiers à l' AWS Management Console aide de l'API, the AWS Command Line Interface (AWS CLI) ou Amazon FSx for Lustre. Pour plus d'informations, consultez Étape 1 : Créez votre système de fichiers FSx for Lustre et consultez CreateFileSystemle Amazon FSx API Reference.

Systèmes de fichiers persistants

Les systèmes de fichiers persistants sont conçus pour le stockage et les charges de travail à long terme. Pour les systèmes de fichiers SSD et HDD, les données sont automatiquement répliquées dans la même zone de disponibilité que celle dans laquelle se trouve le système de fichiers. Pour les systèmes de fichiers à hiérarchisation intelligente, les données sont répliquées sur plusieurs zones de disponibilité. Les volumes de données attachés aux serveurs de fichiers sont répliqués indépendamment des serveurs de fichiers auxquels ils sont attachés.

Amazon surveille FSx en permanence les systèmes de fichiers persistants pour détecter les défaillances matérielles et remplace automatiquement les composants de l'infrastructure en cas de panne. Sur un système de fichiers persistant, si un serveur de fichiers devient indisponible, il est automatiquement remplacé dans les minutes qui suivent la panne. Pendant ce temps, le client demande des données sur ce serveur de manière transparente et finit par réussir après le remplacement du serveur de fichiers. Les données des systèmes de fichiers persistants sont répliquées sur des disques, et tous les disques défaillants sont automatiquement remplacés de manière transparente.

Utilisez des systèmes de fichiers persistants pour le stockage à long terme et pour les charges de travail axées sur le débit qui s'exécutent pendant de longues périodes ou indéfiniment, et qui peuvent être sensibles aux interruptions de disponibilité.

Les types de déploiement persistants chiffrent automatiquement les données en transit lorsqu'elles sont accessibles depuis des instances Amazon EC2 qui prennent en charge le chiffrement en transit.

Amazon FSx for Lustre prend en charge deux types de déploiement persistants : Persistent 1 et Persistent 2.

Type de déploiement persistant 2

Persistent 2 est le type de déploiement persistant de dernière génération, parfaitement adapté aux cas d'utilisation qui nécessitent un stockage à long terme et qui nécessitent les niveaux les plus élevés d'IOPS et de débit. Les systèmes de fichiers Persistent 2 prennent en charge les classes de stockage SSD et Intelligent-Tiering.

Vous pouvez créer des systèmes de fichiers Persistent 2 avec une configuration de métadonnées et EFA activé à l'aide de la FSx console Amazon et de FSx l'API Amazon. AWS Command Line Interface

Type de déploiement persistant 1

Le type de déploiement Persistent 1 convient parfaitement aux cas d'utilisation nécessitant un stockage à long terme. Les types de déploiement persistants 1 prennent en charge les classes de stockage SSD (Solid State Drive) et HDD (disque dur).

Vous pouvez créer des types de déploiement Persistent 1 uniquement à l'aide de l' FSx API AWS CLI et de l'Amazon.

Systèmes de fichiers Scratch

Les systèmes de fichiers Scratch sont conçus pour le stockage temporaire et le traitement des données à court terme. Les données ne sont pas répliquées et ne sont pas conservées en cas de défaillance d'un serveur de fichiers. Les systèmes de fichiers Scratch fournissent un débit en rafale élevé, jusqu'à six fois supérieur au débit de base de 200 par MBps TiB de capacité de stockage. Pour de plus amples informations, veuillez consulter Caractéristiques de performance des classes de stockage SSD et HDD.

Utilisez des systèmes de fichiers temporaires lorsque vous avez besoin d'un stockage optimisé en termes de coûts pour des charges de travail lourdes à court terme.

Sur un système de fichiers temporaire, les serveurs de fichiers ne sont pas remplacés s'ils tombent en panne et les données ne sont pas répliquées. Si un serveur de fichiers ou un disque de stockage devient indisponible sur un système de fichiers Scratch, les fichiers stockés sur d'autres serveurs

restent accessibles. Si les clients tentent d'accéder aux données qui se trouvent sur le serveur ou le disque indisponible, ils rencontrent une I/O erreur immédiate.

Le tableau suivant illustre la disponibilité ou la durabilité pour lesquelles les systèmes de fichiers scratch de la taille d'exemple sont conçus, au cours d'une journée et d'une semaine. Dans la mesure où les systèmes de fichiers de plus grande taille comportent davantage de serveurs de fichiers et de disques, les probabilités de défaillance augmentent.

Taille du système de fichiers (TiB)	Nombre de serveurs de fichiers	Disponibilité/durabilité sur une journée	Disponibilité/durabilité supérieure à une semaine
1.2	2	99,9 %	99,4 %
2,4	2	99,9 %	99,4 %
4.8	3	99,8 %	99,2 %
9,6	5	99,8 %	98,6 %
50,4	22	99,1 %	93,9 %

Adresses IP pour les systèmes de fichiers

Chaque système de fichiers FSx pour Lustre nécessite une adresse IP pour chaque serveur de métadonnées (MDS) et une adresse IP pour chaque serveur de stockage (OSS).

Systèmes de fichiers utilisant la classe de stockage SSD ou HDD

Type de système de fichiers	Débit, /TiB MBps	Stockage par OSS
Persistent 2 EFA*	125	38,4 TiB par OSS
	250	19,2 TiB par OSS
	500	9,6 TiB par OSS

Type de système de fichiers	Débit, /TiB MBps	Stockage par OSS
	1 000	4,8 TiB par OSS
Persistant 2 sans EFA*	125, 250, 500, 1 000	2,4 TiB par OSS
1 SSD persistant	50, 100, 200	2,4 TiB par OSS
Disque dur persistant	12	6 TiB par OSS
	40	1,8 TiB par OSS
Scratch 2	200	2,4 TiB par OSS
Scratch 1	200	3,6 TiB par OSS

Systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering

Type de système de fichiers	Débit par OSS
Hiérarchisation intelligent*	4000 MBps par OSS

> **Note**
>
> * Amazon fournit FSx un serveur de métadonnées pour 12 000 IOPS de métadonnées sur des systèmes de fichiers SSD Persistent 2 et Intelligent-Tiering configurés avec une configuration de métadonnées.
> Les systèmes de fichiers Amazon FSx for Lustre Intelligent-Tiering prennent en charge un maximum de 512 TiB de stockage par système d'exploitation.

FSx pour les classes de stockage Lustre

Amazon FSx for Lustre propose des classes de stockage sur disque SSD (Solid State Drive), Intelligent-Tiering et sur disque dur (HDD) optimisées pour répondre aux différentes exigences en matière de traitement des données :

- La classe de stockage SSD fournit un accès à faible latence (inférieur à la milliseconde) à l'ensemble de données complet. La classe de stockage SSD est provisionnée, ce qui signifie que vous spécifiez une taille de système de fichiers et que vous payez les frais de stockage correspondant à la quantité de stockage allouée. Utilisez la classe de stockage SSD pour les charges de travail sensibles à la latence qui nécessitent les performances d'un stockage 100 % flash pour toutes les données.

  Les systèmes de fichiers persistants à 2 avec stockage SSD prennent en charge des niveaux de débit supérieurs par unité de stockage (250, 500 ou 1 000 MBps par TiB) par rapport aux systèmes de fichiers persistants 1. Pour un système de fichiers Persistent 1 avec stockage SSD, le débit par unité de stockage est de 50, 100 ou 200 MBps par TiB. Pour un système de fichiers Scratch avec stockage SSD, le débit par unité de stockage est de 200 MBps par TiB.
- La classe de stockage Intelligent-Tiering fournit un stockage entièrement élastique et hiérarchisé de manière intelligente. L'élasticité signifie que vous payez pour la quantité de données que vous stockez et que vous n'avez pas à spécifier la taille du système de fichiers. La hiérarchisation intelligente signifie que vous payez automatiquement moins pour stocker des données auxquelles vous n'avez pas accédé récemment. Cette classe de stockage optimise automatiquement les coûts en hiérarchisant les données confidentielles vers des niveaux de stockage moins coûteux. Vous pouvez configurer un cache de lecture SSD en option pour un accès à faible latence (inférieur à une milliseconde) aux données auxquelles vous accédez fréquemment. La classe de stockage Intelligent-Tiering offre le meilleur équilibre entre prix et performances pour la plupart des charges de travail. Utilisez la classe de stockage Intelligent-Tiering pour les charges de travail compatibles avec le cache et ne nécessitant pas les performances d'un stockage 100 % flash pour toutes les données. Les systèmes de fichiers à hiérarchisation intelligente prennent en charge des capacités de débit par incréments de 4 000. MBps
- La classe de stockage HDD peut être utilisée avec des charges de travail nécessitant une latence constante d'un chiffre en ms pour toutes les données. Vous pouvez configurer un cache de lecture SSD en option dont la taille correspond à 20 % de la capacité de stockage de votre disque dur afin de fournir un accès à faible latence aux données fréquemment consultées. Avec le stockage sur disque dur, vous spécifiez la taille du système de fichiers et vous payez pour la quantité de

stockage que vous fournissez. Pour un système de fichiers Persistent 1 avec stockage sur disque dur, le débit par unité de stockage est de 12 ou 40 MBps par TiB.

Pour plus d'informations sur les performances de ces classes de stockage, reportez-vous Caractéristiques de performance des classes de stockage SSD et HDD aux sections etCaractéristiques de performance de la classe de stockage Intelligent-Tiering.

Comment la classe de stockage Intelligent-Tiering hiérarchise les données

La classe de stockage Amazon FSx Intelligent-Tiering stocke automatiquement les données sur trois niveaux d'accès. Il est conçu pour optimiser les coûts de stockage en déplaçant automatiquement les données vers le niveau d'accès le plus rentable, sans impact sur les performances ni surcharge opérationnelle. La classe de stockage Intelligent-Tiering hiérarchise automatiquement les données en fonction de l'heure du dernier accès, optimisant ainsi automatiquement les coûts pour les données moins actives :

- Les données consultées au cours des 30 derniers jours sont stockées dans le niveau Accès fréquent.
- Les données qui n'ont pas été consultées pendant 30 jours consécutifs passent automatiquement au niveau Accès peu fréquent et coûtent moins cher que les données du niveau Accès fréquent.
- Les données qui n'ont pas été consultées pendant 90 jours consécutifs passent automatiquement au niveau Archive Instant Access et coûtent moins cher que les données du niveau Accès peu fréquent.

Lorsque vous accédez aux données dans les niveaux Accès peu fréquent ou Accès instantané aux archives, les données reviennent automatiquement au niveau Accès fréquent. En outre, des opérations telles que la modification de la capacité de débit (qui rééquilibre les données entre elles OSTs), le redécoupage de fichiers ou de répertoires ou l'utilisation de « lfs migrate » peuvent ramener certaines données vers le niveau d'accès fréquent.

Tous les accès aux données non mises en cache présentent les mêmes caractéristiques de performance, quel que soit le niveau des données, et il n'y a pas de coûts d'IOPS, de récupération ou de transition supplémentaires au-delà de vos coûts d'exploitation normaux. read/write

Disponibilité du type de déploiement

Les types de déploiement Scratch 2, Persistent 1 et Persistent 2 sont disponibles dans les catégories suivantes Régions AWS :

Région AWS	Persistant (2)	Persistant 1	Scratch 2
USA Est (Ohio)	✓	✓	✓
USA Est (Virginie du Nord)	✓	✓	✓
Zone locale de l'est des États-Unis (Atlanta)	✓ *		
Zone locale de l'est des États-Unis (Dallas)	✓ *		
USA Ouest (Californie du Nord)	✓	✓	✓
Zone locale de l'ouest des États-Unis (Los Angeles)		✓	✓
USA Ouest (Oregon)	✓	✓	✓
Zone locale de l'ouest des États-Unis (Phoenix)	✓ *		
Afrique (Le Cap)		✓	✓
Asie-Pacifique (Hong Kong)	✓	✓	✓
Asie-Pacifique (Hyderabad)		✓	✓
Asie-Pacifique (Jakarta)		✓	✓
Asie-Pacifique (Malaisie)	✓ *		
Asie-Pacifique (Melbourne)		✓	✓
Asie-Pacifique (Mumbai)	✓	✓	✓

Région AWS	Persistant (2)	Persistant 1	Scratch 2
Asie-Pacifique (Osaka)		✓	✓
Asia Pacific (Seoul)	✓	✓	✓
Asie-Pacifique (Singapour)	✓	✓	✓
Asie-Pacifique (Sydney)	✓	✓	✓
Asie-Pacifique (Taipei)	✓ *		
Asie-Pacifique (Thaïlande)	✓ *		
Asie-Pacifique (Tokyo)	✓	✓	✓
Canada (Centre)	✓	✓	✓
Canada-Ouest (Calgary)	✓ *		
Europe (Francfort)	✓	✓	✓
Europe (Irlande)	✓	✓	✓
Europe (Londres)	✓	✓	✓
Europe (Milan)		✓	✓
Europe (Paris)		✓	✓
Europe (Espagne)		✓	✓
Europe (Stockholm)	✓	✓	✓
Europe (Zurich)		✓	✓
Israël (Tel Aviv)	✓ *		✓
Mexique (Centre)	✓ *		
Middle East (Bahrain)		✓	✓

Région AWS	Persistant (2)	Persistant 1	Scratch 2
Moyen-Orient (EAU)		✓	✓
Amérique du Sud (São Paulo)		✓	✓
AWS GovCloud (USA Est)		✓	✓
AWS GovCloud (US-Ouest)		✓	✓

> **Note**
>
> * Ils Régions AWS prennent en charge les systèmes de fichiers Persistent-125 et Persistent-250 avec classe de stockage SSD sans EFA.

Utilisation de référentiels de données avec Amazon FSx for Lustre

Amazon FSx for Lustre fournit des systèmes de fichiers à hautes performances optimisés pour un traitement rapide des charges de travail. Il peut prendre en charge des charges de travail telles que l'apprentissage automatique, le calcul haute performance (HPC), le traitement vidéo, la modélisation financière et l'automatisation de la conception électronique (EDA). Ces charges de travail nécessitent généralement que les données soient présentées à l'aide d'une interface de système de fichiers évolutive et à haut débit pour l'accès aux données. Les ensembles de données utilisés pour ces charges de travail sont souvent stockés dans des référentiels de données à long terme dans Amazon S3. FSx for Lustre est intégré nativement à Amazon S3, ce qui facilite le traitement des ensembles de données avec le système de Lustre fichiers.

> **Note**
>
> - Les sauvegardes de systèmes de fichiers ne sont pas prises en charge sur les systèmes de fichiers liés à un référentiel de données Amazon S3. Pour de plus amples informations, veuillez consulter Protection de vos données grâce à des sauvegardes.
> - Les systèmes de fichiers à hiérarchisation intelligente ne prennent pas en charge les liens vers les référentiels de données Amazon S3.

Rubriques

- Vue d'ensemble des référentiels de données
- Support des métadonnées POSIX pour les référentiels de données
- Lier votre système de fichiers à un compartiment Amazon S3
- Importation de modifications depuis votre référentiel de données
- Exportation des modifications vers le référentiel de données
- Tâches du référentiel de données
- Publication de fichiers
- Utilisation d'Amazon FSx avec vos données sur site
- Journaux d'événements du référentiel de données

- Utilisation d'anciens types de déploiement

Vue d'ensemble des référentiels de données

Lorsque vous utilisez Amazon FSx for Lustre avec des référentiels de données, vous pouvez ingérer et traiter de gros volumes de données de fichiers dans un système de fichiers performant en utilisant des tâches d'importation et d'importation automatiques de référentiels de données. Dans le même temps, vous pouvez enregistrer les résultats dans vos référentiels de données à l'aide de tâches d'exportation ou d'exportation automatiques de référentiels de données. Grâce à ces fonctionnalités, vous pouvez redémarrer votre charge de travail à tout moment en utilisant les dernières données stockées dans votre référentiel de données.

> **Note**
>
> Les associations de référentiels de données, l'exportation automatique et la prise en charge de plusieurs référentiels de données ne sont pas disponibles sur FSx les systèmes de fichiers ou `Scratch 1` les systèmes de fichiers Lustre 2.10.

FSx for Lustre est profondément intégré à Amazon S3. Cette intégration signifie que vous pouvez accéder facilement aux objets stockés dans vos compartiments Amazon S3 à partir des applications qui montent votre système de fichiers FSx for Lustre. Vous pouvez également exécuter vos charges de travail gourmandes en ressources informatiques sur des instances Amazon EC2 dans le référentiel de données AWS Cloud et en exporter les résultats une fois votre charge de travail terminée.

Pour accéder aux objets du référentiel de données Amazon S3 sous forme de fichiers et de répertoires du système de fichiers, les métadonnées des fichiers et des répertoires doivent être chargées dans le système de fichiers. Vous pouvez charger des métadonnées à partir d'un référentiel de données lié lorsque vous créez une association de référentiel de données.

En outre, vous pouvez importer des métadonnées de fichiers et de répertoires depuis vos référentiels de données liés vers le système de fichiers en utilisant l'importation automatique ou en utilisant une tâche d'importation de référentiel de données. Lorsque vous activez l'importation automatique pour une association de référentiels de données, votre système de fichiers importe automatiquement les métadonnées des fichiers au fur et à mesure que les fichiers sont créés, modifiés and/or ou supprimés dans le référentiel de données S3. Vous pouvez également importer des métadonnées

pour des fichiers et des répertoires nouveaux ou modifiés à l'aide d'une tâche de référentiel de données d'importation.

> **Note**
>
> Les tâches d'importation automatique et de référentiel de données d'importation peuvent être utilisées simultanément sur un système de fichiers.

Vous pouvez également exporter des fichiers et leurs métadonnées associées de votre système de fichiers vers votre référentiel de données à l'aide de l'exportation automatique ou d'une tâche d'exportation du référentiel de données. Lorsque vous activez l'exportation automatique sur une association de référentiels de données, votre système de fichiers exporte automatiquement les données et les métadonnées des fichiers au fur et à mesure que les fichiers sont créés, modifiés ou supprimés. Vous pouvez également exporter des fichiers ou des répertoires à l'aide d'une tâche d'exportation du référentiel de données. Lorsque vous utilisez une tâche de référentiel de données d'exportation, les données de fichier et les métadonnées créées ou modifiées depuis la dernière tâche de ce type sont exportées.

> **Note**
>
> - Les tâches d'exportation et d'exportation automatiques du référentiel de données ne peuvent pas être utilisées simultanément sur un système de fichiers.
> - Les associations de référentiels de données n'exportent que des fichiers, des liens symboliques et des répertoires ordinaires. Cela signifie que tous les autres types de fichiers (FIFO spécial, bloc spécial, caractère spécial et socket) ne seront pas exportés dans le cadre des processus d'exportation tels que l'exportation automatique et les tâches de référentiel de données d'exportation.

FSx for Lustre prend également en charge les charges de travail surchargées dans le cloud avec des systèmes de fichiers locaux en vous permettant de copier des données provenant de clients locaux à l'aide d'un VPN. Direct Connect

> **Important**
>
> Si vous avez lié un ou plusieurs systèmes de fichiers FSx for Lustre à un référentiel de données sur Amazon S3, ne supprimez pas le compartiment Amazon S3 tant que vous n'avez pas supprimé ou dissocié tous les systèmes de fichiers liés.

Support des régions et des comptes pour les compartiments S3 liés

Lorsque vous créez des liens vers des compartiments S3, gardez à l'esprit les limites de prise en charge des régions et des comptes suivantes :

- L'exportation automatique prend en charge les configurations interrégionales. Le système de FSx fichiers Amazon et le compartiment S3 lié peuvent être situés dans le même emplacement Région AWS ou dans un autre Régions AWS.
- L'importation automatique ne prend pas en charge les configurations interrégionales. Le système de FSx fichiers Amazon et le compartiment S3 lié doivent tous deux se trouver dans le même emplacement Région AWS.
- L'exportation automatique et l'importation automatique prennent en charge les configurations entre comptes. Le système de FSx fichiers Amazon et le compartiment S3 lié peuvent appartenir au même Compte AWS ou à un autre Comptes AWS.

Support des métadonnées POSIX pour les référentiels de données

Amazon FSx for Lustre transfère automatiquement les métadonnées de l'interface du système d'exploitation portable (POSIX) pour les fichiers, les répertoires et les liens symboliques (liens symboliques) lors de l'importation et de l'exportation de données vers et depuis un référentiel de données lié sur Amazon S3. Lorsque vous exportez les modifications de votre système de fichiers vers son référentiel de données lié, FSx for Lustre exporte également les modifications de métadonnées POSIX sous forme de métadonnées d'objet S3. Cela signifie que si un autre système de fichiers FSx pour Lustre importe les mêmes fichiers depuis S3, les fichiers auront les mêmes métadonnées POSIX dans ce système de fichiers, y compris la propriété et les autorisations.

FSx for Lustre importe uniquement des objets S3 dotés de clés d'objet conformes à POSIX, comme les suivantes.

```
mydir/
```

```
mydir/myfile1
mydir/mysubdir/
mydir/mysubdir/myfile2.txt
```

FSx for Lustre stocke les répertoires et les liens symboliques sous forme d'objets distincts dans le référentiel de données lié sur S3. Pour les annuaires, FSx pour Lustre crée un objet S3 avec un nom de clé qui se termine par une barre oblique («/»), comme suit :

- La clé de l'objet `mydir/` S3 correspond au répertoire FSx for Lustre`mydir/`.
- La clé de l'objet `mydir/mysubdir/` S3 correspond au répertoire FSx for Lustre`mydir/mysubdir/`.

Pour les liens symboliques, FSx Lustre utilise le schéma Amazon S3 suivant :

- Clé d'objet S3 — Le chemin vers le lien, relatif au répertoire de montage FSx for Lustre
- Données de l'objet S3 — Le chemin cible de ce lien symbolique
- Métadonnées de l'objet S3 — Les métadonnées du lien symbolique

FSx for Lustre stocke les métadonnées POSIX, y compris la propriété, les autorisations et les horodatages des fichiers, des répertoires et des liens symboliques, dans des objets S3 comme suit :

- `Content-Type`— L'en-tête de l'entité HTTP utilisé pour indiquer le type de média de la ressource pour les navigateurs Web.
- `x-amz-meta-file-permissions`— Le type de fichier et les autorisations dans le format`<octal file type><octal permission mask>`, conformément `st_mode` à la page de manuel de Linux stat (2).

  > **Note**
  >
  > FSx for Lustre n'importe ni ne conserve `setuid` d'informations.

- `x-amz-meta-file-owner`— L'ID utilisateur (UID) du propriétaire exprimé sous forme de nombre entier.
- `x-amz-meta-file-group`— L'ID de groupe (GID) exprimé sous la forme d'un entier.

- `x-amz-meta-file-atime`— La durée du dernier accès en nanosecondes depuis le début de l'ère Unix. Terminez la valeur temporelle par `ns` ; sinon, FSx Lustre interprète la valeur en millisecondes.
- `x-amz-meta-file-mtime`— Le temps de dernière modification en nanosecondes depuis le début de l'ère Unix. Terminez la valeur temporelle par `ns` ; sinon, FSx car Lustre interprète la valeur en millisecondes.
- `x-amz-meta-user-agent`— L'agent utilisateur, ignoré lors de l'importation FSx de Lustre. Lors de l'exportation, FSx for Lustre définit cette valeur sur`aws-fsx-lustre`.

Lorsque vous importez des objets depuis S3 auxquels aucune autorisation POSIX n'est associée, l'autorisation POSIX par défaut attribuée par Lustre à un fichier est. FSx `755` Cette autorisation autorise l'accès en lecture et en exécution à tous les utilisateurs et l'accès en écriture au propriétaire du fichier.

> **Note**
>
> FSx for Lustre ne conserve aucune métadonnée personnalisée définie par l'utilisateur sur les objets S3.

Liens physiques et exportation vers Amazon S3

Si l'exportation automatique (avec des politiques NOUVELLES et MODIFIÉES) est activée sur un DRA de votre système de fichiers, chaque lien physique contenu dans le DRA est exporté vers Amazon S3 sous la forme d'un objet S3 distinct pour chaque lien physique. Si un fichier comportant plusieurs liens physiques est modifié dans le système de fichiers, toutes les copies de S3 sont mises à jour, quel que soit le lien physique utilisé lors de la modification du fichier.

Si des liens physiques sont exportés vers S3 à l'aide de tâches du référentiel de données (DRTs), chaque lien matériel contenu dans les chemins spécifiés pour le DRT est exporté vers S3 en tant qu'objet S3 distinct pour chaque lien dur. Si un fichier comportant plusieurs liens physiques est modifié dans le système de fichiers, chaque copie dans S3 est mise à jour au moment où le lien dur correspondant est exporté, quel que soit le lien dur utilisé lors de la modification du fichier.

> **Important**
>
> Lorsqu'un nouveau système de fichiers FSx pour Lustre est lié à un compartiment S3 vers lequel des liens physiques ont été précédemment exportés par un autre système de fichiers FSx pour Lustre AWS DataSync, ou Amazon FSx File Gateway, les liens physiques sont ensuite importés sous forme de fichiers séparés dans le nouveau système de fichiers.

Liens physiques et fichiers publiés

Un fichier publié est un fichier dont les métadonnées sont présentes dans le système de fichiers, mais dont le contenu est uniquement stocké dans S3. Pour plus d'informations sur les fichiers publiés, consultezPublication de fichiers.

> **Important**
>
> L'utilisation de liens physiques dans un système de fichiers comportant des associations de référentiels de données (DRAs) est soumise aux restrictions suivantes :
>
> - La suppression et la recréation d'un fichier publié contenant plusieurs liens physiques peuvent entraîner le remplacement du contenu de tous les liens physiques.
> - La suppression d'un fichier publié supprimera le contenu de tous les liens physiques situés en dehors d'une association de référentiel de données.
> - La création d'un lien physique vers un fichier publié dont l'objet S3 correspondant se trouve dans l'une des classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive ne créera pas de nouvel objet dans S3 pour le lien physique.

Procédure pas à pas : associer des autorisations POSIX lors du téléchargement d'objets dans un compartiment Amazon S3

La procédure suivante explique le processus de téléchargement d'objets dans Amazon S3 avec des autorisations POSIX. Cela vous permet d'importer les autorisations POSIX lorsque vous créez un système de FSx fichiers Amazon lié à ce compartiment S3.

Pour télécharger des objets dotés d'autorisations POSIX sur Amazon S3

1. À partir de votre ordinateur ou machine local, utilisez les exemples de commandes suivants pour créer un répertoire de test (`s3cptestdir`) et un fichier (`s3cptest.txt`) qui seront téléchargés dans le compartiment S3.

   ```
   $ mkdir s3cptestdir
   $ echo "S3cp metadata import test" >> s3cptestdir/s3cptest.txt
   $ ls -ld s3cptestdir/ s3cptestdir/s3cptest.txt
   drwxr-xr-x 3 500 500 96 Jan 8 11:29 s3cptestdir/
   -rw-r--r-- 1 500 500 26 Jan 8 11:29 s3cptestdir/s3cptest.txt
   ```

   Le fichier et le répertoire nouvellement créés ont un ID utilisateur (UID) et un ID de groupe (GID) du propriétaire du fichier (GID) de 500, ainsi que des autorisations, comme indiqué dans l'exemple précédent.

2. Appelez l'API Amazon S3 pour créer le répertoire `s3cptestdir` avec les autorisations de métadonnées. Vous devez spécifier le nom du répertoire avec une barre oblique ()`/`. Pour plus d'informations sur les métadonnées POSIX prises en charge, consultezSupport des métadonnées POSIX pour les référentiels de données.

   *`bucket_name`*Remplacez-le par le nom réel de votre compartiment S3.

   ```
   $ aws s3api put-object --bucket bucket_name --key s3cptestdir/ --metadata '{"user-
   agent":"aws-fsx-lustre" , \
         "file-atime":"1595002920000000000ns" , "file-owner":"500" , "file-
   permissions":"0100664","file-group":"500" , \
         "file-mtime":"1595002920000000000ns"}'
   ```

3. Vérifiez que les autorisations POSIX sont associées aux métadonnées de l'objet S3.

   ```
   $ aws s3api head-object --bucket bucket_name --key s3cptestdir/
   {
       "AcceptRanges": "bytes",
       "LastModified": "Fri, 08 Jan 2021 17:32:27 GMT",
       "ContentLength": 0,
       "ETag": "\"d41d8cd98f00b204e9800998ecf8427e\"",
       "VersionId": "bAlhCoWq7aIEjc3R6Myc6UOb8sHHtJkR",
       "ContentType": "binary/octet-stream",
       "Metadata": {
           "user-agent": "aws-fsx-lustre",
           "file-atime": "1595002920000000000ns",
   ```

```
        "file-owner": "500",
        "file-permissions": "0100664",
        "file-group": "500",
        "file-mtime": "1595002920000000000ns"
    }
}
```

4. Téléchargez le fichier de test (créé à l'étape 1) depuis votre ordinateur vers le compartiment S3 avec les autorisations de métadonnées.

```
$ aws s3 cp s3cptestdir/s3cptest.txt s3://bucket_name/s3cptestdir/s3cptest.txt \
      --metadata '{"user-agent":"aws-fsx-lustre" , "file-
atime":"1595002920000000000ns" , \
      "file-owner":"500" , "file-permissions":"0100664","file-group":"500" , "file-
mtime":"1595002920000000000ns"}'
```

5. Vérifiez que les autorisations POSIX sont associées aux métadonnées de l'objet S3.

```
$ aws s3api head-object --bucket bucket_name --key s3cptestdir/s3cptest.txt
{
    "AcceptRanges": "bytes",
    "LastModified": "Fri, 08 Jan 2021 17:33:35 GMT",
    "ContentLength": 26,
    "ETag": "\"eb33f7e1f44a14a8e2f9475ae3fc45d3\"",
    "VersionId": "w9ztRoEhB832m8NC3a_JTlTyIx7Uzql6",
    "ContentType": "text/plain",
    "Metadata": {
        "user-agent": "aws-fsx-lustre",
        "file-atime": "1595002920000000000ns",
        "file-owner": "500",
        "file-permissions": "0100664",
        "file-group": "500",
        "file-mtime": "1595002920000000000ns"
    }
}
```

6. Vérifiez les autorisations sur le système de FSx fichiers Amazon lié au compartiment S3.

```
$ sudo lfs df -h /fsx
UUID                       bytes        Used   Available Use% Mounted on
3rnxfbmv-MDT0000_UUID       34.4G        6.1M       34.4G   0% /fsx[MDT:0]
3rnxfbmv-OST0000_UUID        1.1T        4.5M        1.1T   0% /fsx[OST:0]
```

```
filesystem_summary:         1.1T        4.5M        1.1T   0% /fsx

$ cd /fsx/s3cptestdir/
$ ls -ld s3cptestdir/
drw-rw-r-- 2 500 500 25600 Jan  8 17:33 s3cptestdir/

$ ls -ld s3cptestdir/s3cptest.txt
-rw-rw-r-- 1 500 500 26 Jan 8 17:33 s3cptestdir/s3cptest.txt
```

Le `s3cptestdir` répertoire et le `s3cptest.txt` fichier ont tous deux des autorisations POSIX importées.

Lier votre système de fichiers à un compartiment Amazon S3

Vous pouvez lier votre système de fichiers Amazon FSx for Lustre aux référentiels de données d'Amazon S3. Vous pouvez créer le lien lors de la création du système de fichiers ou à tout moment après la création du système de fichiers.

Un lien entre un répertoire du système de fichiers et un compartiment ou un préfixe S3 est appelé association de référentiel de données (DRA). Vous pouvez configurer un maximum de 8 associations de référentiels de données sur un système de fichiers FSx for Lustre. Un maximum de 8 demandes DRA peuvent être mises en file d'attente, mais le système de fichiers ne peut traiter qu'une seule demande à la fois. Chaque DRA doit avoir un répertoire unique FSx pour le système de fichiers Lustre et un compartiment ou un préfixe S3 unique qui lui est associé.

> **Note**
>
> Les associations de référentiels de données, l'exportation automatique et la prise en charge de plusieurs référentiels de données ne sont pas disponibles sur FSx les systèmes de fichiers ou `Scratch 1` les systèmes de fichiers Lustre 2.10.

Pour accéder aux objets du référentiel de données S3 sous forme de fichiers et de répertoires du système de fichiers, les métadonnées des fichiers et des répertoires doivent être chargées dans le système de fichiers. Vous pouvez charger des métadonnées à partir d'un référentiel de données lié lorsque vous créez le DRA ou charger des métadonnées pour des lots de fichiers et de répertoires auxquels vous souhaitez accéder ultérieurement à l'aide du système de fichiers FSx for Lustre à l'aide d'une tâche d'importation de référentiel de données, ou utiliser l'exportation automatique pour

charger automatiquement les métadonnées lorsque des objets sont ajoutés, modifiés ou supprimés du référentiel de données.

Vous pouvez configurer un DRA pour l'importation automatique uniquement, pour l'exportation automatique uniquement, ou pour les deux. Une association de référentiel de données configurée à la fois avec une importation et une exportation automatiques propage les données dans les deux sens entre le système de fichiers et le compartiment S3 lié. Lorsque vous modifiez les données de votre référentiel de données S3, FSx for Lustre détecte les modifications puis les importe automatiquement dans votre système de fichiers. Lorsque vous créez, modifiez ou supprimez des fichiers, FSx for Lustre exporte automatiquement les modifications vers Amazon S3 de manière asynchrone une fois que votre application a fini de modifier le fichier.

⚠ Important

- Si vous modifiez le même fichier à la fois dans le système de fichiers et dans le compartiment S3, vous devez garantir la coordination au niveau de l'application afin d'éviter les conflits. FSx for Lustre n'empêche pas les écritures conflictuelles à plusieurs endroits.
- Pour les fichiers marqués d'un attribut immuable, FSx for Lustre n'est pas en mesure de synchroniser les modifications entre votre système de fichiers FSx for Lustre et un compartiment S3 lié au système de fichiers. La définition d'un indicateur immuable pendant une période prolongée peut entraîner une dégradation des performances du transfert de données entre Amazon FSx et S3.

Lorsque vous créez une association de référentiel de données, vous pouvez configurer les propriétés suivantes :

- Chemin du système de fichiers — Entrez un chemin local sur le système de fichiers qui pointe vers un répertoire (tel que `/ns1/`) ou un sous-répertoire (tel que `/ns1/subdir/`) qui sera mappé one-to-one avec le chemin du référentiel de données spécifié ci-dessous. Une barre oblique est requise au début du nom. Deux associations de référentiels de données ne peuvent pas avoir des chemins d'accès de système de fichiers qui se chevauchent. Par exemple, si un référentiel de données est associé au chemin d'accès du système de fichiers `/ns1`, vous ne pouvez pas lier un autre référentiel de données au chemin d'accès du système de fichiers `/ns1/ns2`.

> **Note**
>
> Si vous spécifiez uniquement une barre oblique (/) comme chemin d'accès du système de fichiers, vous ne pouvez lier qu'un seul référentiel de données au système de fichiers. Vous pouvez uniquement spécifier « / » comme chemin d'accès du système de fichiers pour le premier référentiel de données associé à un système de fichiers.

- Chemin du référentiel de données — Entrez un chemin dans le référentiel de données S3. Le chemin d'accès peut être un compartiment S3 ou un préfixe au format `s3://bucket-name/prefix/`. Cette propriété indique l'endroit depuis lequel les fichiers seront importés ou exportés dans le référentiel de données S3. FSx for Lustre ajoutera un «/» final au chemin de votre référentiel de données si vous n'en fournissez pas un. Par exemple, si vous fournissez un chemin de référentiel de données des`s3://amzn-s3-demo-bucket/my-prefix`, FSx for Lustre l'interprétera comme`s3://amzn-s3-demo-bucket/my-prefix/`.

  Deux associations de référentiels de données ne peuvent pas avoir de chemins de référentiel de données qui se chevauchent. Par exemple, si un référentiel de données avec chemin `s3://amzn-s3-demo-bucket/my-prefix/` est lié au système de fichiers, vous ne pouvez pas créer une autre association de référentiel de données avec le chemin du référentiel de données`s3://amzn-s3-demo-bucket/my-prefix/my-sub-prefix`.
- Importer des métadonnées depuis le référentiel : vous pouvez sélectionner cette option pour importer les métadonnées de l'ensemble du référentiel de données immédiatement après avoir créé l'association du référentiel de données. Vous pouvez également exécuter une tâche d'importation de référentiel de données pour charger la totalité ou un sous-ensemble des métadonnées du référentiel de données lié dans le système de fichiers à tout moment après la création de l'association de référentiel de données.
- Paramètres d'importation : choisissez une politique d'importation qui spécifie le type d'objets mis à jour (toute combinaison de nouveaux, de modifiés et de supprimés) qui seront automatiquement importés du compartiment S3 lié vers votre système de fichiers. L'importation automatique (nouvelle, modifiée, supprimée) est activée par défaut lorsque vous ajoutez un référentiel de données depuis la console, mais elle est désactivée par défaut lorsque vous utilisez l' FSx API AWS CLI ou Amazon.
- Paramètres d'exportation : choisissez une politique d'exportation qui spécifie le type d'objets mis à jour (toute combinaison de nouveaux, de modifiés et de supprimés) qui seront automatiquement exportés vers le compartiment S3. L'exportation automatique (nouvelle, modifiée, supprimée) est

activée par défaut lorsque vous ajoutez un référentiel de données depuis la console, mais elle est désactivée par défaut lorsque vous utilisez l' FSx API AWS CLI ou Amazon.

Les paramètres du chemin du système de fichiers et du chemin du référentiel de données fournissent un mappage 1:1 entre les chemins dans Amazon FSx et les clés d'objet dans S3.

Rubriques

- Création d'un lien vers un compartiment S3
- Mise à jour des paramètres d'association du référentiel de données
- Supprimer une association vers un compartiment S3
- Afficher les détails des associations de référentiels de données
- État du cycle de vie des associations au référentiel de données
- Utilisation de compartiments Amazon S3 chiffrés côté serveur

Création d'un lien vers un compartiment S3

Les procédures suivantes vous guident dans le processus de création d'une association de référentiel de données pour un système de fichiers FSx for Lustre à un compartiment S3 existant, à l'aide de la AWS Management Console commande and AWS Command Line Interface (AWS CLI). Pour plus d'informations sur l'ajout d'autorisations à un compartiment S3 afin de le lier à votre système de fichiers, consultezAjouter des autorisations pour utiliser les référentiels de données dans Amazon S3.

> **Note**
>
> Les référentiels de données ne peuvent pas être liés à des systèmes de fichiers sur lesquels les sauvegardes de systèmes de fichiers sont activées. Désactivez les sauvegardes avant de créer un lien vers un référentiel de données.

Pour lier un compartiment S3 lors de la création d'un système de fichiers (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau système de fichiers décrite Étape 1 : Créez votre système de fichiers FSx for Lustre dans la section Mise en route.
3. Ouvrez le référentiel de données Import/Export - section facultative. La fonctionnalité est désactivée par défaut.

4. Choisissez Importer des données depuis et exporter des données vers S3.
5. Dans la boîte de dialogue Informations d'association du référentiel de données, fournissez des informations pour les champs suivants.

   - Chemin du système de fichiers : entrez le nom d'un répertoire de haut niveau (tel que`/ns1`) ou d'un sous-répertoire (tel que`/ns1/subdir`) dans le système de FSx fichiers Amazon qui sera associé au référentiel de données S3. La barre oblique principale de la trajectoire est obligatoire. Deux associations de référentiels de données ne peuvent pas avoir des chemins d'accès de système de fichiers qui se chevauchent. Par exemple, si un référentiel de données est associé au chemin d'accès du système de fichiers `/ns1`, vous ne pouvez pas lier un autre référentiel de données au chemin d'accès du système de fichiers `/ns1/ns2`. Le paramètre de chemin du système de fichiers doit être unique pour toutes les associations de référentiels de données du système de fichiers.
   - Chemin du référentiel de données : entrez le chemin d'un compartiment ou d'un préfixe S3 existant à associer à votre système de fichiers (par exemple,`s3://amzn-s3-demo-bucket/my-prefix`). Deux associations de référentiels de données ne peuvent pas avoir de chemins de référentiel de données qui se chevauchent. Le paramètre du chemin du référentiel de données doit être unique pour toutes les associations de référentiels de données du système de fichiers.
   - Importer des métadonnées depuis le référentiel : sélectionnez cette propriété pour éventuellement exécuter une tâche d'importation du référentiel de données afin d'importer les métadonnées immédiatement après la création du lien.
6. Pour les paramètres d'importation (facultatif), définissez une politique d'importation qui détermine la manière dont vos listes de fichiers et de répertoires sont mises à jour lorsque vous ajoutez, modifiez ou supprimez des objets dans votre compartiment S3. Par exemple, choisissez Nouveau pour importer les métadonnées dans votre système de fichiers pour les nouveaux objets créés dans le compartiment S3. Pour plus d'informations sur les politiques d'importation, consultezImportez automatiquement des mises à jour depuis votre compartiment S3.
7. Pour la politique d'exportation, définissez une politique d'exportation qui détermine la manière dont vos fichiers sont exportés vers votre compartiment S3 lié lorsque vous ajoutez, modifiez ou supprimez des objets dans votre système de fichiers. Par exemple, choisissez Modifié pour exporter des objets dont le contenu ou les métadonnées ont été modifiés dans votre système de fichiers. Pour plus d'informations sur les politiques d'exportation, consultezExportez automatiquement les mises à jour vers votre compartiment S3.
8. Passez à la section suivante de l'assistant de création de système de fichiers.

Pour lier un compartiment S3 à un système de fichiers existant (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord, choisissez Systèmes de fichiers, puis sélectionnez le système de fichiers pour lequel vous souhaitez créer une association de référentiel de données.
3. Choisissez l'onglet Référentiel de données.
4. Dans le volet Associations de référentiels de données, choisissez Créer une association de référentiel de données.
5. Dans la boîte de dialogue Informations d'association du référentiel de données, fournissez des informations pour les champs suivants.

   - Chemin du système de fichiers : entrez le nom d'un répertoire de haut niveau (tel que`/ns1`) ou d'un sous-répertoire (tel que`/ns1/subdir`) dans le système de FSx fichiers Amazon qui sera associé au référentiel de données S3. La barre oblique principale de la trajectoire est obligatoire. Deux associations de référentiels de données ne peuvent pas avoir des chemins d'accès de système de fichiers qui se chevauchent. Par exemple, si un référentiel de données est associé au chemin d'accès du système de fichiers `/ns1`, vous ne pouvez pas lier un autre référentiel de données au chemin d'accès du système de fichiers `/ns1/ns2`. Le paramètre de chemin du système de fichiers doit être unique pour toutes les associations de référentiels de données du système de fichiers.
   - Chemin du référentiel de données : entrez le chemin d'un compartiment ou d'un préfixe S3 existant à associer à votre système de fichiers (par exemple,`s3://amzn-s3-demo-bucket/my-prefix`). Deux associations de référentiels de données ne peuvent pas avoir de chemins de référentiel de données qui se chevauchent. Le paramètre du chemin du référentiel de données doit être unique pour toutes les associations de référentiels de données du système de fichiers.
   - Importer des métadonnées depuis le référentiel : sélectionnez cette propriété pour éventuellement exécuter une tâche d'importation du référentiel de données afin d'importer les métadonnées immédiatement après la création du lien.
6. Pour les paramètres d'importation (facultatif), définissez une politique d'importation qui détermine la manière dont vos listes de fichiers et de répertoires sont mises à jour lorsque vous ajoutez, modifiez ou supprimez des objets dans votre compartiment S3. Par exemple, choisissez Nouveau pour importer les métadonnées dans votre système de fichiers pour les nouveaux objets créés dans le compartiment S3. Pour plus d'informations sur les politiques d'importation, consultezImportez automatiquement des mises à jour depuis votre compartiment S3.

7. Pour la politique d'exportation, définissez une politique d'exportation qui détermine la manière dont vos fichiers sont exportés vers votre compartiment S3 lié lorsque vous ajoutez, modifiez ou supprimez des objets dans votre système de fichiers. Par exemple, choisissez Modifié pour exporter des objets dont le contenu ou les métadonnées ont été modifiés dans votre système de fichiers. Pour plus d'informations sur les politiques d'exportation, consultezExportez automatiquement les mises à jour vers votre compartiment S3.
8. Choisissez Créer.

Pour lier un système de fichiers à un compartiment S3 (AWS CLI)

L'exemple suivant crée une association de référentiel de données qui lie un système de FSx fichiers Amazon à un compartiment S3, avec une politique d'importation qui importe les fichiers nouveaux ou modifiés dans le système de fichiers et une politique d'exportation qui exporte les fichiers nouveaux, modifiés ou supprimés vers le compartiment S3 lié.

- Pour créer une association de référentiel de données, utilisez la commande Amazon FSx CLI`create-data-repository-association`, comme indiqué ci-dessous.

```
$ aws fsx create-data-repository-association \
      --file-system-id fs-0123456789abcdef0 \
      --file-system-path /ns1/path1/ \
      --data-repository-path s3://amzn-s3-demo-bucket/myprefix/ \
      --s3
 "AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

Amazon FSx renvoie immédiatement la description JSON du DRA. Le DRA est créé de manière asynchrone.

Vous pouvez utiliser cette commande pour créer une association de référentiel de données avant même que le système de fichiers n'ait terminé sa création. La demande sera mise en file d'attente et l'association du référentiel de données sera créée une fois que le système de fichiers sera disponible.

Mise à jour des paramètres d'association du référentiel de données

Vous pouvez mettre à jour les paramètres d'une association de référentiel de données existante à l' AWS Management Console aide des FSx API AWS CLI, et Amazon, comme indiqué dans les procédures suivantes.

> **Note**
>
> Vous ne pouvez pas mettre à jour le `File system path` ou `Data repository path` d'un DRA après sa création. Si vous souhaitez modifier le `File system path` ou`Data repository path`, vous devez supprimer le DRA et le créer à nouveau.

Pour mettre à jour les paramètres d'une association de référentiels de données existante (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord, choisissez Systèmes de fichiers, puis sélectionnez le système de fichiers que vous souhaitez gérer.
3. Choisissez l'onglet Référentiel de données.
4. Dans le volet Associations de référentiels de données, choisissez l'association de référentiel de données que vous souhaitez modifier.
5. Choisissez Mettre à jour. Une boîte de dialogue de modification s'affiche pour l'association du référentiel de données.
6. Pour les paramètres d'importation (facultatif), vous pouvez mettre à jour votre politique d'importation. Pour plus d'informations sur les politiques d'importation, consultezImportez automatiquement des mises à jour depuis votre compartiment S3.
7. Pour les paramètres d'exportation (facultatif), vous pouvez mettre à jour votre politique d'exportation. Pour plus d'informations sur les politiques d'exportation, consultezExportez automatiquement les mises à jour vers votre compartiment S3.
8. Choisissez Mettre à jour.

Pour mettre à jour les paramètres d'une association de référentiels de données (CLI) existante

- Pour mettre à jour une association de référentiel de données, utilisez la commande Amazon FSx CLIupdate-data-repository-association, comme indiqué ci-dessous.

```
$ aws fsx update-data-repository-association \
      --association-id 'dra-872abab4b4503bfc2' \
      --s3
 "AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

Après avoir correctement mis à jour les politiques d'importation et d'exportation de l'association du référentiel de données, Amazon FSx renvoie la description de l'association du référentiel de données mise à jour au format JSON.

Supprimer une association vers un compartiment S3

Les procédures suivantes vous guident dans le processus de suppression d'une association de référentiel de données d'un système de FSx fichiers Amazon existant vers un compartiment S3 existant, à l'aide de la AWS Management Console commande and AWS Command Line Interface (AWS CLI). La suppression de l'association du référentiel de données dissocie le système de fichiers du compartiment S3.

Pour supprimer un lien d'un système de fichiers vers un compartiment S3 (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord, choisissez Systèmes de fichiers, puis sélectionnez le système de fichiers dont vous souhaitez supprimer une association de référentiel de données.
3. Choisissez l'onglet Référentiel de données.
4. Dans le volet Associations de référentiels de données, choisissez l'association de référentiel de données que vous souhaitez supprimer.
5. Pour Actions, choisissez Supprimer l'association.
6. Dans la boîte de dialogue Supprimer, vous pouvez choisir Supprimer les données dans le système de fichiers pour supprimer physiquement les données du système de fichiers correspondant à l'association du référentiel de données.

   Choisissez cette option si vous envisagez de créer une nouvelle association de référentiel de données en utilisant le même chemin de système de fichiers mais pointant vers un préfixe de compartiment S3 différent, ou si vous n'avez plus besoin des données de votre système de fichiers.
7. Choisissez Supprimer pour supprimer l'association du référentiel de données du système de fichiers.

Pour supprimer un lien d'un système de fichiers vers un compartiment S3 (AWS CLI)

L'exemple suivant supprime une association de référentiel de données qui lie un système de FSx fichiers Amazon à un compartiment S3. Le `--association-id` paramètre indique l'ID de l'association du référentiel de données à supprimer.

- Pour supprimer une association de référentiel de données, utilisez la commande Amazon FSx CLI`delete-data-repository-association`, comme indiqué ci-dessous.

```
$ aws fsx delete-data-repository-association \
      --association-id dra-872abab4b4503bfc \
      --delete-data-in-file-system false
```

Après avoir correctement supprimé l'association du référentiel de données, Amazon FSx renvoie sa description au format JSON.

> **Recréation DRAs avec le même chemin de système de fichiers**
>
> Il est déconseillé de supprimer et de recréer les associations de référentiels de données qui utilisent le même chemin de système de fichiers. Si vous supprimez un DRA et que vous en créez ultérieurement un nouveau en utilisant le même chemin de système de fichiers, certains fichiers peuvent conserver l'état HSM du DRA précédemment supprimé.
> Si vous devez exporter des fichiers à partir d'un DRA recréé qui ont été gérés par un DRA précédemment supprimé, vous devez marquer ces fichiers comme sales à l'aide de la commande ci-dessous, puis exécuter une tâche de référentiel de données d'exportation :
>
> ```
> sudo lfs hsm_set --dirty file_path
> ```

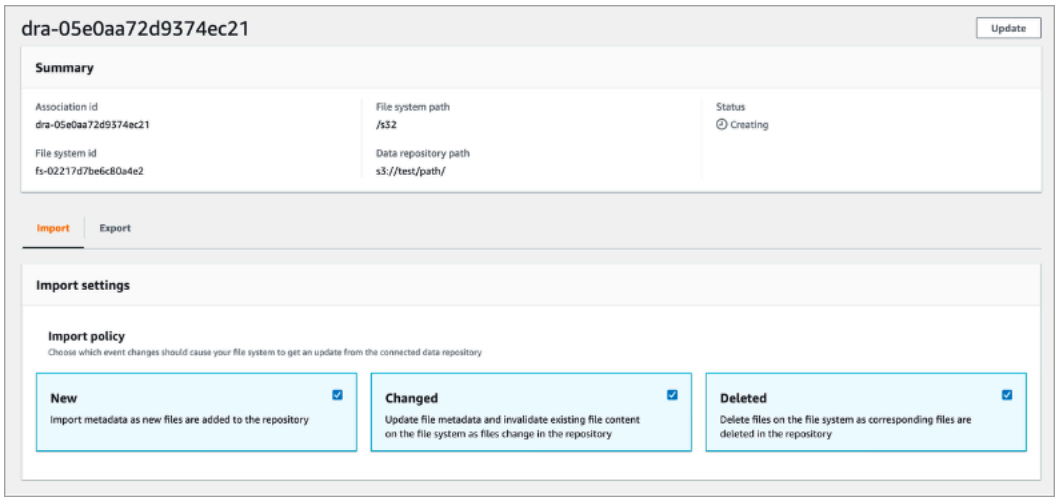
Afficher les détails des associations de référentiels de données

Vous pouvez consulter les détails d'une association de référentiels de données à l'aide de la console FSx for Lustre, du AWS CLI, et de l'API. Les détails incluent l'ID d'association du DRA, le chemin du système de fichiers, le chemin du référentiel de données, les paramètres d'importation, les paramètres d'exportation, le statut et l'ID du système de fichiers associé.

Pour afficher les détails du DRA (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord, choisissez Systèmes de fichiers, puis sélectionnez le système de fichiers pour lequel vous souhaitez consulter les détails de l'association d'un référentiel de données.
3. Choisissez l'onglet Référentiel de données.

4. Dans le volet Associations de référentiels de données, choisissez l'association de référentiel de données que vous souhaitez afficher. La page Résumé apparaît, affichant les détails du DRA.



Pour afficher les détails du DRA (CLI)

- Pour afficher les détails d'une association de référentiel de données spécifique, utilisez la commande Amazon FSx CLI`describe-data-repository-associations`, comme indiqué ci-dessous.

```
$ aws fsx describe-data-repository-associations \
      --association-ids dra-872abab4b4503bfc2
```

  Amazon FSx renvoie la description de l'association du référentiel de données au format JSON.

État du cycle de vie des associations au référentiel de données

L'état du cycle de vie des associations de référentiels de données fournit des informations sur le statut d'un DRA spécifique. Une association de référentiel de données peut avoir les états de cycle de vie suivants :

- Création : Amazon crée FSx l'association du référentiel de données entre le système de fichiers et le référentiel de données lié. Le référentiel de données n'est pas disponible.
- Disponible — L'association du référentiel de données peut être utilisée.
- Mise à jour : l'association du référentiel de données fait l'objet d'une mise à jour initiée par le client qui pourrait affecter sa disponibilité.

- Suppression : l'association du référentiel de données est en cours de suppression à l'initiative du client.
- Configuration incorrecte : Amazon FSx ne peut pas importer automatiquement les mises à jour depuis le compartiment S3 ou exporter automatiquement les mises à jour vers le compartiment S3 tant que la configuration des associations de référentiels de données n'est pas corrigée.

  Un DRA peut être mal configuré pour les raisons suivantes :

  - Amazon FSx ne dispose pas des autorisations IAM nécessaires pour accéder au compartiment S3.
  - La configuration des notifications d' FSx événements sur le compartiment S3 est supprimée ou modifiée.
  - Le compartiment S3 contient des notifications d'événements existantes qui se recoupent avec les types d' FSx événements.

  Une fois le problème sous-jacent résolu, le DRA revient automatiquement à l'état Disponible dans les 15 minutes, ou vous pouvez immédiatement déclencher le changement d'état à l'aide de la AWS CLI commande update-data-repository-association.
- Échec : l'association du référentiel de données est dans un état terminal qui ne peut pas être restauré (par exemple, parce que le chemin du système de fichiers est supprimé ou que le compartiment S3 est supprimé).

Vous pouvez consulter l'état du cycle de vie d'une association de référentiels de données à l'aide de la FSx console Amazon AWS Command Line Interface, du, et de l' FSx API Amazon. Pour de plus amples informations, veuillez consulter Afficher les détails des associations de référentiels de données.

Utilisation de compartiments Amazon S3 chiffrés côté serveur

FSx for Lustre prend en charge les compartiments Amazon S3 qui utilisent le chiffrement côté serveur avec des clés gérées par S3 (SSE-S3) et stockées dans (SSE-KMS). AWS KMS keys AWS Key Management Service

Si vous souhaitez qu'Amazon FSx chiffre les données lorsque vous écrivez dans votre compartiment S3, vous devez définir le chiffrement par défaut de votre compartiment S3 sur SSE-S3 ou SSE-KMS. Pour plus d'informations, consultez la section Configuration du chiffrement par défaut dans le guide de l'utilisateur Amazon S3. Lorsque vous écrivez des fichiers dans votre compartiment S3, Amazon FSx suit la politique de chiffrement par défaut de votre compartiment S3.

Par défaut, Amazon FSx prend en charge les compartiments S3 chiffrés à l'aide du protocole SSE-S3. Si vous souhaitez lier votre système de FSx fichiers Amazon à un compartiment S3 chiffré à l'aide du chiffrement SSE-KMS, vous devez ajouter une déclaration à votre politique de clé gérée par le client qui autorise Amazon FSx à chiffrer et à déchiffrer les objets de votre compartiment S3 à l'aide de votre clé KMS.

L'instruction suivante permet à un système de FSx fichiers Amazon spécifique de chiffrer et de déchiffrer des objets pour un compartiment S3 spécifique,. *bucket_name*

```
{
    "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
 in the given S3 bucket",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::aws_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fsx_file_system_id"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "aws_account_id",
            "kms:ViaService": "s3.bucket-region.amazonaws.com"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        }
    }
}
```

> **Note**
>
> Si vous utilisez un KMS avec une clé CMK pour chiffrer votre compartiment S3 avec les clés de compartiment S3 activées, définissez l'ARN du `EncryptionContext` compartiment, et non l'ARN de l'objet, comme dans cet exemple :

```
"StringLike": {
    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name"
}
```

La déclaration de politique suivante permet à tous les systèmes de FSx fichiers Amazon de votre compte d'être liés à un compartiment S3 spécifique.

```
{
      "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
 in the given S3 bucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "s3.bucket-region.amazonaws.com",
          "kms:CallerAccount": "aws_account_id"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        },
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws_partition:iam::aws_account_id:role/aws-service-
role/s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fs-*"
        }
      }
}
```

Accès aux compartiments Amazon S3 chiffrés côté serveur dans un autre VPC Compte AWS ou à partir d'un VPC partagé

Après avoir créé un système de fichiers FSx for Lustre lié à un compartiment Amazon S3 chiffré, vous devez accorder au rôle `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`* lié au service (SLR) l'accès à la clé KMS utilisée pour chiffrer le compartiment S3 avant de lire ou d'écrire des données depuis le compartiment S3 lié. Vous pouvez utiliser un rôle IAM déjà autorisé à accéder à la clé KMS.

> **Note**
>
> Ce rôle IAM doit figurer dans le compte dans lequel le système de fichiers FSx for Lustre a été créé (qui est le même compte que le S3 SLR), et non dans le compte auquel appartient la clé KM/le compartiment S3.

Vous utilisez le rôle IAM pour appeler l' AWS KMS API suivante afin de créer une autorisation pour le SLR S3 afin que le SLR obtienne l'autorisation d'accéder aux objets S3. Pour trouver l'ARN associé à votre SLR, recherchez vos rôles IAM en utilisant l'ID de votre système de fichiers comme chaîne de recherche.

```
$ aws kms create-grant --region fs_account_region \
      --key-id arn:aws:kms:s3_bucket_account_region:s3_bucket_account:key/key_id \
      --grantee-principal arn:aws:iam::fs_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_file-system-id \
      --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Pour plus d'informations sur les rôles liés à un service, consultez Utilisation de rôles liés à un service pour Amazon FSx.

Importation de modifications depuis votre référentiel de données

Vous pouvez importer les modifications apportées aux données et aux métadonnées POSIX depuis un référentiel de données lié vers votre système de FSx fichiers Amazon. Les métadonnées POSIX associées incluent la propriété, les autorisations et les horodatages.

Pour importer les modifications apportées au système de fichiers, appliquez l'une des méthodes suivantes :

- Configurez votre système de fichiers pour importer automatiquement les fichiers nouveaux, modifiés ou supprimés de votre référentiel de données lié. Pour de plus amples informations, veuillez consulter Importez automatiquement des mises à jour depuis votre compartiment S3.
- Sélectionnez l'option permettant d'importer des métadonnées lorsque vous créez une association de référentiels de données. Cela lancera une tâche d'importation du référentiel de données immédiatement après la création de l'association du référentiel de données.
- Utilisez une tâche de référentiel de données d'importation à la demande. Pour de plus amples informations, veuillez consulter Utilisation des tâches du référentiel de données pour importer des modifications.

Les tâches d'importation automatique et d'importation du référentiel de données peuvent être exécutées simultanément.

Lorsque vous activez l'importation automatique pour une association de référentiels de données, votre système de fichiers met automatiquement à jour les métadonnées des fichiers au fur et à mesure que des objets sont créés, modifiés ou supprimés dans S3. Lorsque vous sélectionnez l'option permettant d'importer des métadonnées lors de la création d'une association de référentiel de données, votre système de fichiers importe les métadonnées de tous les objets du référentiel de données. Lorsque vous importez à l'aide d'une tâche de référentiel de données d'importation, votre système de fichiers importe uniquement les métadonnées des objets créés ou modifiés depuis la dernière importation.

FSx for Lustre copie automatiquement le contenu d'un fichier depuis votre référentiel de données et le charge dans le système de fichiers lorsque votre application accède pour la première fois au fichier dans le système de fichiers. Ce mouvement de données est géré par FSx for Lustre et est transparent pour vos applications. Les lectures suivantes de ces fichiers sont diffusées directement depuis le système de fichiers avec des latences inférieures à la milliseconde.

Vous pouvez également précharger l'ensemble de votre système de fichiers ou un répertoire de votre système de fichiers. Pour de plus amples informations, veuillez consulter Préchargement de fichiers dans votre système de fichiers. Si vous demandez le préchargement de plusieurs fichiers simultanément, FSx for Lustre charge les fichiers depuis votre référentiel de données Amazon S3 en parallèle.

FSx for Lustre importe uniquement des objets S3 dotés de clés d'objet conformes à POSIX. Les tâches d'importation et d'importation automatiques du référentiel de données importent des métadonnées POSIX. Pour de plus amples informations, veuillez consulter Support des métadonnées POSIX pour les référentiels de données.

> **Note**
>
> FSx for Lustre ne prend pas en charge l'importation de métadonnées pour les liens symboliques (liens symboliques) à partir des classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive. Les métadonnées des objets S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive qui ne sont pas des liens symboliques peuvent être importées (c'est-à-dire qu'un inode est créé sur le système de fichiers FSx for Lustre avec les métadonnées correctes). Toutefois, pour lire ces données depuis le système de fichiers, vous devez d'abord restaurer l'objet S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. L'importation de données de fichiers directement depuis des objets Amazon S3 de la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive vers FSx for Lustre n'est pas prise en charge.

Importez automatiquement des mises à jour depuis votre compartiment S3

Vous pouvez configurer Lustre FSx pour qu'il mette automatiquement à jour les métadonnées dans le système de fichiers lorsque des objets sont ajoutés, modifiés ou supprimés de votre compartiment S3. FSx for Lustre crée, met à jour ou supprime la liste des fichiers et des répertoires, correspondant à la modification apportée dans S3. Si l'objet modifié dans le compartiment S3 ne contient plus ses métadonnées, FSx for Lustre conserve les valeurs de métadonnées actuelles du fichier, y compris les autorisations actuelles.

> **Note**
>
> Le système de fichiers FSx for Lustre et le compartiment S3 lié doivent se trouver dans le même emplacement Région AWS pour importer automatiquement les mises à jour.

Vous pouvez configurer l'importation automatique lorsque vous créez l'association au référentiel de données, et vous pouvez mettre à jour les paramètres d'importation automatique à tout moment à l'aide de la console de FSx gestion, de l' AWS CLI API ou de l' AWS API.

> **Note**
>
> Vous pouvez configurer à la fois l'importation automatique et l'exportation automatique sur la même association de référentiels de données. Cette rubrique décrit uniquement la fonctionnalité d'importation automatique.

> **Important**
>
> - Si un objet est modifié dans S3 alors que toutes les politiques d'importation automatique sont activées et que l'exportation automatique est désactivée, le contenu de cet objet est toujours importé dans un fichier correspondant du système de fichiers. Si un fichier existe déjà dans l'emplacement cible, il est remplacé.
> - Si un fichier est modifié à la fois dans le système de fichiers et dans S3, alors que toutes les politiques d'importation et d'exportation automatiques sont activées, le fichier du système de fichiers ou l'objet de S3 peuvent être remplacés par l'autre. Il n'est pas garanti qu'une modification ultérieure à un endroit remplacera une modification antérieure à un autre emplacement. Si vous modifiez le même fichier à la fois dans le système de fichiers et dans le compartiment S3, vous devez garantir la coordination au niveau de l'application afin d'éviter de tels conflits. FSx for Lustre n'empêche pas les écritures conflictuelles à plusieurs endroits.

La politique d'importation indique comment vous souhaitez que FSx Lustre mette à jour votre système de fichiers lorsque le contenu change dans le compartiment S3 lié. Une association de référentiels de données peut avoir l'une des politiques d'importation suivantes :

- Nouveau : FSx pour Lustre met automatiquement à jour les métadonnées des fichiers et des répertoires uniquement lorsque de nouveaux objets sont ajoutés au référentiel de données S3 lié.
- Modifié : FSx pour Lustre met automatiquement à jour les métadonnées des fichiers et des répertoires uniquement lorsqu'un objet existant dans le référentiel de données est modifié.
- Supprimé : FSx pour Lustre met automatiquement à jour les métadonnées des fichiers et des répertoires uniquement lorsqu'un objet du référentiel de données est supprimé.
- Toute combinaison de Nouveau, Modifié et Supprimé — FSx for Lustre met automatiquement à jour les métadonnées du fichier et du répertoire lorsque l'une des actions spécifiées se produit dans le référentiel de données S3. Par exemple, vous pouvez spécifier que le système de fichiers

est mis à jour lorsqu'un objet est ajouté au référentiel S3 (Nouveau) ou supprimé (supprimé), mais qu'il n'est pas mis à jour lorsqu'un objet est modifié.

- Aucune politique configurée : car FSx Lustre ne met pas à jour les métadonnées des fichiers et des répertoires sur le système de fichiers lorsque des objets sont ajoutés, modifiés ou supprimés du référentiel de données S3. Si vous ne configurez pas de politique d'importation, l'importation automatique est désactivée pour l'association du référentiel de données. Vous pouvez toujours importer manuellement les modifications des métadonnées à l'aide d'une tâche de référentiel de données d'importation, comme décrit dansUtilisation des tâches du référentiel de données pour importer des modifications.

> **⚠ Important**
>
> L'importation automatique ne synchronisera pas les actions S3 suivantes avec votre système de fichiers Linked FSx for Lustre :
>
> - Supprimer un objet à l'aide des expirations du cycle de vie des objets S3
> - Suppression définitive de la version actuelle de l'objet dans un compartiment activé pour la gestion des versions
> - Annulation de la suppression d'un objet dans un compartiment activé pour la gestion des versions

Dans la plupart des cas d'utilisation, nous vous recommandons de configurer une politique d'importation comprenant les valeurs Nouveau, Modifié et Supprimé. Cette politique garantit que toutes les mises à jour effectuées dans votre référentiel de données S3 lié sont automatiquement importées dans votre système de fichiers.

Lorsque vous définissez une politique d'importation pour mettre à jour les métadonnées des fichiers et des répertoires de votre système de fichiers en fonction des modifications apportées au référentiel de données S3 lié, FSx for Lustre crée une configuration de notification d'événement sur le compartiment S3 lié. La configuration des notifications d'événements est nomméeFSx. Ne modifiez ni ne supprimez la configuration des notifications d'FSxévénements dans le compartiment S3. Cela empêchera l'importation automatique des métadonnées de fichiers et de répertoires mises à jour dans votre système de fichiers.

Lorsque FSx for Lustre met à jour une liste de fichiers qui a changé dans le référentiel de données S3 lié, il remplace le fichier local par la version mise à jour, même si le fichier est verrouillé en écriture.

FSx for Lustre fait de son mieux pour mettre à jour votre système de fichiers. FSx for Lustre ne peut pas mettre à jour le système de fichiers dans les situations suivantes :

- If FSx for Lustre n'est pas autorisé à ouvrir l'objet S3 modifié ou nouveau. Dans ce cas, FSx for Lustre ignore l'objet et continue. L'état du cycle de vie du DRA n'est pas affecté.
- If FSx for Lustre ne dispose pas d'autorisations au niveau du bucket, comme pour. `GetBucketAcl` Cela entraînera une mauvaise configuration de l'état du cycle de vie du référentiel de données. Pour de plus amples informations, veuillez consulter État du cycle de vie des associations au référentiel de données.
- Si la configuration des notifications d'`FSx`événements sur le compartiment S3 lié est supprimée ou modifiée. Cela entraînera une mauvaise configuration de l'état du cycle de vie du référentiel de données. Pour de plus amples informations, veuillez consulter État du cycle de vie des associations au référentiel de données.

Nous vous recommandons d'activer la journalisation dans CloudWatch Logs pour consigner les informations relatives aux fichiers ou répertoires qui n'ont pas pu être importés automatiquement. Les avertissements et les erreurs figurant dans le journal contiennent des informations sur la raison de l'échec. Pour de plus amples informations, veuillez consulter Journaux d'événements du référentiel de données.

Conditions préalables

Les conditions suivantes sont requises FSx pour que Lustre puisse importer automatiquement des fichiers nouveaux, modifiés ou supprimés à partir du compartiment S3 lié :

- Le système de fichiers et son compartiment S3 lié se trouvent dans le même emplacement Région AWS.
- L'état du cycle de vie du compartiment S3 n'est pas mal configuré. Pour de plus amples informations, veuillez consulter État du cycle de vie des associations au référentiel de données.
- Votre compte dispose des autorisations requises pour configurer et recevoir des notifications d'événements sur le compartiment S3 lié.

Types de modifications de fichiers pris en charge

FSx for Lustre prend en charge l'importation des modifications suivantes apportées aux fichiers et aux répertoires qui se produisent dans le compartiment S3 lié :

- Modifications apportées au contenu des fichiers.
- Modifications apportées aux métadonnées des fichiers ou des répertoires.
- Modifications apportées à la cible ou aux métadonnées du lien symbolique.
- Suppressions de fichiers et de répertoires. Si vous supprimez un objet dans le compartiment S3 lié qui correspond à un répertoire du système de fichiers (c'est-à-dire un objet dont le nom clé se termine par une barre oblique), FSx for Lustre supprime le répertoire correspondant dans le système de fichiers uniquement s'il est vide.

Mise à jour des paramètres d'importation

Vous pouvez définir les paramètres d'importation d'un système de fichiers pour un compartiment S3 lié lorsque vous créez l'association du référentiel de données. Pour de plus amples informations, veuillez consulter Création d'un lien vers un compartiment S3.

Vous pouvez également mettre à jour les paramètres d'importation à tout moment, y compris la politique d'importation. Pour de plus amples informations, veuillez consulter Mise à jour des paramètres d'association du référentiel de données.

Surveillance de l'importation automatique

Si le taux de modification de votre compartiment S3 dépasse le taux auquel l'importation automatique peut traiter ces modifications, les modifications de métadonnées correspondantes importées dans votre système de fichiers FSx for Lustre sont retardées. Dans ce cas, vous pouvez utiliser la `AgeOfOldestQueuedMessage` métrique pour surveiller l'âge de la modification la plus ancienne en attente de traitement par importation automatique. Pour plus d'informations sur cette métrique, consultezFSx pour les métriques du référentiel Lustre S3.

Si le délai d'importation des modifications des métadonnées dépasse 14 jours (tel que mesuré à l'aide de la `AgeOfOldestQueuedMessage` métrique), les modifications de votre compartiment S3 qui n'ont pas été traitées par importation automatique ne sont pas importées dans votre système de fichiers. En outre, le cycle de vie des associations de votre référentiel de données est marqué comme MAL CONFIGURÉ et l'importation automatique est arrêtée. Si l'exportation automatique est activée, l'exportation automatique continue de surveiller les modifications apportées FSx à votre système de fichiers pour Lustre. Cependant, les modifications supplémentaires ne sont pas synchronisées entre votre système de fichiers FSx for Lustre et S3.

Pour que votre association de référentiel de données passe de l'état de cycle de vie MAL CONFIGURÉ à l'état de cycle de vie DISPONIBLE, vous devez mettre à jour votre association

de référentiel de données. Vous pouvez mettre à jour l'association de votre référentiel de données à l'aide de la commande update-data-repository-associationCLI (ou de l'opération UpdateDataRepositoryAssociationAPI correspondante). Le seul paramètre de demande dont vous avez besoin est celui `AssociationID` de l'association du référentiel de données que vous souhaitez mettre à jour.

Une fois que l'état du cycle de vie de l'association du référentiel de données est passé à DISPONIBLE, l'importation automatique (et l'exportation automatique si activée) redémarre. Au redémarrage, l'exportation automatique reprend la synchronisation des modifications du système de fichiers avec S3. Pour synchroniser les métadonnées des objets nouveaux et modifiés dans S3 avec votre système de fichiers FSx for Lustre qui n'ont pas été importés ou qui proviennent d'une association de référentiel de données mal configurée, exécutez une tâche d'importation de référentiel de données. Les tâches du référentiel de données d'importation ne synchronisent pas les suppressions de votre compartiment S3 avec votre système de fichiers FSx for Lustre. Si vous souhaitez synchroniser entièrement S3 avec votre système de fichiers (y compris les suppressions), vous devez recréer votre système de fichiers.

Pour garantir que les délais d'importation des modifications des métadonnées ne dépassent pas 14 jours, nous vous recommandons de définir une alarme sur la `AgeOfOldestQueuedMessage` métrique et de réduire l'activité dans votre compartiment S3 si la `AgeOfOldestQueuedMessage` métrique dépasse votre seuil d'alarme. Pour un système de fichiers FSx pour Lustre connecté à un compartiment S3 avec une seule partition envoyant en permanence le maximum de modifications possibles depuis S3, l'importation automatique étant uniquement exécutée sur le système de fichiers FSx pour Lustre, l'importation automatique peut traiter un arriéré de 7 heures de modifications S3 en 14 jours.

En outre, avec une seule action S3, vous pouvez générer plus de modifications que ce que l'importation automatique pourra traiter en 14 jours. Des exemples de ces types d'actions incluent, sans toutefois s'y limiter, les AWS Snowball téléchargements vers S3 et les suppressions à grande échelle. Si vous apportez une modification importante à votre compartiment S3 que vous souhaitez synchroniser avec votre système de fichiers FSx pour Lustre, afin d'éviter que les modifications d'importation automatiques ne dépassent 14 jours, vous devez supprimer votre système de fichiers et le recréer une fois la modification S3 terminée.

Si votre `AgeOfOldestQueuedMessage` métrique augmente, passez en revue votre compartiment S3`GetRequests`,`PutRequests`,`PostRequests`, et `DeleteRequests` les métriques pour détecter les changements d'activité susceptibles d'entraîner une augmentation du and/or nombre de

modifications envoyées à l'importation automatique. Pour plus d'informations sur les métriques S3 disponibles, consultez la section Surveillance d'Amazon S3 dans le guide de l'utilisateur Amazon S3.

Pour une liste de toutes les métriques disponibles FSx pour Lustre, voirSurveillance avec Amazon CloudWatch.

Utilisation des tâches du référentiel de données pour importer des modifications

La tâche d'importation du référentiel de données importe les métadonnées des objets nouveaux ou modifiés dans votre référentiel de données S3, créant ainsi une nouvelle liste de fichiers ou de répertoires pour tout nouvel objet dans le référentiel de données S3. Pour tout objet modifié dans le référentiel de données, la liste de fichiers ou de répertoires correspondante est mise à jour avec les nouvelles métadonnées. Aucune action n'est entreprise pour les objets qui ont été supprimés du référentiel de données.

Utilisez les procédures suivantes pour importer les modifications de métadonnées à l'aide de la FSx console Amazon et de la CLI. Notez que vous pouvez utiliser une tâche de référentiel de données pour plusieurs DRAs.

Pour importer des modifications de métadonnées (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Systèmes de fichiers, puis choisissez votre système de Lustre fichiers.
3. Choisissez l'onglet Référentiel de données.
4. Dans le volet Associations de référentiels de données, choisissez les associations de référentiels de données pour lesquelles vous souhaitez créer la tâche d'importation.
5. Dans le menu Actions, choisissez Importer une tâche. Ce choix n'est pas disponible si le système de fichiers n'est pas lié à un référentiel de données. La page de tâches Créer un référentiel de données d'importation apparaît.
6. (Facultatif) Spécifiez jusqu'à 32 répertoires ou fichiers à importer à partir de vos compartiments S3 liés en fournissant les chemins d'accès à ces répertoires ou fichiers dans Chemins du référentiel de données à importer.

> **Note**
>
> Si le chemin que vous fournissez n'est pas valide, la tâche échoue.

7. (Facultatif) Choisissez Activer sous Rapport d'achèvement pour générer un rapport d'achèvement de la tâche une fois la tâche terminée. Un rapport d'achèvement de tâche fournit des détails sur les fichiers traités par la tâche qui répondent à l'étendue indiquée dans la section Étendue du rapport. Pour spécifier l'emplacement où Amazon doit FSx envoyer le rapport, entrez un chemin relatif dans un référentiel de données S3 lié pour le chemin du rapport.
8. Choisissez Créer.

   Une notification en haut de la page Systèmes de fichiers indique que la tâche que vous venez de créer est en cours.

Pour afficher l'état et les détails des tâches, faites défiler l'écran vers le bas jusqu'au volet Tâches du référentiel de données dans l'onglet Référentiel de données du système de fichiers. L'ordre de tri par défaut indique la tâche la plus récente en haut de la liste.

Pour afficher un résumé des tâches à partir de cette page, choisissez l'ID de tâche pour la tâche que vous venez de créer. La page Récapitulatif de la tâche apparaît.

Pour importer des modifications de métadonnées (CLI)

- Utilisez la commande `create-data-repository-task`CLI pour importer les modifications de métadonnées dans votre système de fichiers FSx for Lustre. L'opération d'API correspondante est `CreateDataRepositoryTask`.

  ```
  $ aws fsx create-data-repository-task \
      --file-system-id fs-0123456789abcdef0 \
      --type IMPORT_METADATA_FROM_REPOSITORY \
      --paths s3://bucketname1/dir1/path1 \
      --report Enabled=true,Path=s3://bucketname1/dir1/
  path1,Format=REPORT_CSV_20191124,Scope=FAILED_FILES_ONLY
  ```

  Après avoir créé avec succès la tâche du référentiel de données, Amazon FSx renvoie la description de la tâche au format JSON.

Après avoir créé la tâche d'importation de métadonnées depuis le référentiel de données lié, vous pouvez vérifier le statut de la tâche d'importation du référentiel de données. Pour plus d'informations sur l'affichage des tâches du référentiel de données, consultezAccès aux tâches du référentiel de données.

Préchargement de fichiers dans votre système de fichiers

Vous pouvez éventuellement précharger le contenu de fichiers ou de répertoires individuels dans votre système de fichiers.

Importation de fichiers à l'aide de commandes HSM

Amazon FSx copie les données de votre référentiel de données Amazon S3 lors du premier accès à un fichier. En raison de cette approche, la lecture ou l'écriture initiale d'un fichier entraîne une faible latence. Si votre application est sensible à cette latence et que vous savez à quels fichiers ou répertoires elle doit accéder, vous pouvez éventuellement précharger le contenu de fichiers ou de répertoires individuels. Pour ce faire, utilisez la `hsm_restore` commande suivante.

Vous pouvez utiliser la `hsm_action` commande (émise avec l'utilitaire `lfs` utilisateur) pour vérifier que le chargement du contenu du fichier dans le système de fichiers est terminé. Une valeur renvoyée de `NOOP` indique que le fichier a été chargé avec succès. Exécutez les commandes suivantes à partir d'une instance de calcul avec le système de fichiers monté. *`path/to/file`*Remplacez-le par le chemin du fichier que vous êtes en train de précharger dans votre système de fichiers.

```
sudo lfs hsm_restore path/to/file
sudo lfs hsm_action path/to/file
```

Vous pouvez précharger l'ensemble de votre système de fichiers ou un répertoire entier au sein de votre système de fichiers à l'aide des commandes suivantes. (L'esperluette de fin fait exécuter une commande en arrière-plan.) Si vous demandez le préchargement de plusieurs fichiers simultanément, Amazon FSx charge vos fichiers depuis votre référentiel de données Amazon S3 en parallèle. Si un fichier a déjà été chargé dans le système de fichiers, la `hsm_restore` commande ne le recharge pas.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_restore &
```

> **Note**
>
> Si votre compartiment S3 lié est plus grand que votre système de fichiers, vous devriez être en mesure d'importer toutes les métadonnées du fichier dans votre système de fichiers. Cependant, vous ne pouvez charger que la quantité de données de fichier réelles correspondant à l'espace de stockage restant dans le système de fichiers. Vous recevrez un message d'erreur si vous tentez d'accéder aux données d'un fichier alors qu'il n'y a plus d'espace de stockage sur le système de fichiers. Dans ce cas, vous pouvez augmenter la capacité de stockage selon vos besoins. Pour de plus amples informations, veuillez consulter Gestion de la capacité de stockage.

Étape de validation

Vous pouvez exécuter le script bash répertorié ci-dessous pour découvrir le nombre de fichiers ou d'objets archivés (publiés).

Pour améliorer les performances du script, en particulier dans les systèmes de fichiers contenant un grand nombre de fichiers, les threads du processeur sont automatiquement déterminés en fonction du `/proc/cpuproc` fichier. En d'autres termes, vous bénéficierez de performances plus rapides avec une instance Amazon EC2 dotée d'un plus grand nombre de vCPU.

1. Configurez le script bash.

```
#!/bin/bash

# Check if a directory argument is provided
if [ $# -ne 1 ]; then
    echo "Usage: $0 /path/to/lustre/mount"
    exit 1
fi

# Set the root directory from the argument
ROOT_DIR="$1"

# Check if the provided directory exists
if [ ! -d "$ROOT_DIR" ]; then
    echo "Error: Directory $ROOT_DIR does not exist."
    exit 1
fi
```

```
# Automatically detect number of CPUs and set threads
if command -v nproc &> /dev/null; then
    THREADS=$(nproc)
elif [ -f /proc/cpuinfo ]; then
    THREADS=$(grep -c ^processor /proc/cpuinfo)
else
    echo "Unable to determine number of CPUs. Defaulting to 1 thread."
    THREADS=1
fi

# Output file
OUTPUT_FILE="released_objects_$(date +%Y%m%d_%H%M%S).txt"

echo "Searching in $ROOT_DIR for all released objects using $THREADS threads"
echo "This may take a while depending on the size of the filesystem..."

# Find all released files in the specified lustre directory using parallel
# If you  get false positives for file names/paths that include the word
 'released',
# you can grep 'released exists archived' instead of just 'released'
time sudo lfs find "$ROOT_DIR" -type f | \
parallel --will-cite -j "$THREADS" -n 1000 "sudo lfs hsm_state {} | grep released"
 > "$OUTPUT_FILE"

echo "Search complete. Released objects are listed in $OUTPUT_FILE"
echo "Total number of released objects: $(wc -l <"$OUTPUT_FILE")"
```

2. Rendez le script exécutable :

```
$ chmod +x find_lustre_released_files.sh
```

3. Exécutez le script, comme dans l'exemple suivant :

```
$ ./find_lustre_released_files.sh /fsxl/sample
Searching in /fsxl/sample for all released objects using 16 threads
This may take a while depending on the size of the filesystem...
real 0m9.906s
user 0m1.502s
sys 0m5.653s
Search complete. Released objects are listed in
 released_objects_20241121_184537.txt
Total number of released objects: 30000
```

Si des objets publiés sont présents, effectuez une restauration en bloc dans les répertoires souhaités afin de transférer les fichiers vers Lustre FSx depuis S3, comme dans l'exemple suivant :

```
$ DIR=/path/to/lustre/mount
$ nohup find $DIR -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_restore &
```

Notez que cela `hsm_restore` prendra un certain temps lorsqu'il y a des millions de fichiers.

Exportation des modifications vers le référentiel de données

Vous pouvez exporter les modifications apportées aux données et aux métadonnées POSIX de votre système de fichiers FSx for Lustre vers un référentiel de données lié. Les métadonnées POSIX associées incluent la propriété, les autorisations et les horodatages.

Pour exporter les modifications depuis le système de fichiers, appliquez l'une des méthodes suivantes.

- Configurez votre système de fichiers pour exporter automatiquement les fichiers nouveaux, modifiés ou supprimés vers votre référentiel de données lié. Pour de plus amples informations, veuillez consulter Exportez automatiquement les mises à jour vers votre compartiment S3.
- Utilisez une tâche de référentiel de données d'exportation à la demande. Pour de plus amples informations, consultez Utilisation des tâches du référentiel de données pour exporter les modifications.

Les tâches d'exportation automatique et d'exportation du référentiel de données ne peuvent pas être exécutées en même temps.

> **Important**
>
> L'exportation automatique ne synchronisera pas les opérations de métadonnées suivantes sur votre système de fichiers avec S3 si les objets correspondants sont stockés dans S3 Glacier Flexible Retrieval :
>
> - chmod
> - étouffé
> - renommer

Lorsque vous activez l'exportation automatique pour une association de référentiels de données, votre système de fichiers exporte automatiquement les données des fichiers et les modifications de métadonnées au fur et à mesure que les fichiers sont créés, modifiés ou supprimés. Lorsque vous exportez des fichiers ou des répertoires à l'aide d'une tâche de référentiel de données d'exportation, votre système de fichiers exporte uniquement les fichiers de données et les métadonnées créés ou modifiés depuis la dernière exportation.

Les tâches d'exportation et d'exportation automatiques du référentiel de données exportent les métadonnées POSIX. Pour de plus amples informations, veuillez consulter Support des métadonnées POSIX pour les référentiels de données.

Important

- FSx Pour que Lustre puisse exporter vos données vers votre compartiment S3, celles-ci doivent être stockées dans un format compatible UTF-8.
- Les clés d'objet S3 ont une longueur maximale de 1 024 octets. FSx for Lustre n'exportera pas les fichiers dont la clé d'objet S3 correspondante serait supérieure à 1 024 octets.

Note

Tous les objets créés par les tâches de référentiel de données d'exportation et d'exportation automatiques sont écrits à l'aide de la classe de stockage S3 Standard.

Rubriques

- Exportez automatiquement les mises à jour vers votre compartiment S3
- Utilisation des tâches du référentiel de données pour exporter les modifications
- Exportation de fichiers à l'aide de commandes HSM

Exportez automatiquement les mises à jour vers votre compartiment S3

Vous pouvez configurer votre système de fichiers FSx for Lustre pour mettre à jour automatiquement le contenu d'un compartiment S3 lié à mesure que des fichiers sont ajoutés, modifiés ou supprimés dans le système de fichiers. FSx for Lustre crée, met à jour ou supprime l'objet dans S3, en fonction de la modification du système de fichiers.

> **Note**
>
> L'exportation automatique n'est pas disponible sur FSx les systèmes de fichiers Lustre 2.10 ou les systèmes de `Scratch 1` fichiers.

Vous pouvez exporter vers un référentiel de données qui se trouve dans le même système de fichiers Région AWS que le système de fichiers ou dans un autre Région AWS.

Vous pouvez configurer l'exportation automatique lorsque vous créez l'association au référentiel de données et que vous mettez à jour les paramètres d'exportation automatique à tout moment à l'aide de la console de FSx gestion AWS CLI, du et de l' AWS API.

> **Important**
>
> - Si un fichier est modifié dans le système de fichiers alors que toutes les politiques d'exportation automatique sont activées et que l'importation automatique est désactivée, le contenu de ce fichier est toujours exporté vers un objet correspondant dans S3. Si un objet existe déjà à l'emplacement cible, il est remplacé.
> - Si un fichier est modifié à la fois dans le système de fichiers et dans S3, alors que toutes les politiques d'importation et d'exportation automatiques sont activées, le fichier du système de fichiers ou l'objet de S3 peuvent être remplacés par l'autre. Il n'est pas garanti qu'une modification ultérieure à un endroit remplacera une modification antérieure à un autre emplacement. Si vous modifiez le même fichier à la fois dans le système de fichiers et dans le compartiment S3, vous devez garantir la coordination au niveau de l'application afin d'éviter de tels conflits. FSx for Lustre n'empêche pas les écritures conflictuelles à plusieurs endroits.

La politique d'exportation indique comment vous souhaitez que FSx Lustre mette à jour votre compartiment S3 lié à mesure que le contenu change dans le système de fichiers. Une association de référentiels de données peut avoir l'une des politiques d'exportation automatique suivantes :

- Nouveau — FSx for Lustre met automatiquement à jour le référentiel de données S3 uniquement lorsqu'un nouveau fichier, répertoire ou lien symbolique est créé sur le système de fichiers.
- Modifié — FSx pour Lustre met automatiquement à jour le référentiel de données S3 uniquement lorsqu'un fichier existant dans le système de fichiers est modifié. Pour les modifications du contenu

du fichier, le fichier doit être fermé avant d'être propagé dans le référentiel S3. Les modifications des métadonnées (changement de nom, propriété, autorisations et horodatages) sont propagées lorsque l'opération est terminée. Pour renommer les modifications (y compris les déplacements), l'objet S3 existant (prérenommé) est supprimé et un nouvel objet S3 est créé avec le nouveau nom.

- Supprimé : FSx pour Lustre met automatiquement à jour le référentiel de données S3 uniquement lorsqu'un fichier, un répertoire ou un lien symbolique est supprimé dans le système de fichiers.
- Toute combinaison de Nouveau, Modifié et Supprimé — FSx for Lustre met automatiquement à jour le référentiel de données S3 lorsque l'une des actions spécifiées se produit dans le système de fichiers. Par exemple, vous pouvez spécifier que le référentiel S3 est mis à jour lorsqu'un fichier est ajouté au système de fichiers (Nouveau) ou supprimé de (Supprimé), mais pas lorsqu'un fichier est modifié.
- Aucune politique configurée : FSx car Lustre ne met pas automatiquement à jour le référentiel de données S3 lorsque des fichiers sont ajoutés, modifiés ou supprimés du système de fichiers. Si vous ne configurez pas de politique d'exportation, l'exportation automatique est désactivée. Vous pouvez toujours exporter manuellement les modifications à l'aide d'une tâche de référentiel de données d'exportation, comme décrit dansUtilisation des tâches du référentiel de données pour exporter les modifications.

Dans la plupart des cas d'utilisation, nous vous recommandons de configurer une politique d'exportation comprenant les valeurs Nouveau, Modifié et Supprimé. Cette politique garantit que toutes les mises à jour effectuées sur votre système de fichiers sont automatiquement exportées vers votre référentiel de données S3 lié.

Nous vous recommandons d'activer la journalisation dans CloudWatch Logs pour consigner les informations relatives aux fichiers ou répertoires qui n'ont pas pu être exportés automatiquement. Les avertissements et les erreurs figurant dans le journal contiennent des informations sur la raison de l'échec. Pour de plus amples informations, veuillez consulter Journaux d'événements du référentiel de données.

> **Note**
>
> Bien que l'heure d'accès (`atime`) et l'heure de modification (`mtime`) soient synchronisées avec S3 pendant les opérations d'exportation, les modifications apportées à ces horodatages ne déclenchent pas à elles seules l'exportation automatique. Seules les modifications apportées au contenu du fichier ou à d'autres métadonnées (telles que la propriété ou les autorisations) déclencheront une exportation automatique vers S3.

Mise à jour des paramètres d'exportation

Vous pouvez définir les paramètres d'exportation d'un système de fichiers vers un compartiment S3 lié lorsque vous créez l'association du référentiel de données. Pour de plus amples informations, veuillez consulter Création d'un lien vers un compartiment S3.

Vous pouvez également mettre à jour les paramètres d'exportation à tout moment, y compris la politique d'exportation. Pour de plus amples informations, veuillez consulter Mise à jour des paramètres d'association du référentiel de données.

Surveillance de l'exportation automatique

Vous pouvez surveiller les associations de référentiels de données activées pour l'exportation automatique à l'aide d'un ensemble de statistiques publiées sur Amazon CloudWatch. La `AgeOfOldestQueuedMessage` métrique représente l'âge de la plus ancienne mise à jour apportée au système de fichiers qui n'a pas encore été exportée vers S3. Si le nombre `AgeOfOldestQueuedMessage` est supérieur à zéro pendant une période prolongée, nous recommandons de réduire temporairement le nombre de modifications (renommage de répertoire en particulier) qui sont activement apportées au système de fichiers jusqu'à ce que la file de messages soit réduite. Pour de plus amples informations, veuillez consulter FSx pour les métriques du référentiel Lustre S3.

> **Important**
>
> Lorsque vous supprimez une association de référentiel de données ou un système de fichiers avec l'exportation automatique activée, vous devez d'abord vous assurer que ce chiffre `AgeOfOldestQueuedMessage` est égal à zéro, ce qui signifie qu'aucune modification n'a encore été exportée. S'il `AgeOfOldestQueuedMessage` est supérieur à zéro lorsque vous supprimez votre association de référentiel de données ou votre système de fichiers, les modifications qui n'ont pas encore été exportées n'atteindront pas votre compartiment S3 lié. Pour éviter cela, attendez d'`AgeOfOldestQueuedMessage`atteindre zéro avant de supprimer votre association de référentiel de données ou votre système de fichiers.

Utilisation des tâches du référentiel de données pour exporter les modifications

La tâche d'exportation du référentiel de données permet d'exporter les fichiers nouveaux ou modifiés dans votre système de fichiers. Il crée un nouvel objet dans S3 pour tout nouveau fichier du système de fichiers. Pour tout fichier modifié dans le système de fichiers ou dont les métadonnées ont été modifiées, l'objet correspondant dans S3 est remplacé par un nouvel objet contenant les nouvelles données et métadonnées. Aucune action n'est entreprise pour les fichiers qui ont été supprimés du système de fichiers.

> **Note**
>
> Tenez compte des points suivants lorsque vous utilisez des tâches de référentiel de données d'exportation :
>
> - L'utilisation de caractères génériques pour inclure ou exclure des fichiers à exporter n'est pas prise en charge.
> - Lorsque vous effectuez `mv` des opérations, le fichier cible après avoir été déplacé sera exporté vers S3 même s'il n'y a aucun UID, GID, autorisation ou modification du contenu.

Utilisez les procédures suivantes pour exporter les modifications de données et de métadonnées du système de fichiers vers des compartiments S3 liés à l'aide de la FSx console Amazon et de la CLI. Notez que vous pouvez utiliser une tâche de référentiel de données pour plusieurs DRAs.

Pour exporter les modifications (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Systèmes de fichiers, puis choisissez votre système de Lustre fichiers.
3. Choisissez l'onglet Référentiel de données.
4. Dans le volet Associations de référentiels de données, choisissez l'association de référentiels de données pour laquelle vous souhaitez créer la tâche d'exportation.
5. Pour Actions, choisissez Exporter la tâche. Ce choix n'est pas disponible si le système de fichiers n'est pas lié à un référentiel de données sur S3. La boîte de dialogue Créer un référentiel de données d'exportation apparaît.

6. (Facultatif) Spécifiez jusqu'à 32 répertoires ou fichiers à exporter depuis votre système de FSx fichiers Amazon en fournissant les chemins d'accès à ces répertoires ou fichiers dans Chemins du système de fichiers à exporter. Les chemins que vous fournissez doivent être relatifs au point de montage du système de fichiers. Si le point de montage `/mnt/fsx/path1` est `/mnt/fsx` et reste un répertoire ou un fichier du système de fichiers que vous souhaitez exporter, le chemin à fournir est`path1`.

   > **Note**
   >
   > Si le chemin que vous fournissez n'est pas valide, la tâche échoue.

7. (Facultatif) Choisissez Activer sous Rapport d'achèvement pour générer un rapport d'achèvement de la tâche une fois la tâche terminée. Un rapport d'achèvement de tâche fournit des détails sur les fichiers traités par la tâche qui répondent à l'étendue indiquée dans la section Étendue du rapport. Pour spécifier l'emplacement où Amazon doit FSx envoyer le rapport, entrez un chemin relatif dans le référentiel de données S3 lié au système de fichiers pour le chemin du rapport.
8. Choisissez Créer.

   Une notification en haut de la page Systèmes de fichiers indique que la tâche que vous venez de créer est en cours.

Pour afficher l'état et les détails des tâches, faites défiler l'écran vers le bas jusqu'au volet Tâches du référentiel de données dans l'onglet Référentiel de données du système de fichiers. L'ordre de tri par défaut indique la tâche la plus récente en haut de la liste.

Pour afficher un résumé des tâches à partir de cette page, choisissez l'ID de tâche pour la tâche que vous venez de créer. La page Récapitulatif de la tâche apparaît.

Pour exporter les modifications (CLI)

- Utilisez la commande `create-data-repository-task`CLI pour exporter les modifications de données et de métadonnées sur votre système de fichiers FSx for Lustre. L'opération d'API correspondante est `CreateDataRepositoryTask`.

```
$ aws fsx create-data-repository-task \
    --file-system-id fs-0123456789abcdef0 \
    --type EXPORT_TO_REPOSITORY \
    --paths path1,path2/file1 \
```

```
    --report Enabled=true
```

Après avoir créé avec succès la tâche du référentiel de données, Amazon FSx renvoie la description de la tâche au format JSON, comme illustré dans l'exemple suivant.

```
{
    "Task": {
        "TaskId": "task-123f8cd8e330c1321",
        "Type": "EXPORT_TO_REPOSITORY",
        "Lifecycle": "PENDING",
        "FileSystemId": "fs-0123456789abcdef0",
        "Paths": ["path1", "path2/file1"],
        "Report": {
            "Path":"s3://dataset-01/reports",
            "Format":"REPORT_CSV_20191124",
            "Enabled":true,
            "Scope":"FAILED_FILES_ONLY"
        },
        "CreationTime": "1545070680.120",
        "ClientRequestToken": "10192019-drt-12",
        "ResourceARN": "arn:aws:fsx:us-
east-1:123456789012:task:task-123f8cd8e330c1321"
    }
}
```

Après avoir créé la tâche d'exportation des données vers le référentiel de données lié, vous pouvez vérifier le statut de la tâche d'exportation du référentiel de données. Pour plus d'informations sur l'affichage des tâches du référentiel de données, consultezAccès aux tâches du référentiel de données.

Exportation de fichiers à l'aide de commandes HSM

> **Note**
>
> Pour exporter les modifications apportées aux données et aux métadonnées de votre FSx système de fichiers for Lustre vers un référentiel de données durable sur Amazon S3, utilisez la fonctionnalité d'exportation automatique décrite dansExportez automatiquement les mises à jour vers votre compartiment S3. Vous pouvez également utiliser les tâches du référentiel

de données d'exportation, décrites dansUtilisation des tâches du référentiel de données pour exporter les modifications.

Pour exporter un fichier individuel vers votre référentiel de données et vérifier que le fichier a bien été exporté vers votre référentiel de données, vous pouvez exécuter les commandes ci-dessous. Une valeur de retour de `states: (0x00000009) exists archived` indique que le fichier a été correctement exporté.

```
sudo lfs hsm_archive path/to/export/file
sudo lfs hsm_state path/to/export/file
```

> **Note**
>
> Vous devez exécuter les commandes HSM (par exemple`hsm_archive`) en tant qu'utilisateur root ou en utilisant`sudo`.

Pour exporter l'intégralité de votre système de fichiers ou un répertoire entier de votre système de fichiers, exécutez les commandes suivantes. Si vous exportez plusieurs fichiers simultanément, Amazon FSx for Lustre les exporte en parallèle vers votre référentiel de données Amazon S3.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 sudo lfs hsm_archive &
```

Pour déterminer si l'exportation est terminée, exécutez la commande suivante.

```
find path/to/export/file -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_state | awk
 '!/\<archived\>/ || /\<dirty\>/' | wc -l
```

Si la commande revient alors qu'il ne reste aucun fichier, l'exportation est terminée.

Tâches du référentiel de données

En utilisant des tâches d'importation et d'exportation de référentiels de données, vous pouvez gérer le transfert de données et de métadonnées entre votre système de fichiers FSx for Lustre et l'un de ses référentiels de données durables sur Amazon S3.

Les tâches de référentiel de données optimisent les transferts de données et de métadonnées entre votre système de fichiers FSx for Lustre et un référentiel de données sur S3. Pour ce faire, ils suivent notamment les modifications entre votre système de FSx fichiers Amazon et son référentiel de données lié. Pour ce faire, ils utilisent également des techniques de transfert parallèle pour transférer des données à des vitesses allant jusqu'à des centaines de GBps. Vous créez et visualisez les tâches du référentiel de données à l'aide de la FSx console Amazon AWS CLI, du, et de l' FSx API Amazon.

Les tâches du référentiel de données conservent les métadonnées de l'interface du système d'exploitation portable (POSIX) du système de fichiers, notamment la propriété, les autorisations et les horodatages. Étant donné que les tâches conservent ces métadonnées, vous pouvez implémenter et maintenir des contrôles d'accès entre votre système de fichiers FSx for Lustre et ses référentiels de données liés.

Vous pouvez utiliser une tâche de référentiel de données de publication pour libérer de l'espace dans le système de fichiers pour les nouveaux fichiers en libérant les fichiers exportés vers Amazon S3. Le contenu du fichier publié est supprimé, mais les métadonnées du fichier publié restent dans le système de fichiers. Les utilisateurs et les applications peuvent toujours accéder à un fichier publié en le lisant à nouveau. Lorsque l'utilisateur ou l'application lit le fichier publié, FSx for Lustre récupère de manière transparente le contenu du fichier sur Amazon S3.

Types de tâches liées au référentiel de données

Il existe trois types de tâches de référentiel de données :

- Les tâches d'exportation du référentiel de données sont exportées de votre système de Lustre fichiers vers un compartiment S3 lié.
- Importer les tâches du référentiel de données est importé depuis un compartiment S3 lié vers votre système de Lustre fichiers.
- Les tâches du référentiel de données de publication libèrent les fichiers exportés vers un compartiment S3 lié depuis votre système de Lustre fichiers.

Pour de plus amples informations, veuillez consulter Création d'une tâche de référentiel de données.

Rubriques

- Comprendre le statut et les détails d'une tâche
- Utilisation des tâches du référentiel de données

- Utilisation des rapports d'achèvement des tâches
- Résolution des défaillances des tâches du référentiel de données

Comprendre le statut et les détails d'une tâche

Une tâche de référentiel de données contient des informations descriptives et un état du cycle de vie.

Après la création d'une tâche, vous pouvez consulter les informations détaillées suivantes pour une tâche de référentiel de données à l'aide de la FSx console, de la CLI ou de l'API Amazon :

- Type de tâche :
  - `EXPORT_TO_REPOSITORY`indique une tâche d'exportation.
  - `IMPORT_METADATA_FROM_REPOSITORY`indique une tâche d'importation.
  - `RELEASE_DATA_FROM_FILESYSTEM`indique une tâche de publication.
- Système de fichiers sur lequel la tâche s'est exécutée.
- Heure de création de la tâche.
- État de la tâche.
- Nombre total de fichiers traités par la tâche.
- Nombre total de fichiers traités avec succès par la tâche.
- Nombre total de fichiers que la tâche n'a pas pu traiter. Cette valeur est supérieure à zéro lorsque le statut de la tâche est FAILED. Des informations détaillées sur les fichiers qui ont échoué sont disponibles dans un rapport d'achèvement des tâches. Pour de plus amples informations, veuillez consulter Utilisation des rapports d'achèvement des tâches.
- Heure à laquelle la tâche a commencé.
- Heure à laquelle le statut de la tâche a été mis à jour pour la dernière fois. L'état de la tâche est mis à jour toutes les 30 secondes.

Une tâche de référentiel de données peut avoir l'un des statuts suivants :

- PENDING indique qu'Amazon n' FSx a pas démarré la tâche.
- EXECUTING indique qu'Amazon FSx est en train de traiter la tâche.
- FAILED indique qu'Amazon FSx n'a pas traité correctement la tâche. Par exemple, il se peut que la tâche n'ait pas pu traiter certains fichiers. Les détails de la tâche fournissent plus d'informations

sur l'échec. Pour plus d'informations sur les tâches qui ont échoué, consultezRésolution des défaillances des tâches du référentiel de données.

- SUCCEDED indique qu'Amazon FSx a terminé la tâche avec succès.
- CANCELLED indique que la tâche a été annulée et n'est pas terminée.
- L'ANNULATION indique qu'Amazon FSx est en train d'annuler la tâche.

Les informations sur les tâches du référentiel de données sont conservées pendant 14 jours après la fin de la tâche. Pour plus d'informations sur l'accès aux tâches du référentiel de données existantes, consultezAccès aux tâches du référentiel de données.

Utilisation des tâches du référentiel de données

Dans les sections suivantes, vous trouverez des informations détaillées sur la gestion des tâches du référentiel de données. Vous pouvez créer, dupliquer, afficher les détails et annuler les tâches du référentiel de données à l'aide de la FSx console, de la CLI ou de l'API Amazon.

Rubriques

- Création d'une tâche de référentiel de données
- Dupliquer une tâche
- Accès aux tâches du référentiel de données
- Annulation d'une tâche de référentiel de données

Création d'une tâche de référentiel de données

Vous pouvez créer une tâche de référentiel de données à l'aide de la FSx console, de la CLI ou de l'API Amazon. Après avoir créé une tâche, vous pouvez consulter sa progression et son statut à l'aide de la console, de la CLI ou de l'API.

Vous pouvez créer trois types de tâches de référentiel de données :

- La tâche Exporter le référentiel de données permet d'exporter depuis votre système de Lustre fichiers vers un compartiment S3 lié. Pour de plus amples informations, veuillez consulter Utilisation des tâches du référentiel de données pour exporter les modifications.
- La tâche Importer un référentiel de données permet d'importer depuis un compartiment S3 lié vers votre système de Lustre fichiers. Pour de plus amples informations, veuillez consulter Utilisation des tâches du référentiel de données pour importer des modifications.

- La tâche Publier le référentiel de données libère les fichiers de votre Lustre système de fichiers qui ont été exportés vers un compartiment S3 lié. Pour de plus amples informations, veuillez consulter Utilisation des tâches du référentiel de données pour publier des fichiers.

Dupliquer une tâche

Vous pouvez dupliquer une tâche de référentiel de données existante dans la FSx console Amazon. Lorsque vous dupliquez une tâche, une copie exacte de la tâche existante s'affiche sur la page Créer une tâche de référentiel de données d'importation ou Créer une tâche de référentiel de données d'exportation. Vous pouvez modifier les chemins à exporter ou à importer, selon vos besoins, avant de créer et d'exécuter la nouvelle tâche.

> **Note**
>
> Une demande d'exécution d'une tâche dupliquée échouera si une copie exacte de cette tâche est déjà en cours d'exécution. Une copie exacte d'une tâche déjà en cours d'exécution contient le ou les mêmes chemins de système de fichiers dans le cas d'une tâche d'exportation ou les mêmes chemins de référentiel de données dans le cas d'une tâche d'importation.

Vous pouvez dupliquer une tâche depuis la vue détaillée des tâches, le volet Tâches du référentiel de données de l'onglet Référentiel de données du système de fichiers ou depuis la page des tâches du référentiel de données.

Pour dupliquer une tâche existante

1. Choisissez une tâche dans le volet Tâches du référentiel de données de l'onglet Référentiel de données du système de fichiers.
2. Choisissez Dupliquer la tâche. Selon le type de tâche que vous avez choisi, la page Créer une tâche de référentiel de données d'importation ou Créer une tâche de référentiel de données d'exportation apparaît. Tous les paramètres de la nouvelle tâche sont identiques à ceux de la tâche que vous dupliquez.
3. Modifiez ou ajoutez les chemins que vous souhaitez importer ou vers lesquels vous souhaitez exporter.
4. Choisissez Créer.

Accès aux tâches du référentiel de données

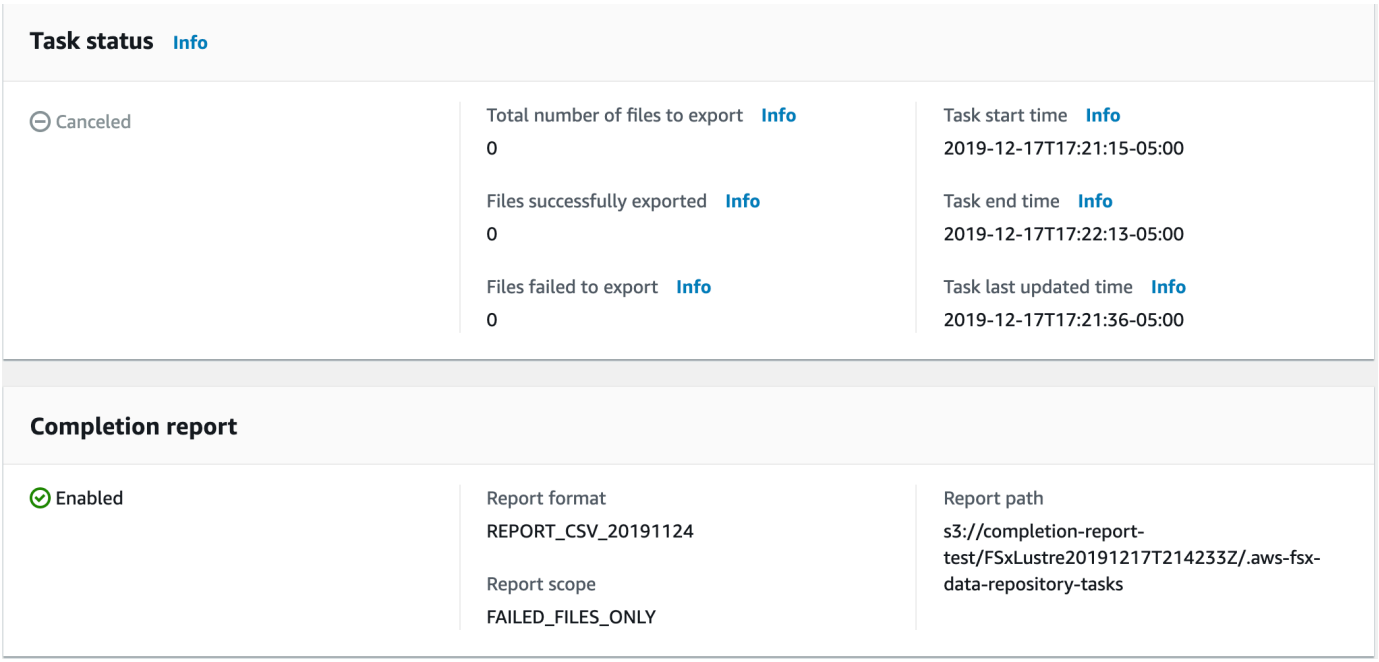
Après avoir créé une tâche de référentiel de données, vous pouvez accéder à cette tâche, ainsi qu'à toutes les tâches existantes de votre compte, à l'aide de la FSx console, de la CLI et de l'API Amazon. Amazon FSx fournit les informations détaillées suivantes sur les tâches :

- Toutes les tâches existantes.
- Toutes les tâches relatives à un système de fichiers spécifique.
- Toutes les tâches relatives à une association de référentiels de données spécifique.
- Toutes les tâches ayant un statut de cycle de vie spécifique. Pour plus d'informations sur les valeurs d'état du cycle de vie des tâches, consultezComprendre le statut et les détails d'une tâche.

Vous pouvez accéder à toutes les tâches du référentiel de données existantes dans votre compte à l'aide de la FSx console, de la CLI ou de l'API Amazon, comme décrit ci-dessous.

Pour afficher les tâches du référentiel de données et les détails des tâches (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez le système de fichiers pour lequel vous souhaitez afficher les tâches du référentiel de données. La page de détails du système de fichiers apparaît.
3. Sur la page des détails du système de fichiers, choisissez l'onglet Référentiel de données. Toutes les tâches de ce système de fichiers apparaissent dans le panneau des tâches du référentiel de données.
4. Pour voir les détails d'une tâche, choisissez l'ID de tâche ou le nom de la tâche dans le panneau des tâches du référentiel de données. La page détaillée de la tâche apparaît.



Pour récupérer les tâches du référentiel de données et les détails des tâches (CLI)

À l'aide de la commande Amazon FSx `describe-data-repository-tasks`CLI, vous pouvez consulter toutes les tâches du référentiel de données, ainsi que leurs détails, dans votre compte. `DescribeDataRepositoryTasks`est la commande API équivalente.

- Utilisez la commande suivante pour afficher tous les objets de tâche du référentiel de données de votre compte.

```
aws fsx describe-data-repository-tasks
```

Si la commande aboutit, Amazon FSx renvoie la réponse au format JSON.

```
{
    "DataRepositoryTasks": [
        {
            "Lifecycle": "EXECUTING",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-01/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
```

```
            "StartTime": 1591863862.288,
            "EndTime": ,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef3",
            "Status": {
                "SucceededCount": 4255,
                "TotalCount": 4200,
                "FailedCount": 55,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789a7",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef3"
        },
        {
            "Lifecycle": "FAILED",
            "Paths": [],
            "Report": {
                "Enabled": false,
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef1",
            "Status": {
                "SucceededCount": 1153,
                "TotalCount": 1156,
                "FailedCount": 3,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
        },
        {
            "Lifecycle": "SUCCEEDED",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-04/reports",
                "Format":"REPORT_CSV_20191124",
```

```
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-04299453935122318",
            "Status": {
                "SucceededCount": 258,
                "TotalCount": 258,
                "FailedCount": 0,
                "LastUpdatedTime": 1771848950.012,
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1771848950.012,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
        }
    ]
}
```

Affichage des tâches par système de fichiers

Vous pouvez afficher toutes les tâches relatives à un système de fichiers spécifique à l'aide de la FSx console, de la CLI ou de l'API Amazon, comme décrit ci-dessous.

Pour afficher les tâches par système de fichiers (console)

1. Choisissez Systèmes de fichiers dans le volet de navigation. La page Systèmes de fichiers apparaît.
2. Choisissez le système de fichiers pour lequel vous souhaitez afficher les tâches du référentiel de données. La page de détails du système de fichiers apparaît.
3. Sur la page des détails du système de fichiers, choisissez l'onglet Référentiel de données. Toutes les tâches de ce système de fichiers apparaissent dans le panneau des tâches du référentiel de données.

Pour récupérer des tâches par système de fichiers (CLI)

- Utilisez la commande suivante pour afficher toutes les tâches du référentiel de données pour le système de fichiers`fs-0123456789abcdef0`.

```
aws fsx describe-data-repository-tasks \
    --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

Si la commande aboutit, Amazon FSx renvoie la réponse au format JSON.

```
{
    "DataRepositoryTasks": [
        {
            "Lifecycle": "FAILED",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-04/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef1",
            "Status": {
                "SucceededCount": 1153,
                "TotalCount": 1156,
                "FailedCount": 3,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
        },
        {
            "Lifecycle": "SUCCEEDED",
            "Paths": [],
            "Report": {
                "Enabled": false,
```

```
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef0",
            "Status": {
                "SucceededCount": 258,
                "TotalCount": 258,
                "FailedCount": 0,
                "LastUpdatedTime": 1771848950.012,
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1771848950.012,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
        }
    ]
}
```


Annulation d'une tâche de référentiel de données

Vous pouvez annuler une tâche du référentiel de données lorsqu'elle est en attente ou en cours d'exécution. Lorsque vous annulez une tâche, les événements suivants se produisent :

- Amazon FSx ne traite aucun fichier figurant dans la file d'attente à traiter.
- Amazon FSx continue de traiter tous les fichiers en cours de traitement.
- Amazon FSx ne rétablit aucun fichier déjà traité par la tâche.

Pour annuler une tâche de référentiel de données (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Cliquez sur le système de fichiers pour lequel vous souhaitez annuler une tâche de référentiel de données.
3. Ouvrez l'onglet Référentiel de données et faites défiler la page vers le bas pour afficher le panneau Tâches du référentiel de données.
4. Choisissez un ID de tâche ou un nom de tâche pour la tâche que vous souhaitez annuler.
5. Choisissez Annuler la tâche pour annuler la tâche.

6. Entrez l'ID de tâche pour confirmer la demande d'annulation.

Pour annuler une tâche de référentiel de données (CLI)

Utilisez la commande Amazon FSx `cancel-data-repository-task`CLI pour annuler une tâche. `CancelDataRepositoryTask`est la commande API équivalente.

- Utilisez la commande suivante pour annuler une tâche de référentiel de données.

```
aws fsx cancel-data-repository-task \
    --task-id task-0123456789abcdef0
```

Si la commande aboutit, Amazon FSx renvoie la réponse au format JSON.

```
{
    "Status": "CANCELING",
    "TaskId": "task-0123456789abcdef0"
}
```

Utilisation des rapports d'achèvement des tâches

Un rapport d'achèvement de tâche fournit des détails sur les résultats d'une tâche d'exportation, d'importation ou de publication du référentiel de données. Le rapport inclut les résultats des fichiers traités par la tâche qui correspondent à l'étendue du rapport. Vous pouvez spécifier si vous souhaitez générer un rapport pour une tâche à l'aide du `Enabled` paramètre.

Amazon FSx envoie le rapport au référentiel de données lié du système de fichiers dans Amazon S3, en utilisant le chemin que vous spécifiez lorsque vous activez le rapport pour une tâche. Le nom de fichier du rapport est `report.csv` destiné aux tâches d'importation et `failures.csv` aux tâches d'exportation ou de publication.

Le format du rapport est un fichier de valeurs séparées par des virgules (CSV) qui comporte trois champs : `FilePathFileStatus`, et. `ErrorCode`

Les rapports sont codés au format RFC-4180 comme suit :

- Les chemins commençant par l'un des caractères suivants sont placés entre guillemets simples : `@ + - =`

- Les chaînes contenant au moins l'un des caractères suivants sont placées entre guillemets doubles : " ,
- Tous les guillemets doubles sont masqués par un guillemet double supplémentaire.

Voici quelques exemples de codage des rapports :

- `@filename.txt`devient `"""@filename.txt"""`
- `+filename.txt`devient `"""+filename.txt"""`
- `file,name.txt`devient `"file,name.txt"`
- `file"name.txt`devient `"file""name.txt"`

Pour plus d'informations sur le codage RFC-4180, voir RFC-4180 - Format commun et type MIME pour les fichiers CSV (Comma-Separated Values) sur le site Web de l'IETF.

Voici un exemple des informations fournies dans un rapport d'achèvement de tâche qui inclut uniquement les fichiers ayant échoué.

```
myRestrictedFile,failed,S3AccessDenied
dir1/myLargeFile,failed,FileSizeTooLarge
dir2/anotherLargeFile,failed,FileSizeTooLarge
```

Pour plus d'informations sur les échecs de tâches et sur la manière de les résoudre, consultezRésolution des défaillances des tâches du référentiel de données.

Résolution des défaillances des tâches du référentiel de données

Vous pouvez activer la journalisation dans les CloudWatch journaux pour consigner les informations relatives aux défaillances survenues lors de l'importation ou de l'exportation de fichiers à l'aide de tâches du référentiel de données. Pour plus d'informations sur CloudWatch les journaux d'événements Logs, consultezJournaux d'événements du référentiel de données.

Lorsqu'une tâche de référentiel de données échoue, vous pouvez trouver le nombre de fichiers qu'Amazon FSx n'a pas pu traiter dans la section Fichiers n'ayant pas pu être exportés sur la page d'état des tâches de la console. Vous pouvez également utiliser la CLI ou l'API et afficher les `Status: FailedCount` propriétés de la tâche. Pour plus d'informations sur l'accès à ces informations, consultezAccès aux tâches du référentiel de données.

Pour les tâches liées au référentiel de données, Amazon fournit FSx également, en option, des informations sur les fichiers et répertoires spécifiques qui ont échoué dans un rapport d'achèvement. Le rapport d'achèvement de la tâche contient le chemin du fichier ou du répertoire du système de Lustre fichiers défaillant, son état et la raison de l'échec. Pour de plus amples informations, veuillez consulter Utilisation des rapports d'achèvement des tâches.

Une tâche de référentiel de données peut échouer pour plusieurs raisons, notamment celles répertoriées ci-dessous.

Code d’erreur	Explication
`FileSizeTooLarge`	La taille d'objet maximale prise en charge par Amazon S3 est de 5 TiB.
`InternalError`	Une erreur s'est produite dans le système de FSx fichiers Amazon lors d'une tâche d'importation, d'exportation ou de publication. En général, ce code d'erreur signifie que le système de FSx fichiers Amazon sur lequel la tâche a échoué est dans un état d'échec du cycle de vie. Dans ce cas, les fichiers concernés risquent de ne pas être récupérab les en raison d'une perte de données. Sinon, vous pouvez utiliser les commandes de gestion hiérarchique du stockage (HSM) pour exporter les fichiers et les répertoires vers le référenti el de données sur S3. Pour de plus amples informations, veuillez consulter Exportation de fichiers à l'aide de commandes HSM.
`OperationNotPermitted`	Amazon FSxn'a pas pu publier le fichier car il n'a pas été exporté vers un compartiment S3 lié. Vous devez utiliser des tâches d'exporta tion ou de référentiel de données automatiques pour vous assurer que vos fichiers sont d'abord exportés vers votre compartiment Amazon S3 associé.

Code d’erreur	Explication
`PathSizeTooLong`	Le chemin d'exportation est trop long. La longueur maximale de la clé d'objet prise en charge par S3 est de 1 024 caractères.
`ResourceBusy`	Amazon FSxn'a pas pu exporter ou publier le fichier car un autre client du système de fichiers y accédait. Vous pouvez réessayer une DataRepositoryTask fois que votre flux de travail aura terminé d'écrire dans le fichier.

Code d’erreur	Explication
`S3AccessDenied`	L'accès à Amazon S3 a été refusé pour une tâche d'exportation ou d'importation d'un référentiel de données. Pour les tâches d'exportation, le système de FSx fichiers Amazon doit être autorisé à effectuer l'`S3:PutObject` opération d'exportation vers un référentiel de données lié sur S3. Cette autorisation est accordée dans le rôle `AWSServiceRoleForFSxS3Access_` *`fs-0123456789abcdef0`* lié au service. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon FSx. Pour les tâches d'exportation, étant donné que la tâche d'exportation nécessite que les données circulent en dehors du VPC d'un système de fichiers, cette erreur peut se produire si le référentiel cible dispose d'une politique de compartiment contenant l'une des clés de condition globales `aws:SourceVpc` ou `aws:SourceVpce` IAM. Pour les tâches d'importation, le système de FSx fichiers Amazon doit être autorisé à effectuer les `S3:GetObject` opérations `S3:HeadObject` et à importer à partir d'un référentiel de données lié sur S3. Pour les tâches d'importation, si votre compartiment S3 utilise le chiffrement côté serveur avec des clés gérées par le client stockées dans AWS Key Management Service (SSE-KMS), vous devez suivre les configurations de politique contenues dans. Utilisation

Code d’erreur	Explication
	de compartiments Amazon S3 chiffrés côté serveur Si votre compartiment S3 contient des objets chargés depuis un compte de compartiment S3 différent de Compte AWS celui associé à votre système de fichiers, vous pouvez vous assurer que les tâches de votre référentiel de données peuvent modifier les métadonnées S3 ou remplacer les objets S3, quel que soit le compte qui les a chargés. Nous vous recommandons d'activer la fonctionnalité S3 Object Ownership pour votre compartiment S3. Cette fonctionnalité vous permet de vous approprier les nouveaux objets que d'autres Comptes AWS téléchargeront dans votre bucket, en forçant les chargements à fournir l'ACL `-/-acl bucket-owner-full-control` prédéfinie. Vous activez la propriété des objets S3 en choisissant l'option préférée du propriétaire du compartiment dans votre compartiment S3. Pour plus d'informations, consultez la section Contrôle de la propriété des objets chargés à l'aide de S3 Object Ownership dans le guide de l'utilisateur Amazon S3.
`S3Error`	Amazon FSx a rencontré une erreur liée au S3 qui ne l'était pas. `S3AccessDenied`
`S3FileDeleted`	Amazon n' FSx a pas pu exporter un fichier de liens physiques car le fichier source n'existe pas dans le référentiel de données.

Code d’erreur	Explication
`S3ObjectInUnsupportedTier`	Amazon FSx a importé avec succès un objet autre que des liens symboliques depuis une classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Ils `FileStatus` figureront `succeeded with warning` dans le rapport d'achèvement des tâches. L'avertissement indique que pour récupérer les données, vous devez d'abord restaurer l'objet S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, puis utiliser une `hsm_restore` commande pour importer l'objet.
`S3ObjectNotFound`	Amazon n' FSx a pas pu importer ou exporter le fichier car il n'existe pas dans le référentiel de données.
`S3ObjectPathNotPosixCompliant`	L'objet Amazon S3 existe mais ne peut pas être importé car il ne s'agit pas d'un objet compatible POSIX. Pour plus d'informations sur les métadonnées POSIX prises en charge, consultezSupport des métadonnées POSIX pour les référentiels de données.
`S3ObjectUpdateInProgressFromFileRename`	Amazon FSxn'a pas pu publier le fichier car l'exportation automatique traite le changement de nom du fichier. Le processus de renommage automatique des exportations doit être terminé avant que le fichier ne puisse être publié.

Code d’erreur	Explication
`S3SymlinkInUnsupportedTier`	Amazon n' FSx a pas pu importer un objet de lien symbolique car il appartient à une classe de stockage Amazon S3 qui n'est pas prise en charge, telle qu'une classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Ils `FileStatus` figureront `failed` dans le rapport d'achèvement des tâches.
`SourceObjectDeletedBeforeReleasing`	Amazon n' FSx a pas pu libérer le fichier depuis le système de fichiers car il a été supprimé du référentiel de données avant de pouvoir être publié.

Publication de fichiers

Les tâches du référentiel de données de publication libèrent les données des fichiers de votre système de fichiers FSx for Lustre afin de libérer de l'espace pour de nouveaux fichiers. La libération d'un fichier conserve la liste des fichiers et les métadonnées, mais supprime la copie locale du contenu de ce fichier. Si un utilisateur ou une application accède à un fichier publié, les données sont automatiquement et de manière transparente rechargées dans votre système de fichiers à partir de votre compartiment Amazon S3 associé.

> **Note**
>
> Les tâches du référentiel de données de publication ne sont pas disponibles sur FSx les systèmes de fichiers Lustre 2.10.

Les paramètres Chemins du système de fichiers à publier et Durée minimale depuis le dernier accès déterminent les fichiers qui seront publiés.

- Chemins du système de fichiers à publier : Spécifie le chemin à partir duquel les fichiers seront publiés.
- Durée minimale depuis le dernier accès : indique la durée, en jours, pendant laquelle tout fichier non consulté pendant cette durée doit être publié. La durée écoulée depuis le dernier accès à un

fichier est calculée en prenant la différence entre l'heure de création de la tâche de publication et le dernier accès à un fichier (valeur maximale de `atimemtime`, et`ctime`).

Les fichiers ne seront publiés le long du chemin du fichier que s'ils ont été exportés vers S3 et s'ils ont une durée depuis le dernier accès supérieure à la durée minimale depuis la valeur du dernier accès. Si vous indiquez une durée minimale de plusieurs `0` jours depuis le dernier accès, les fichiers seront publiés indépendamment de leur durée depuis le dernier accès.

> **Note**
>
> L'utilisation de caractères génériques pour inclure ou exclure des fichiers à publier n'est pas prise en charge.

Les tâches du référentiel de données de publication ne publieront que les données provenant de fichiers déjà exportés vers un référentiel de données S3 lié. Vous pouvez exporter des données vers S3 à l'aide de la fonctionnalité d'exportation automatique, d'une tâche de référentiel de données d'exportation ou de commandes HSM. Pour vérifier qu'un fichier a été exporté vers votre référentiel de données, vous pouvez exécuter la commande suivante. Une valeur de retour de `states: (0x00000009) exists archived` indique que le fichier a été correctement exporté.

```
sudo lfs hsm_state path/to/export/file
```

> **Note**
>
> Vous devez exécuter la commande HSM en tant qu'utilisateur root ou en utilisant`sudo`.

Pour publier des données de fichiers à intervalles réguliers, vous pouvez planifier une tâche de référentiel de données de publication récurrente à l'aide d'Amazon EventBridge Scheduler. Pour plus d'informations, consultez Getting started with EventBridge Scheduler dans le guide de l'utilisateur d'Amazon EventBridge Scheduler.

Rubriques

- Utilisation des tâches du référentiel de données pour publier des fichiers

Utilisation des tâches du référentiel de données pour publier des fichiers

Utilisez les procédures suivantes pour créer des tâches qui libèrent des fichiers du système de fichiers à l'aide de la FSx console Amazon et de la CLI. La libération d'un fichier conserve la liste des fichiers et les métadonnées, mais supprime la copie locale du contenu de ce fichier.

Pour publier des fichiers (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis choisissez votre système de Lustre fichiers.
3. Choisissez l'onglet Référentiel de données.
4. Dans le volet Associations de référentiels de données, choisissez l'association de référentiel de données pour laquelle vous souhaitez créer la tâche de publication.
5. Pour Actions, choisissez Créer une tâche de publication. Ce choix n'est disponible que si le système de fichiers est lié à un référentiel de données sur S3. La boîte de dialogue de tâches Créer un référentiel de données de version apparaît.
6. Dans Chemins du système de fichiers à publier, spécifiez jusqu'à 32 répertoires ou fichiers à libérer depuis votre système de FSx fichiers Amazon en fournissant les chemins d'accès à ces répertoires ou fichiers. Les chemins que vous fournissez doivent être relatifs au point de montage du système de fichiers. Par exemple, si le point de montage `/mnt/fsx/path1` est `/mnt/fsx` et reste un fichier du système de fichiers que vous souhaitez publier, le chemin à fournir est`path1`. Pour libérer tous les fichiers du système de fichiers, spécifiez une barre oblique (/) comme chemin.

   > **Note**
   >
   > Si le chemin que vous fournissez n'est pas valide, la tâche échoue.

7. Pour Durée minimale depuis le dernier accès, spécifiez la durée, en jours, de telle sorte que tout fichier non consulté pendant cette durée soit publié. L'heure du dernier accès est calculée à l'aide de la valeur maximale de `atime`, `mtime`, et`ctime`. Les fichiers dont la durée du dernier accès est supérieure à la durée minimale depuis le dernier accès (par rapport à l'heure de création de la tâche) seront publiés. Les fichiers dont la durée du dernier accès est inférieure à ce nombre de jours ne seront pas publiés, même s'ils figurent dans le champ Chemins du système de fichiers vers la publication. Indiquez une durée de plusieurs `0` jours pour publier les fichiers indépendamment de la durée écoulée depuis le dernier accès.

8. (Facultatif) Sous Rapport d'achèvement, choisissez Activer pour générer un rapport d'achèvement des tâches fournissant des détails sur les fichiers correspondant à l'étendue spécifiée dans Étendue du rapport. Pour spécifier un emplacement où Amazon doit FSx envoyer le rapport, entrez un chemin relatif dans le référentiel de données S3 lié au système de fichiers pour le chemin du rapport.
9. Choisissez Créer une tâche de référentiel de données.

   Une notification en haut de la page Systèmes de fichiers indique que la tâche que vous venez de créer est en cours.

Pour afficher le statut et les détails des tâches, dans l'onglet Référentiel de données, faites défiler l'écran jusqu'à Tâches du référentiel de données. L'ordre de tri par défaut indique la tâche la plus récente en haut de la liste.

Pour afficher un résumé des tâches à partir de cette page, choisissez l'ID de tâche pour la tâche que vous venez de créer.

Pour publier des fichiers (CLI)

- Utilisez la commande `create-data-repository-task`CLI pour créer une tâche qui libère des fichiers sur votre système de fichiers FSx for Lustre. L'opération d'API correspondante est `CreateDataRepositoryTask`.

  Définissez les paramètres suivants :

  - `--file-system-id`Défini sur l'ID du système de fichiers à partir duquel vous publiez des fichiers.
  - Définissez `--paths` les chemins du système de fichiers à partir duquel les données seront publiées. Si un répertoire est spécifié, les fichiers qu'il contient sont publiés. Si un chemin de fichier est spécifié, seul ce fichier est publié. Pour libérer tous les fichiers du système de fichiers qui ont été exportés vers un compartiment S3 lié, spécifiez une barre oblique (/) pour le chemin.
  - Définissez `--type` sur `RELEASE_DATA_FROM_FILESYSTEM`.
  - Définissez les `--release-configuration DurationSinceLastAccess` options comme suit :
    - `Unit` – Défini sur `DAYS`.

- `Value`— Spécifiez un entier qui représente la durée, en jours, de telle sorte que tout fichier non consulté pendant cette durée doit être publié. Les fichiers consultés pendant une période inférieure à ce nombre de jours ne seront pas publiés, même s'ils figurent dans le `--paths` paramètre. Indiquez une durée de plusieurs `0` jours pour publier les fichiers indépendamment de la durée écoulée depuis le dernier accès.

Cet exemple de commande indique que les fichiers exportés vers un compartiment S3 lié et répondant aux `--release-configuration` critères seront libérés des répertoires dans les chemins spécifiés.

```
$ aws fsx create-data-repository-task \
    --file-system-id fs-0123456789abcdef0 \
    --type RELEASE_DATA_FROM_FILESYSTEM \
    --paths path1,path2/file1 \
    --release-configuration '{"DurationSinceLastAccess":
{"Unit":"DAYS","Value":10}}' \
    --report Enabled=false
```

Après avoir créé avec succès la tâche du référentiel de données, Amazon FSx renvoie la description de la tâche au format JSON.

Après avoir créé la tâche de publication des fichiers, vous pouvez vérifier le statut de la tâche. Pour plus d'informations sur l'affichage des tâches du référentiel de données, consultezAccès aux tâches du référentiel de données.

Utilisation d'Amazon FSx avec vos données sur site

Vous pouvez utiliser Lustre FSx pour traiter vos données sur site avec des instances de calcul dans le cloud. FSx for Lustre prend en charge l'accès Direct Connect et le VPN, ce qui vous permet de monter vos systèmes de fichiers à partir de clients locaux.

À utiliser FSx pour Lustre avec vos données sur site

1. Créez un système de fichiers. Pour plus d'informations, reportez-vous Étape 1 : Créez votre système de fichiers FSx for Lustre à l'exercice de mise en route.

2. Montez le système de fichiers à partir de clients locaux. Pour de plus amples informations, veuillez consulter Montage de systèmes de FSx fichiers Amazon sur site ou depuis un Amazon VPC pair.
3. Copiez les données que vous souhaitez traiter dans votre système de fichiers FSx for Lustre.
4. Exécutez votre charge de travail gourmande en ressources informatiques sur des instances Amazon EC2 dans le cloud qui montent votre système de fichiers.
5. Lorsque vous avez terminé, copiez les résultats finaux de votre système de fichiers vers votre emplacement de données local et supprimez votre système de fichiers FSx for Lustre.

Journaux d'événements du référentiel de données

Vous pouvez activer la journalisation dans CloudWatch les journaux pour consigner les informations relatives aux défaillances survenues lors de l'importation ou de l'exportation de fichiers à l'aide de tâches d'importation, d'exportation, de référentiel de données et d'événements de restauration. Pour de plus amples informations, veuillez consulter Journalisation avec Amazon CloudWatch Logs.

> **Note**
>
> Lorsqu'une tâche du référentiel de données échoue, Amazon écrit FSx également les informations relatives à l'échec dans le rapport d'achèvement de la tâche. Pour plus d'informations sur les informations relatives aux défaillances figurant dans les rapports d'achèvement, consultezRésolution des défaillances des tâches du référentiel de données.

Rubriques

- Importer des événements
- Exporter des événements
- Événements de restauration HSM

Importer des événements

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Échec de la liste des objets	ERROR	Impossible de répertorier les objets S3 dans le compartiment S3 *bucket_name* avec le préfixe*prefix*.	Amazon FSx n'a pas réussi à répertorier les objets S3 dans le compartiment S3. Cela peut se produire si la politique du compartiment S3 ne fournit pas d'autorisations suffisantes à Amazon FSx.	N/A
Classe de stockage S3 non prise en charge	WARN	Impossible d'importer un objet S3 avec une clé *key_value* dans le compartiment S3 *bucket_name* en raison d'un objet S3 situé dans un niveau *S3_tier_n*	Amazon n'FSx a pas pu importer un objet S3 car il appartient à une classe de stockage Amazon S3 qui n'est pas prise en charge, telle que S3 Glacier Flexible Retrieval ou S3	`S3ObjectInUnsupportedTier`

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
		ame non pris en charge.	Glacier Deep Archive.	
Classe de stockage de liens symboliques non prise en charge	ERROR	Impossible d'importer un objet S3 avec une clé *key_value* dans le compartiment S3 *bucket_name* en raison d'un objet de lien symbolique S3 dans un niveau non pris en charge. *S3_tier_name*	Amazon n'FSx a pas pu importer un objet de lien symbolique car il appartient à une classe de stockage Amazon S3 qui n'est pas prise en charge, telle que S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.	`S3SymlinkInUnsupportedTier`

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Accès S3 refusé	ERROR	Impossible d'importer l'objet S3 avec la clé *key_value* dans le compartiment S3 *bucket_name* car l'accès à l'objet S3 a été refusé.	L'accès à Amazon S3 a été refusé pour une tâche d'importation d'exportation d'un référentiel de données. Pour les tâches d'importation, le système de FSx fichiers Amazon doit être autorisé à effectuer les `s3:GetObject` opérations `s3:HeadObject` et à importer à partir d'un référentiel de données lié sur S3. Pour les tâches d'importation, si votre compartiment S3 utilise le chiffrement	`S3AccessDenied`

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
			côté serveur avec des clés gérées par le client stockées dans AWS Key Management Service (SSE-KMS), vous devez suivre les configurations de politique contenues dans. Utilisation de compartiments Amazon S3 chiffrés côté serveur	

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Supprimer l'accès refusé	ERROR	Impossible de supprimer le fichier local pour l'objet S3 dont la clé se *key_value* trouve dans le compartiment S3 *bucket_name* car l'accès à l'objet S3 a été refusé.	L'importation automatique s'est vu refuser l'accès à un objet S3.	N/A

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Objet non compatible POSIX	ERROR	Impossible d'importer un objet S3 avec une clé *key_value* dans le compartiment S3 *bucket_name* car l'objet S3 n'est pas conforme à POSIX.	L'objet Amazon S3 existe mais ne peut pas être importé car il ne s'agit pas d'un objet compatible POSIX. Pour plus d'informations sur les métadonnées POSIX prises en charge, consultez Support des métadonnées POSIX pour les référentiels de données.	`S3ObjectPathNotPosixCompliant`

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Incompatibilité du type d'objet	ERROR	Impossible d'importer un objet S3 avec une clé *key_value* dans le compartiment S3 *bucket_name* car un objet S3 portant le même nom a déjà été importé dans le système de fichiers.	L'objet S3 importé est d'un type (fichier ou répertoire) différent de celui d'un objet existant portant le même nom dans le système de fichiers.	`S3ObjectTypeMismatch`
Echec de la mise à jour des métadonnées	ERROR	Impossible de mettre à jour les métadonnées du répertoire local en raison d'une erreur interne.	Les métadonnées du répertoire n'ont pas pu être importées en raison d'une erreur interne.	N/A

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Objet S3 introuvable	ERROR	Impossible d'importer l'objet S3 avec la clé *key_value* car il n'a pas été trouvé dans le compartiment S3*bucket_name* .	Amazon n' FSx a pas pu importer les métadonnées du fichier car l'objet correspondant n'existe pas dans le référentiel de données.	`S3FileDeleted`
Compartiment S3 introuvable	ERROR	Impossible d'importer un objet S3 avec une clé *key_value* dans le compartiment S3 *bucket_name* car le compartiment n'existe pas.	Amazon FSx ne peut pas importer automatiquement un objet S3 dans le système de fichiers car le compartiment S3 n'existe plus.	N/A

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Compartiment S3 introuvable	ERROR	Impossible de supprimer le fichier local pour l'objet S3 dont la clé *key_value* se trouve dans le compartiment S3 *bucket_name* car le compartiment n'existe pas.	Amazon FSx ne peut pas supprimer un fichier lié à un objet S3 dans le système de fichiers car le compartiment S3 n'existe plus.	N/A
Echec de création de répertoire	ERROR	Impossible de créer le répertoire local en raison d'une erreur interne.	Amazon FSx n'a pas réussi à importer automatiquement une création de répertoire dans le système de fichiers en raison d'une erreur interne.	N/A

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Espace disque plein	ERROR	Impossible d'importer un objet S3 avec une clé *key_value* dans le compartiment S3 *bucket_name* car le système de fichiers est plein.	Le système de fichiers a manqué d'espace disque sur le ou les serveurs de métadonnées lors de la création du fichier ou du répertoire.	N/A

Exporter des événements

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Accès refusé	ERROR	Impossible d'exporter le fichier car l'accès à l'objet S3 dont la clé se trouve *key_value* dans le compartiment S3 a été refusé*bucket_name* .	L'accès à Amazon S3 a été refusé pour une tâche d'exportation de référentiel de données. Pour les tâches d'exportation, le système de FSx fichiers Amazon	`S3AccessDenied`

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
			doit être autorisé à effectuer l'`s3:PutObject` opération d'exportation vers un référentiel de données lié sur S3. Cette autorisation est accordée dans le rôle `AWSServiceRoleForFSxS3Access_` *`fs-0123456789abcdef0`* lié au service. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon FSx. Étant donné que la tâche d'exportation nécessite que les données circulent en dehors du VPC d'un système de	

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
			fichiers, cette erreur peut se produire si le référentiel cible dispose d'une politique de compartiment contenant l'une des clés de condition globales `aws:SourceVpc` ou `aws:SourceVpce` IAM. Si votre compartiment S3 contient des objets chargés depuis un compte de compartiment S3 différent de Compte AWS celui associé à votre système de fichiers, vous pouvez vous assurer que les tâches de votre référentiel de données	

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
			peuvent modifier les métadonnées S3 ou remplacer les objets S3, quel que soit le compte qui les a chargés. Nous vous recommandons d'activer la fonctionnalité S3 Object Ownership pour votre compartiment S3. Cette fonctionnalité vous permet de vous approprier les nouveaux objets que d'autres Comptes AWS téléchargeront dans votre bucket, en forçant les chargements à fournir l'ACL `--acl bucket-owner-full-control` prédéfinie. Vous activez la propriété	

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
			des objets S3 en choisissant l'option préférée du propriétaire du compartiment dans votre compartiment S3. Pour plus d'informations, consultez la section Contrôle de la propriété des objets chargés à l'aide de S3 Object Ownership dans le guide de l'utilisateur Amazon S3.	
Le chemin d'exportation est trop long	ERROR	Impossible d'exporter le fichier car la taille du chemin du fichier local dépasse la longueur maximale de clé d'objet prise en charge par S3.	Le chemin d'exportation est trop long. La longueur maximale de la clé d'objet prise en charge par S3 est de 1 024 caractères.	`PathSizeTooLong`

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Fichier trop volumineux	ERROR	Impossible d'exporter le fichier car sa taille dépasse la taille maximale des objets S3 pris en charge.	La taille d'objet maximale prise en charge par Amazon S3 est de 5 TiB.	`FileSizeTooLarge`
Clé KMS introuvable	ERROR	Impossible d'exporter le fichier pour l'objet S3 dont la clé *`key_value`* se trouve dans le compartiment S3 *`bucket_name`* car la clé KMS du compartiment est introuvable.	Amazon n' FSx a pas pu exporter le AWS KMS key fichier car il est introuvable. Assurez-vous d'utiliser une clé identique à Région AWS celle du compartiment S3. Pour plus d'informations sur la création de clés KMS, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.	`N/A`

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Ressource occupée	ERROR	Impossible d'exporter le fichier car il est utilisé par un autre processus.	Amazon n' FSx a pas pu exporter le fichier car il était modifié par un autre client sur le système de fichiers. Vous pouvez réessayer la tâche une fois que votre flux de travail a terminé d'écrire dans le fichier.	`ResourceBusy`
Dossier publié	WARN	Exportation ignorée : le fichier local est à l'état publié et aucun objet S3 lié avec une clé n'*`key_value`* a été trouvé dans le compartiment*`bucket_name`* .	Amazon n' FSx a pas pu exporter le fichier car il était à l'état publié sur le système de fichiers.	N/A

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Incompatibilité du chemin du référentiel de données	WARN	Exportation ignorée : le fichier local n'appartient pas au chemin du système de fichiers lié à un référentiel de données.	Amazon n' FSx a pas pu exporter car l'objet n'appartient pas à un chemin de système de fichiers lié à un référentiel de données.	N/A
Internal failure (Échec interne)	ERROR	L'exportation automatique a rencontré une erreur interne lors de l'exportation d'un objet du système de fichiers	L'exportation a échoué en raison d'une erreur interne (au niveau de l'exportation automatique ou du lustre).	N/A
Échec du téléchargement du rapport d'achèvement	ERROR	Impossible de télécharger le rapport d'achèvement des tâches du référentiel de données dans *bucket_name*	Amazon n' FSx a pas pu télécharger le rapport d'achèvement.	N/A

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde	Code d'erreur dans le rapport d'achèvement
Échec de validation du rapport d'achèvement	ERROR	Impossible de télécharger le rapport d'achèvement des tâches du référentiel de données dans le compartiment *bucket_name* car le chemin du rapport d'achèvement *report_path* n'appartient pas à un référentiel de données associé à ce système de fichiers	Amazon n' FSx a pas pu télécharger le rapport d'achèvement car le chemin S3 fourni par le client n'appartient pas à un référentiel de données lié.	N/A

Événements de restauration HSM

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde
Accès refusé	ERROR	Impossible de restaurer le fichier car l'accès à l'objet S3 *object_name* dans le compartim	L'accès a été refusé à Amazon S3 lors d'une tentative de restauration d'un

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde
		ent S3 a été refusé*bucket_name* .	fichier à l'aide de commandes HSM. Le système de fichiers doit être autorisé à effectuer les `s3:GetObject` opérations `s3:HeadObject` et à restaurer à partir du référentiel de données lié sur S3.
Classe de stockage S3 non prise en charge	WARN	Impossible de restaurer le fichier car l'objet S3 du compartiment *object_name* se *bucket_name* trouvait dans un emplacement non pris en charge*S3_storage_class_name* .	Amazon n' FSx a pas pu restaurer le fichier car l'objet S3 correspondant se trouve dans une classe de stockage S3 non prise en charge, telle que S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Vous devez d'abord restaurer l'objet à partir de la classe de stockage Glacier avant de l'utiliser`hsm_restore` .

Error type (Type d'erreur)	Niveau de journalisation	Message de journal	Cause profonde
Objet S3 introuvable	ERROR	Impossible de restaurer le fichier car aucun objet S3 avec clé n'*key_value* a été trouvé dans le compartiment S3*bucket_name* .	Amazon n' FSx a pas pu restaurer le fichier car l'objet S3 correspondant n'existe pas dans le référentiel de données.
Compartiment S3 introuvable	ERROR	Impossible de restaurer le fichier car le compartiment S3 *bucket_name* n'existe pas.	Amazon FSx ne peut pas restaurer le fichier car le compartiment S3 lié n'existe plus.
Espace disque plein	ERROR	Impossible de restaurer le fichier car il n'y avait pas d'espace de stockage disponible sur le système de fichiers.	Le système de fichiers a manqué d'espace de stockage disponible lors de la tentative de restauration des données du fichier depuis S3. Envisagez d'augmenter la capacité de stockage du système de fichiers ou de libérer des fichiers pour libérer de l'espace.

Utilisation d'anciens types de déploiement

Cette section s'applique aux systèmes de fichiers dotés du type de déploiement Scratch 1, ainsi qu'aux systèmes de fichiers dotés `Scratch 2` ou aux types de `Persistent 1` déploiement n'utilisant pas d'associations de référentiels de données. Notez que l'exportation automatique et la prise en charge de plusieurs référentiels de données ne sont pas disponibles sur FSx les systèmes de fichiers Lustre qui n'utilisent pas d'associations de référentiels de données.

Rubriques

- Liez votre système de fichiers à un compartiment Amazon S3
- Importez automatiquement des mises à jour depuis votre compartiment S3

Liez votre système de fichiers à un compartiment Amazon S3

Lorsque vous créez un système de fichiers Amazon FSx for Lustre, vous pouvez le lier à un référentiel de données durable dans Amazon S3. Avant de créer votre système de fichiers, assurez-vous d'avoir déjà créé le compartiment Amazon S3 auquel vous créez le lien. Dans l'assistant de création de système de fichiers, vous définissez les propriétés de configuration du référentiel de données suivantes dans le volet optionnel Import/Export du référentiel de données.

- Choisissez comment Amazon FSx met à jour votre liste de fichiers et de répertoires lorsque vous ajoutez ou modifiez des objets dans votre compartiment S3 après la création du système de fichiers. Pour de plus amples informations, veuillez consulter Importez automatiquement des mises à jour depuis votre compartiment S3.
- Compartiment d'importation : entrez le nom du compartiment S3 que vous utilisez pour le référentiel lié.
- Préfixe d'importation : entrez un préfixe d'importation facultatif si vous souhaitez importer uniquement certaines listes de fichiers et de répertoires contenant des données de votre compartiment S3 dans votre système de fichiers. Le préfixe d'importation définit l'endroit d'où vous souhaitez importer les données dans votre compartiment S3.
- Préfixe d'exportation : définit l'endroit où Amazon FSx exporte le contenu de votre système de fichiers vers votre compartiment S3 lié.

Vous pouvez avoir un mappage 1:1 dans lequel Amazon FSx exporte les données de votre système de fichiers FSx for Lustre vers les mêmes répertoires du compartiment S3 d'où elles ont été

importées. Pour obtenir un mappage 1:1, spécifiez un chemin d'exportation vers le compartiment S3 sans aucun préfixe lors de la création de votre système de fichiers.

- Lorsque vous créez un système de fichiers à l'aide de la console, choisissez l'option Exporter le préfixe > Un préfixe que vous spécifiez et laissez le champ du préfixe vide.
- Lorsque vous créez un système de fichiers à l'aide de la AWS CLI ou de l'API, spécifiez le chemin d'exportation comme nom du compartiment S3 sans aucun préfixe supplémentaire, par exemple,`ExportPath=s3://amzn-s3-demo-bucket/`.

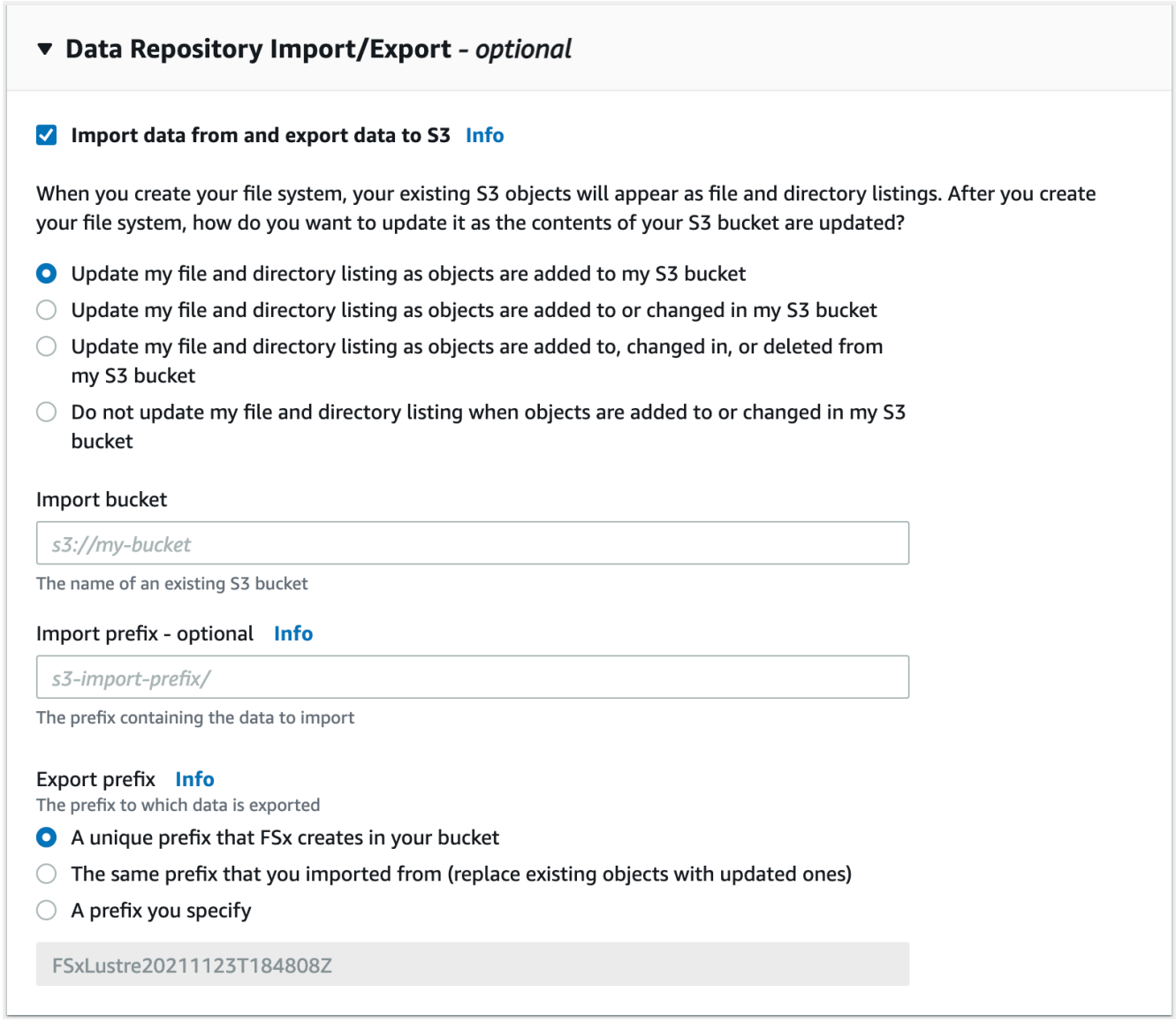
Grâce à cette méthode, vous pouvez inclure un préfixe d'importation lorsque vous spécifiez le chemin d'importation, et cela n'a aucune incidence sur le mappage 1:1 pour les exportations.

Création de systèmes de fichiers liés à un compartiment S3

Les procédures suivantes vous guident dans le processus de création d'un système de FSx fichiers Amazon lié à un compartiment S3 à l'aide de la console de AWS gestion et de l'interface de ligne de AWS commande (AWS CLI).

Console

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord, choisissez Créer un système de fichiers.
3. Pour le type de système de fichiers, choisissez FSx Lustre, puis Next.
4. Fournissez les informations requises pour les sections Détails du système de fichiers et Réseau et sécurité. Pour de plus amples informations, veuillez consulter Étape 1 : Créez votre système de fichiers FSx for Lustre.
5. Vous utilisez le panneau d'importation/exportation du référentiel de données pour configurer un référentiel de données lié dans Amazon S3. Sélectionnez Importer des données depuis et exporter des données vers S3 pour développer la section Import/Export du référentiel de données et configurer les paramètres du référentiel de données.



6. Choisissez comment Amazon FSx met à jour votre liste de fichiers et de répertoires lorsque vous ajoutez ou modifiez des objets dans votre compartiment S3. Lorsque vous créez votre système de fichiers, vos objets S3 existants apparaissent sous forme de listes de fichiers et de répertoires.

   - Mettre à jour la liste de mes fichiers et répertoires au fur et à mesure que des objets sont ajoutés à mon compartiment S3 : (par défaut) Amazon met FSx automatiquement à jour les listes de fichiers et de répertoires de tous les nouveaux objets ajoutés au compartiment S3 lié qui n'existent pas actuellement dans le système de FSx fichiers. Amazon FSx ne met pas à jour les listes d'objets qui ont changé dans le compartiment S3. Amazon FSx ne supprime pas les listes d'objets supprimés dans le compartiment S3.

> **Note**
>
> Le paramètre de préférences d'importation par défaut pour l'importation de données depuis un compartiment S3 lié à l'aide de la CLI et de l'API est`NONE`. Le paramètre des préférences d'importation par défaut lors de l'utilisation de la console est mis à jour à Lustre mesure que de nouveaux objets sont ajoutés au compartiment S3.

- Mettre à jour ma liste de fichiers et de répertoires au fur et à mesure que des objets sont ajoutés ou modifiés dans mon compartiment S3 : Amazon met FSx automatiquement à jour les listes de fichiers et de répertoires de tous les nouveaux objets ajoutés au compartiment S3 et de tous les objets existants modifiés dans le compartiment S3 une fois que vous avez choisi cette option. Amazon FSx ne supprime pas les listes d'objets supprimés dans le compartiment S3.
- Mettre à jour ma liste de fichiers et de répertoires au fur et à mesure que des objets sont ajoutés, modifiés ou supprimés de mon compartiment S3 : Amazon met FSx automatiquement à jour les listes de fichiers et de répertoires de tous les nouveaux objets ajoutés au compartiment S3, de tous les objets existants modifiés dans le compartiment S3 et de tous les objets existants supprimés dans le compartiment S3 une fois que vous avez sélectionné cette option.
- Ne mettez pas à jour mon fichier et ne listez pas directement les objets ajoutés, modifiés ou supprimés de mon compartiment S3. Amazon FSx ne met à jour les listes de fichiers et de répertoires à partir du compartiment S3 lié que lorsque le système de fichiers est créé. FSx ne met pas à jour les listes de fichiers et de répertoires pour les objets nouveaux, modifiés ou supprimés après avoir sélectionné cette option.

7. Entrez un préfixe d'importation facultatif si vous souhaitez importer uniquement certaines listes de fichiers et de répertoires contenant des données de votre compartiment S3 dans votre système de fichiers. Le préfixe d'importation définit l'endroit d'où vous souhaitez importer les données dans votre compartiment S3. Pour de plus amples informations, veuillez consulter Importez automatiquement des mises à jour depuis votre compartiment S3.
8. Choisissez l'une des options de préfixe d'exportation disponibles :

   - Un préfixe unique FSx créé par Amazon dans votre compartiment : choisissez cette option pour exporter des objets nouveaux et modifiés à l'aide d'un préfixe généré par FSx for Lustre. Le préfixe ressemble à ce qui suit :`/FSxLustre`*`file-`*

system-creation- timestamp. L'horodatage est au format UTC, par exemple FSxLustre20181105T222312Z.

- Le même préfixe que celui à partir duquel vous avez importé (remplacez les objets existants par des objets mis à jour) : choisissez cette option pour remplacer les objets existants par des objets mis à jour.
- Un préfixe que vous spécifiez : choisissez cette option pour conserver les données importées et pour exporter les objets nouveaux et modifiés à l'aide d'un préfixe que vous spécifiez. Pour obtenir un mappage 1:1 lors de l'exportation de données vers votre compartiment S3, choisissez cette option et laissez le champ de préfixe vide. FSx exportera les données vers les mêmes répertoires depuis lesquels elles ont été importées.

9. (Facultatif) Définissez les préférences de maintenance ou utilisez les paramètres par défaut du système.
10. Choisissez Next, puis passez en revue les paramètres du système de fichiers. Apportez les modifications nécessaires.
11. Choisissez Create file system (Créer un système de fichiers).

AWS CLI

L'exemple suivant crée un système de FSx fichiers Amazon lié auamzn-s3-demo-bucket, avec une préférence d'importation qui importe tous les fichiers nouveaux, modifiés ou supprimés dans le référentiel de données lié une fois le système de fichiers créé.

> **Note**
>
> Le paramètre de préférences d'importation par défaut pour l'importation de données depuis un compartiment S3 lié à l'aide de la CLI et de l'API estNONE, ce qui est différent du comportement par défaut lors de l'utilisation de la console.

Pour créer un système de fichiers FSx pour Lustre, utilisez la commande Amazon FSx CLI create-file-system, comme indiqué ci-dessous. L'opération d'API correspondante est CreateFileSystem.

```
$ aws fsx create-file-system \
--client-request-token CRT1234 \
--file-system-type LUSTRE \
--file-system-type-version 2.10 \
```

```
--lustre-configuration
AutoImportPolicy=NEW_CHANGED_DELETED,DeploymentType=SCRATCH_1,ImportPath=s
3://amzn-s3-demo-bucket/,ExportPath=s3://amzn-s3-demo-bucket/export,
PerUnitStorageThroughput=50 \
--storage-capacity 2400 \
--subnet-ids subnet-123456 \
--tags Key=Name,Value=Lustre-TEST-1 \
--region us-east-2
```

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

```
{
    "FileSystems": [
        {
            "OwnerId": "owner-id-string",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.10",
            "Lifecycle": "CREATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_1",
                "DataRepositoryConfiguration": {
                    "AutoImportPolicy": "NEW_CHANGED_DELETED",
                    "Lifecycle": "UPDATING",
```

```
                    "ImportPath": "s3://amzn-s3-demo-bucket/",
                    "ExportPath": "s3://amzn-s3-demo-bucket/export",
                    "ImportedFileChunkSize": 1024
                },
                "PerUnitStorageThroughput": 50
            }
        }
    ]
}
```

Afficher le chemin d'exportation d'un système de fichiers

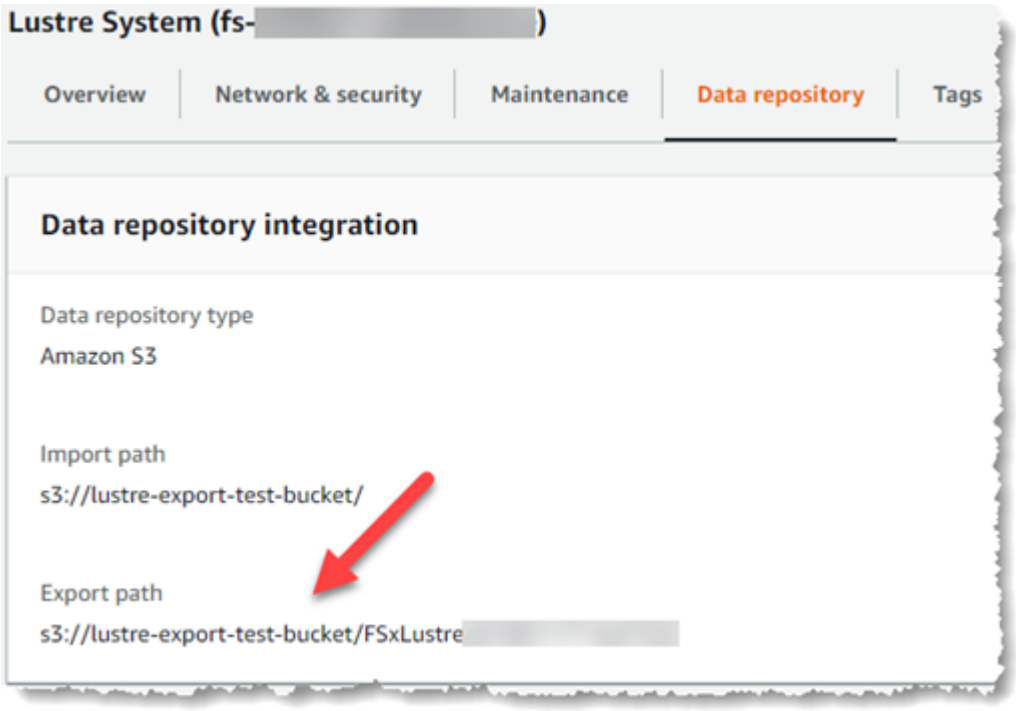
Vous pouvez consulter le chemin d'exportation d'un système de fichiers à l'aide de la console FSx for Lustre, de la AWS CLI et de l'API.

Console

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/
2. Choisissez le nom du système de fichiers ou l'ID du système de fichiers FSx pour le système de fichiers Lustre dont vous souhaitez afficher le chemin d'exportation.

   La page de détails du système de fichiers correspondant à ce système de fichiers apparaît.
3. Choisissez l'onglet Référentiel de données.

   Le panneau d'intégration du référentiel de données apparaît et indique les chemins d'importation et d'exportation.



CLI

Pour déterminer le chemin d'exportation de votre système de fichiers, utilisez la commande `describe-file-systems` AWS CLI.

```
aws fsx describe-file-systems
```

Recherchez la `ExportPath` propriété ci-dessous `LustreConfiguration` dans la réponse.

```
{
    "OwnerId": "111122223333",
    "CreationTime": 1563382847.014,
    "FileSystemId": "",
    "FileSystemType": "LUSTRE",
    "Lifecycle": "AVAILABLE",
    "StorageCapacity": 2400,
    "VpcId": "vpc-6296a00a",
    "SubnetIds": [
        "subnet-1111111"
    ],
    "NetworkInterfaceIds": [
        "eni-0c288d5b8cc06c82d",
        "eni-0f38b702442c6918c"
    ],
```

```
    "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
    "ResourceARN": "arn:aws:fsx:us-east-2:267731178466:file-system/
fs-0123456789abcdef0",
    "Tags": [
        {
          "Key": "Name",
          "Value": "Lustre System"
        }
    ],
 "LustreConfiguration": {
    "DeploymentType": "SCRATCH_1",
    "DataRepositoryConfiguration": {
    "AutoImportPolicy": " NEW_CHANGED_DELETED",
    "Lifecycle": "AVAILABLE",
    "ImportPath": "s3://amzn-s3-demo-bucket/",
    "ExportPath": "s3://amzn-s3-demo-bucket/FSxLustre20190717T164753Z",
    "ImportedFileChunkSize": 1024
    }
  },
  "PerUnitStorageThroughput": 50,
  "WeeklyMaintenanceStartTime": "6:09:30"
}
```

État du cycle de vie du référentiel de données

L'état du cycle de vie du référentiel de données fournit des informations d'état sur le référentiel de données lié du système de fichiers. Un référentiel de données peut avoir les états de cycle de vie suivants.

- Création : Amazon FSx crée la configuration du référentiel de données entre le système de fichiers et le référentiel de données lié. Le référentiel de données n'est pas disponible.
- Disponible : Le référentiel de données est prêt à être utilisé.
- Mise à jour : la configuration du référentiel de données fait actuellement l'objet d'une mise à jour initiée par le client, susceptible d'affecter sa disponibilité.
- Configuration incorrecte : Amazon FSx ne peut pas importer automatiquement les mises à jour depuis le compartiment S3 tant que la configuration du référentiel de données n'est pas corrigée. Pour de plus amples informations, veuillez consulter Résolution des problèmes liés à un compartiment S3 lié mal configuré.

Vous pouvez consulter l'état du cycle de vie d'un référentiel de données lié d'un système de fichiers à l'aide de la FSx console Amazon, de l'interface de ligne de AWS commande et de l' FSx API Amazon. Dans la FSx console Amazon, vous pouvez accéder à l'état du cycle de vie du référentiel de données dans le volet Intégration du référentiel de données de l'onglet Référentiel de données du système de fichiers. La `Lifecycle` propriété se trouve dans l'`DataRepositoryConfiguration`objet en réponse à une commande `describe-file-systems`CLI (l'action d'API équivalente est `DescribeFileSystems`).

Importez automatiquement des mises à jour depuis votre compartiment S3

Par défaut, lorsque vous créez un nouveau système de fichiers, Amazon FSx importe les métadonnées du fichier (nom, propriété, horodatage et autorisations) des objets du compartiment S3 lié lors de la création du système de fichiers. Vous pouvez configurer votre système de fichiers FSx for Lustre pour importer automatiquement les métadonnées des objets ajoutés, modifiés ou supprimés de votre compartiment S3 après la création du système de fichiers. FSx for Lustre met à jour la liste des fichiers et des répertoires d'un objet modifié après sa création de la même manière qu'il importe les métadonnées des fichiers lors de la création du système de fichiers. Lorsqu'Amazon FSx met à jour la liste des fichiers et des répertoires d'un objet modifié, si l'objet modifié dans le compartiment S3 ne contient plus ses métadonnées, Amazon FSx conserve les valeurs de métadonnées actuelles du fichier, plutôt que d'utiliser les autorisations par défaut.

> **Note**
>
> Les paramètres d'importation sont disponibles sur FSx les systèmes de fichiers Lustre créés après 15 h 00 HAE le 23 juillet 2020.

Vous pouvez définir les préférences d'importation lorsque vous créez un nouveau système de fichiers, et vous pouvez mettre à jour les paramètres des systèmes de fichiers existants à l'aide de la console de FSx gestion, de la AWS CLI et de l' AWS API. Lorsque vous créez votre système de fichiers, vos objets S3 existants apparaissent sous forme de listes de fichiers et de répertoires. Après avoir créé votre système de fichiers, comment souhaitez-vous le mettre à jour au fur et à mesure que le contenu de votre compartiment S3 est mis à jour ? Un système de fichiers peut avoir l'une des préférences d'importation suivantes :

> **Note**
>
> Le système de fichiers FSx for Lustre et son compartiment S3 associé doivent être situés dans la même AWS région pour pouvoir importer automatiquement les mises à jour.

- Mettre à jour la liste de mes fichiers et répertoires au fur et à mesure que des objets sont ajoutés à mon compartiment S3 : (par défaut) Amazon met FSx automatiquement à jour les listes de fichiers et de répertoires de tous les nouveaux objets ajoutés au compartiment S3 lié qui n'existent pas actuellement dans le système de FSx fichiers. Amazon FSx ne met pas à jour les listes d'objets qui ont changé dans le compartiment S3. Amazon FSx ne supprime pas les listes d'objets supprimés dans le compartiment S3.

  > **Note**
  >
  > Le paramètre de préférences d'importation par défaut pour l'importation de données depuis un compartiment S3 lié à l'aide de la CLI et de l'API est`NONE`. Le paramètre des préférences d'importation par défaut lors de l'utilisation de la console est mis à jour à Lustre mesure que de nouveaux objets sont ajoutés au compartiment S3.

- Mettre à jour ma liste de fichiers et de répertoires au fur et à mesure que des objets sont ajoutés ou modifiés dans mon compartiment S3 : Amazon met FSx automatiquement à jour les listes de fichiers et de répertoires de tous les nouveaux objets ajoutés au compartiment S3 et de tous les objets existants modifiés dans le compartiment S3 une fois que vous avez choisi cette option. Amazon FSx ne supprime pas les listes d'objets supprimés dans le compartiment S3.
- Mettre à jour ma liste de fichiers et de répertoires au fur et à mesure que des objets sont ajoutés, modifiés ou supprimés de mon compartiment S3 : Amazon met FSx automatiquement à jour les listes de fichiers et de répertoires de tous les nouveaux objets ajoutés au compartiment S3, de tous les objets existants modifiés dans le compartiment S3 et de tous les objets existants supprimés dans le compartiment S3 une fois que vous avez sélectionné cette option.
- Ne mettez pas à jour mon fichier et ne listez pas directement les objets ajoutés, modifiés ou supprimés de mon compartiment S3. Amazon FSx ne met à jour les listes de fichiers et de répertoires à partir du compartiment S3 lié que lorsque le système de fichiers est créé. FSx ne met pas à jour les listes de fichiers et de répertoires pour les objets nouveaux, modifiés ou supprimés après avoir sélectionné cette option.

Lorsque vous définissez les préférences d'importation pour mettre à jour les listes de fichiers et de répertoires de votre système de fichiers en fonction des modifications apportées au compartiment S3 lié, Amazon FSx crée une configuration de notification d'événement sur le compartiment S3 lié nomméFSx. Ne modifiez ni ne supprimez la configuration des notifications d'FSxévénements sur le compartiment S3. Cela empêche l'importation automatique de listes de fichiers et de répertoires nouvelles ou modifiées dans votre système de fichiers.

Lorsqu'Amazon FSx met à jour une liste de fichiers modifiée dans le compartiment S3 lié, il remplace le fichier local par la version mise à jour, même si le fichier est verrouillé en écriture. De même, lorsqu'Amazon FSx met à jour une liste de fichiers lorsque l'objet correspondant a été supprimé dans le compartiment S3 lié, il supprime le fichier local, même s'il est verrouillé en écriture.

Amazon FSx met tout en œuvre pour mettre à jour votre système de fichiers. Amazon FSx ne peut pas mettre à jour le système de fichiers avec des modifications dans les situations suivantes :

- Lorsque Amazon FSx n'est pas autorisé à ouvrir l'objet S3 modifié ou nouveau.
- Lorsque la configuration des notifications d'FSxévénements sur le compartiment S3 lié est supprimée ou modifiée.

L'une ou l'autre de ces conditions entraîne une mauvaise configuration de l'état du cycle de vie du référentiel de données. Pour de plus amples informations, veuillez consulter État du cycle de vie du référentiel de données.

Conditions préalables

Les conditions suivantes sont requises pour FSx qu'Amazon importe automatiquement des fichiers nouveaux, modifiés ou supprimés depuis le compartiment S3 lié :

- Le système de fichiers et son compartiment S3 lié doivent se trouver dans la même AWS région.
- L'état du cycle de vie du compartiment S3 n'est pas mal configuré. Pour de plus amples informations, veuillez consulter État du cycle de vie du référentiel de données.
- Votre compte doit disposer des autorisations requises pour configurer et recevoir des notifications d'événements sur le compartiment S3 lié.

Types de modifications de fichiers pris en charge

Amazon FSx prend en charge l'importation des modifications suivantes apportées aux fichiers et dossiers présents dans le compartiment S3 lié :

- Modifications apportées au contenu des fichiers
- Modifications apportées aux métadonnées d'un fichier ou d'un dossier
- Modifications apportées à la cible ou aux métadonnées du lien symbolique

Mettre à jour les préférences d'importation

Vous pouvez définir les préférences d'importation d'un système de fichiers lorsque vous créez un nouveau système de fichiers. Pour de plus amples informations, veuillez consulter Lier votre système de fichiers à un compartiment Amazon S3.

Vous pouvez également mettre à jour les préférences d'importation d'un système de fichiers après sa création à l'aide de la console de AWS gestion, de la AWS CLI et de l' FSx API Amazon, comme indiqué dans la procédure suivante.

Console

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord, sélectionnez Systèmes de fichiers.
3. Sélectionnez le système de fichiers que vous souhaitez gérer pour afficher les détails du système de fichiers.
4. Choisissez le référentiel de données pour afficher les paramètres du référentiel de données. Vous pouvez modifier les préférences d'importation si l'état du cycle de vie est DISPONIBLE ou MAL CONFIGURÉ. Pour de plus amples informations, veuillez consulter État du cycle de vie du référentiel de données.
5. Choisissez Actions, puis choisissez Mettre à jour les préférences d'importation pour afficher la boîte de dialogue Mettre à jour les préférences d'importation.
6. Sélectionnez le nouveau paramètre, puis choisissez Mettre à jour pour effectuer la modification.

CLI

Pour mettre à jour les préférences d'importation, utilisez la commande `update-file-system`CLI. L'opération d'API correspondante est `UpdateFileSystem`.

Une fois que vous avez correctement mis à jour le système de fichiers`AutoImportPolicy`, Amazon FSx renvoie la description du système de fichiers mis à jour au format JSON, comme indiqué ici :


```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "Lifecycle": "UPDATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "SCRATCH_1",
                "DataRepositoryConfiguration": {
                    "AutoImportPolicy": "NEW_CHANGED_DELETED",
                    "Lifecycle": "UPDATING",
                    "ImportPath": "s3://amzn-s3-demo-bucket/",
                    "ExportPath": "s3://amzn-s3-demo-bucket/export",
                    "ImportedFileChunkSize": 1024
                }
                "PerUnitStorageThroughput": 50,
                "WeeklyMaintenanceStartTime": "2:04:30"
            }
        }
    ]
```

```
}
```

Amazon FSx pour les performances de Lustre

Ce chapitre fournit des informations sur FSx les performances d'Amazon for Lustre, notamment des conseils et des recommandations importants pour optimiser les performances de votre système de fichiers.

Rubriques

- Présentation de
- Comment fonctionnent FSx les systèmes de fichiers Lustre
- Performances des métadonnées du système de fichiers
- Débit vers les instances clientes individuelles
- Disposition du stockage du système de fichiers
- Regrouper les données dans votre système de fichiers
- Surveillance des performances et de l'utilisation
- Caractéristiques de performance des classes de stockage SSD et HDD
- Caractéristiques de performance de la classe de stockage Intelligent-Tiering
- Conseils sur les performances

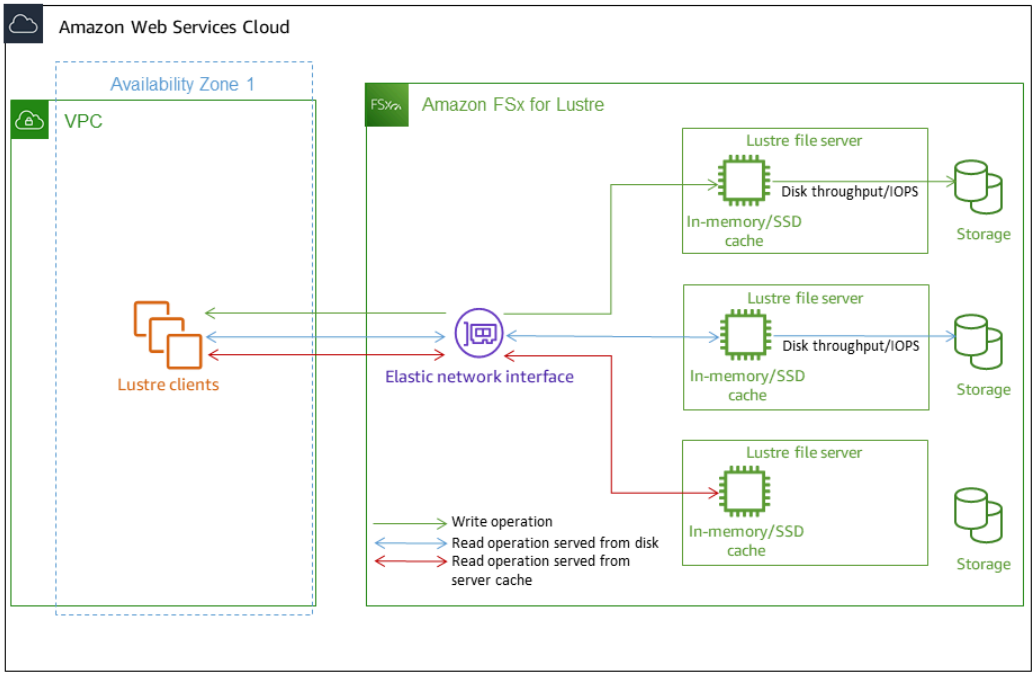
Présentation de

Amazon FSx for Lustre, basé sur Lustre le célèbre système de fichiers hautes performances, fournit des performances d'évolutivité qui augmentent de façon linéaire en fonction de la taille du système de fichiers. Lustreles systèmes de fichiers évoluent horizontalement sur plusieurs serveurs de fichiers et disques. Cette mise à l'échelle donne à chaque client un accès direct aux données stockées sur chaque disque afin de supprimer de nombreux goulots d'étranglement présents dans les systèmes de fichiers traditionnels. Amazon FSx for Lustre s'appuie sur une architecture Lustre évolutive pour garantir des niveaux de performance élevés à un grand nombre de clients.

Comment fonctionnent FSx les systèmes de fichiers Lustre

Chaque système de fichiers FSx pour Lustre comprend les serveurs de fichiers avec lesquels les clients communiquent et un ensemble de disques connectés à chaque serveur de fichiers qui

stockent vos données. Chaque serveur de fichiers utilise un cache rapide en mémoire pour améliorer les performances des données les plus fréquemment consultées. En fonction de la classe de stockage, votre serveur de fichiers peut être doté d'un cache de lecture SSD en option. Lorsqu'un client accède à des données stockées dans le cache en mémoire ou dans le cache SSD, le serveur de fichiers n'a pas besoin de les lire sur le disque, ce qui réduit le temps de latence et augmente le débit total que vous pouvez atteindre. Le schéma suivant illustre les chemins d'une opération d'écriture, d'une opération de lecture effectuée à partir du disque et d'une opération de lecture effectuée à partir d'un cache en mémoire ou d'un cache SSD.



Lorsque vous lisez des données stockées dans le cache en mémoire ou SSD du serveur de fichiers, les performances du système de fichiers sont déterminées par le débit du réseau. Lorsque vous écrivez des données dans votre système de fichiers ou que vous lisez des données qui ne sont pas stockées dans le cache en mémoire, les performances du système de fichiers sont déterminées par la baisse du débit du réseau et du débit du disque.

Pour en savoir plus sur le débit réseau, le débit du disque et les caractéristiques d'IOPS des classes de stockage SSD et HDD, consultez et. Caractéristiques de performance des classes de stockage SSD et HDD Caractéristiques de performance de la classe de stockage Intelligent-Tiering

Performances des métadonnées du système de fichiers

Les opérations d'E/S par seconde (IOPS) des métadonnées du système de fichiers déterminent le nombre de fichiers et de répertoires que vous pouvez créer, répertorier, lire et supprimer par seconde.

Les deux systèmes de fichiers persistants vous permettent de fournir des IOPS de métadonnées indépendamment de la capacité de stockage et de fournir une visibilité accrue sur le nombre et le type de métadonnées que les instances clientes IOPS génèrent sur votre système de fichiers. Avec les systèmes de fichiers SSD, les IOPS de métadonnées sont automatiquement provisionnées en fonction de la capacité de stockage que vous fournissez. Le mode automatique n'est pas pris en charge sur les systèmes de fichiers Intelligent-Tiering.

Dans le FSx cas des systèmes de fichiers Lustre Persistent 2, le nombre d'IOPS de métadonnées que vous fournissez et le type d'opération de métadonnées déterminent le taux d'opérations de métadonnées que votre système de fichiers peut prendre en charge. Le niveau d'IOPS de métadonnées que vous fournissez détermine le nombre d'IOPS provisionnés pour les disques de métadonnées de votre système de fichiers.

Type d'opération	Opérations que vous pouvez effectuer par seconde pour chaque IOPS de métadonnées provisionnée
Création, ouverture et fermeture de fichiers	2
Supprimer le fichier	1
Créer, renommer un répertoire	0.1
Supprimer le répertoire	0.2

Pour les systèmes de fichiers SSD, vous pouvez choisir de fournir des IOPS de métadonnées en mode automatique. En mode automatique, Amazon provisionne FSx automatiquement les IOPS de métadonnées en fonction de la capacité de stockage de votre système de fichiers, conformément au tableau ci-dessous :

Capacité de stockage du système de fichiers	IOPS de métadonnées incluses en mode automatique
1200 GiB	1 500
2400 GiB	3000
4800—9600 GiB	6 000
12 000 à 45 600 GiB	12 000
≥ 48 000 GiB	12 000 IOPS par 24 000 GiB

En mode provisionné par l'utilisateur, vous pouvez éventuellement choisir de spécifier le nombre d'IOPS de métadonnées à fournir. Les valeurs valides sont les suivantes :

- Pour les systèmes de fichiers SSD, les valeurs valides sont `1500`,`3000`,`6000`,`12000`, et des multiples `12000` allant jusqu'à un maximum de`192000`.
- Pour les systèmes de fichiers à hiérarchisation intelligente, les valeurs valides sont et. `6000` `12000`

Pour plus d'informations sur la configuration des IOPS de métadonnées, consultezGestion des performances des métadonnées. Notez que vous payez pour les IOPS de métadonnées mises en service au-delà du nombre d'IOPS de métadonnées par défaut pour votre système de fichiers.

Débit vers les instances clientes individuelles

Si vous créez un système de fichiers avec une capacité GBps de débit supérieure à 10 %, nous vous recommandons d'activer Elastic Fabric Adapter (EFA) afin d'optimiser le débit par instance client. Pour optimiser davantage le débit par instance client, les systèmes de fichiers compatibles EFA prennent également en charge le GPUDirect stockage pour les instances clientes basées sur le GPU NVIDIA compatibles EFA et ENA Express pour les instances clientes compatibles ENA Express.

Le débit que vous pouvez transmettre à une instance cliente unique dépend du type de système de fichiers que vous avez choisi et de l'interface réseau de votre instance cliente.

Type de système de fichiers	Interface réseau de l'instance client	Débit maximal par client, Gbit/s
Non compatible avec l'EFA	N'importe lequel	100 Gbit/s *
Compatible avec l'EFA	ENA	100 Gbit/s *
Compatible avec l'EFA	ENA Express	100 Gbit/s
Compatible avec l'EFA	EFA	700 Gbit/s
Compatible avec l'EFA	EFA avec GDS	1 200 Gbit/s

> **Note**
>
> * Le trafic entre une instance client individuelle et un individu FSx pour le serveur de stockage d'objets Lustre est limité à 5 Gbit/s. Reportez-vous au Adresses IP pour les systèmes de fichiers pour connaître le nombre de serveurs de stockage d'objets qui sous-tendent votre système de fichiers FSx for Lustre.

Disposition du stockage du système de fichiers

Toutes les données des fichiers sont Lustre stockées sur des volumes de stockage appelés cibles de stockage d'objets (OSTs). Toutes les métadonnées des fichiers (y compris les noms de fichiers, les horodatages, les autorisations, etc.) sont stockées sur des volumes de stockage appelés cibles de métadonnées (MDTs). Les systèmes de fichiers Amazon FSx for Lustre sont composés d'un ou plusieurs systèmes MDTs de fichiers OSTs. Amazon FSx for Lustre répartit les données de vos fichiers sur les OSTs éléments qui constituent votre système de fichiers afin d'équilibrer la capacité de stockage avec le débit et la charge IOPS.

Pour afficher l'utilisation du stockage par le MDT et OSTs les éléments constitutifs de votre système de fichiers, exécutez la commande suivante depuis un client sur lequel le système de fichiers est monté.

```
lfs df -h mount/path
```

La sortie de cette commande ressemble à ce qui suit.

Example

```
UUID                       bytes        Used   Available Use% Mounted on
mountname-MDT0000_UUID      68.7G        5.4M       68.7G   0% /fsx[MDT:0]
mountname-OST0000_UUID       1.1T        4.5M        1.1T   0% /fsx[OST:0]
mountname-OST0001_UUID       1.1T        4.5M        1.1T   0% /fsx[OST:1]

filesystem_summary:          2.2T        9.0M        2.2T   0% /fsx
```

Regrouper les données dans votre système de fichiers

Vous pouvez optimiser les performances de débit de votre système de fichiers grâce au découpage des fichiers. Amazon FSx for Lustre répartit automatiquement les fichiers OSTs afin de garantir que les données sont diffusées depuis tous les serveurs de stockage. Vous pouvez appliquer le même concept au niveau des fichiers en configurant la manière dont les fichiers sont répartis sur plusieurs OSTs.

Le striping signifie que les fichiers peuvent être divisés en plusieurs morceaux qui sont ensuite stockés sur différents. OSTs Lorsqu'un fichier est réparti entre plusieurs OSTs, les demandes de lecture ou d'écriture adressées au fichier sont réparties entre celles-ci OSTs, ce qui augmente le débit agrégé ou le nombre d'IOPS que vos applications peuvent traiter.

Voici les mises en page par défaut pour les systèmes de fichiers Amazon FSx for Lustre.

- Pour les systèmes de fichiers créés avant le 18 décembre 2020, la mise en page par défaut indique un nombre de bandes de 1. Cela signifie qu'à moins qu'une disposition différente ne soit spécifiée, chaque fichier créé dans Amazon FSx for Lustre à l'aide d'outils Linux standard est stocké sur un seul disque.
- Pour les systèmes de fichiers créés après le 18 décembre 2020, la mise en page par défaut est une mise en page progressive dans laquelle les fichiers de moins de 1 Go sont stockés sur une bande, tandis que les fichiers plus volumineux se voient attribuer un nombre de bandes de 5.
- Pour les systèmes de fichiers créés après le 25 août 2023, la mise en page par défaut est une mise en page progressive à 4 composants, comme expliqué dansMises en page de fichiers progressives.
- Pour tous les systèmes de fichiers, quelle que soit leur date de création, les fichiers importés depuis Amazon S3 n'utilisent pas la mise en page par défaut, mais celle des `ImportedFileChunkSize` paramètres du système de fichiers. Les fichiers importés au format

S3 plus grands que le `ImportedFileChunkSize` seront stockés sur plusieurs OSTs avec un nombre de bandes de. `(FileSize / ImportedFileChunksize) + 1` La valeur par défaut de `ImportedFileChunkSize` est 1 GiB.

Vous pouvez afficher la configuration de mise en page d'un fichier ou d'un répertoire à l'aide de la `lfs getstripe` commande.

```
lfs getstripe path/to/filename
```

Cette commande indique le nombre de bandes, la taille des bandes et le décalage des bandes d'un fichier. Le nombre de bandes correspond OSTs au nombre de bandes réparties sur le fichier. La taille de bande correspond à la quantité de données continues stockées sur un OST. Le décalage de bande est l'indice du premier OST sur lequel le fichier est réparti par bandes.

Modification de votre configuration de striping

Les paramètres de mise en page d'un fichier sont définis lors de sa création initiale. Utilisez la `lfs setstripe` commande pour créer un nouveau fichier vide avec une mise en page spécifiée.

```
lfs setstripe filename --stripe-count number_of_OSTs
```

La `lfs setstripe` commande affecte uniquement la mise en page d'un nouveau fichier. Utilisez-le pour définir la mise en page d'un fichier avant de le créer. Vous pouvez également définir la mise en page d'un répertoire. Une fois définie dans un répertoire, cette mise en page est appliquée à chaque nouveau fichier ajouté à ce répertoire, mais pas aux fichiers existants. Tout nouveau sous-répertoire que vous créez hérite également de la nouvelle mise en page, qui est ensuite appliquée à tout nouveau fichier ou répertoire que vous créez dans ce sous-répertoire.

Pour modifier la mise en page d'un fichier existant, utilisez la `lfs migrate` commande. Cette commande copie le fichier selon les besoins pour distribuer son contenu conformément à la mise en page que vous spécifiez dans la commande. Par exemple, les fichiers ajoutés ou dont la taille est augmentée ne modifient pas le nombre de bandes. Vous devez donc les migrer pour modifier la mise en page du fichier. Vous pouvez également créer un nouveau fichier à l'aide de la `lfs setstripe` commande pour définir sa mise en page, copier le contenu d'origine dans le nouveau fichier, puis renommer le nouveau fichier pour remplacer le fichier d'origine.

Dans certains cas, la configuration de mise en page par défaut n'est pas optimale pour votre charge de travail. Par exemple, un système de fichiers contenant des dizaines OSTs et un grand nombre

de fichiers de plusieurs gigaoctets peut améliorer ses performances en répartissant les fichiers sur un nombre de bandes supérieur à la valeur de cinq par défaut. OSTs La création de fichiers volumineux avec un faible nombre de bandes peut entraîner des problèmes de I/O performances et peut également entraîner un OSTs surpeuplement. Dans ce cas, vous pouvez créer un répertoire avec un plus grand nombre de bandes pour ces fichiers.

La configuration d'une mise en page par bandes pour les fichiers volumineux (en particulier les fichiers dont la taille est supérieure à un gigaoctet) est importante pour les raisons suivantes :

- Améliore le débit en permettant à plusieurs serveurs OSTs et à leurs serveurs associés de contribuer aux IOPS, à la bande passante réseau et aux ressources du processeur lors de la lecture et de l'écriture de fichiers volumineux.
- Réduit le risque qu'un petit sous-ensemble d'entre eux se OSTs transforme en points chauds limitant les performances globales de la charge de travail.
- Empêche un seul fichier volumineux de remplir un fichier OST, ce qui peut provoquer des erreurs de saturation du disque.

Il n'existe pas de configuration de mise en page optimale unique pour tous les cas d'utilisation. Pour obtenir des conseils détaillés sur la mise en page des fichiers, consultez la section Gestion de la mise en page des fichiers (striping) et de l'espace libre dans la documentation de Lustre.org. Les directives générales suivantes sont les suivantes :

- La mise en page par bandes est particulièrement importante pour les fichiers volumineux, en particulier pour les cas d'utilisation où les fichiers ont généralement une taille de plusieurs centaines de mégaoctets ou plus. Pour cette raison, la mise en page par défaut d'un nouveau système de fichiers assigne un nombre de bandes de cinq pour les fichiers de plus de 1 Go.
- Le nombre de bandes est le paramètre de mise en page que vous devez ajuster pour les systèmes prenant en charge des fichiers volumineux. Le nombre de bandes indique le nombre de volumes OST qui contiendront des fragments d'un fichier par bandes. Par exemple, avec un nombre de bandes de 2 et une taille de bande de 1 Mo, Lustre écrit des segments alternatifs de 1 Mo d'un fichier dans chacun des deux. OSTs
- Le nombre de bandes effectif est le moins élevé entre le nombre réel de volumes OST et la valeur du nombre de bandes que vous spécifiez. Vous pouvez utiliser la valeur spéciale du nombre de bandes `-1` pour indiquer que les bandes doivent être placées sur tous les volumes OST.

- La définition d'un grand nombre de bandes pour les petits fichiers n'est pas optimale, car certaines opérations Lustre nécessitent un aller-retour réseau pour accéder à chaque OST de la mise en page, même si le fichier est trop petit pour consommer de l'espace sur tous les volumes OST.
- Vous pouvez configurer une mise en page progressive (PFL) qui permet à la mise en page d'un fichier de changer en fonction de sa taille. Une configuration PFL peut simplifier la gestion d'un système de fichiers comportant une combinaison de gros et de petits fichiers sans que vous ayez à définir explicitement une configuration pour chaque fichier. Pour de plus amples informations, veuillez consulter Mises en page de fichiers progressives.
- La taille de bande par défaut est de 1 Mo. La définition d'un décalage de bande peut être utile dans des circonstances particulières, mais en général, il est préférable de ne pas le spécifier et d'utiliser la valeur par défaut.

Mises en page de fichiers progressives

Vous pouvez définir une configuration PFL (Progressive File Layout) pour un répertoire afin de définir différentes configurations de bandes pour les petits et les grands fichiers avant de le remplir. Par exemple, vous pouvez définir un PFL dans le répertoire de premier niveau avant que les données ne soient écrites dans un nouveau système de fichiers.

Pour spécifier une configuration PFL, utilisez la `lfs setstripe` commande avec des `-E` options pour spécifier les composants de mise en page pour des fichiers de tailles différentes, comme la commande suivante :

```
lfs setstripe -E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32 /mountname/directory
```

Cette commande définit quatre composants de mise en page :

- Le premier composant (`-E 100M -c 1`) indique une valeur de nombre de bandes de 1 pour les fichiers d'une taille maximale de 100 Mo.
- Le deuxième composant (`-E 10G -c 8`) indique un nombre de bandes de 8 pour les fichiers d'une taille maximale de 10 Go.
- Le troisième composant (`-E 100G -c 16`) indique un nombre de bandes de 16 pour les fichiers d'une taille maximale de 100 Go.
- Le quatrième composant (`-E -1 -c 32`) indique un nombre de bandes de 32 pour les fichiers de plus de 100 Go.

> **Important**
>
> L'ajout de données à un fichier créé avec une mise en page PFL remplira tous ses composants de mise en page. Par exemple, avec la commande à 4 composants illustrée ci-dessus, si vous créez un fichier de 1 Mo puis que vous ajoutez des données à la fin de celui-ci, la mise en page du fichier s'étendra pour atteindre un nombre de bandes de -1, ce qui signifie que tout le système se trouve OSTs dans le système. Cela ne signifie pas que les données seront écrites sur chaque OST, mais une opération telle que la lecture de la longueur du fichier enverra une demande en parallèle à chaque OST, alourdissant ainsi considérablement la charge réseau du système de fichiers.
> Veillez donc à limiter le nombre de bandes pour tout fichier de petite ou moyenne longueur auquel des données peuvent être ajoutées ultérieurement. Étant donné que les fichiers journaux augmentent généralement lorsque de nouveaux enregistrements sont ajoutés, Amazon FSx for Lustre attribue un nombre de bandes par défaut de 1 à tout fichier créé en mode ajout, quelle que soit la configuration de bande par défaut spécifiée par son répertoire parent.

La configuration PFL par défaut sur Amazon FSx pour les systèmes de fichiers Lustre créés après le 25 août 2023 est définie à l'aide de cette commande :

```
lfs setstripe -E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32 /mountname
```

Les clients dont les charges de travail nécessitent un accès simultané élevé à des fichiers de taille moyenne et importante bénéficieront probablement d'une mise en page comportant plus de bandes pour les fichiers de plus petite taille et des bandes sur l'ensemble OSTs pour les fichiers les plus volumineux, comme le montre l'exemple de mise en page à quatre composants.

Surveillance des performances et de l'utilisation

Chaque minute, Amazon FSx for Lustre envoie des statistiques d'utilisation pour chaque disque (MDT et OST) à Amazon. CloudWatch

Pour consulter les détails de l'utilisation globale du système de fichiers, vous pouvez consulter la statistique Sum de chaque métrique. Par exemple, la somme des `DataReadBytes` statistiques indique le débit de lecture total observé par tous les utilisateurs d'un système OSTs de fichiers. De

même, la somme des `FreeDataStorageCapacity` statistiques indique la capacité de stockage totale disponible pour les données de fichiers dans le système de fichiers.

Pour plus d'informations sur la surveillance des performances de votre système de fichiers, consultezSurveillance des systèmes de fichiers Amazon FSx pour Lustre.

Caractéristiques de performance des classes de stockage SSD et HDD

Le débit pris en charge par un système de fichiers FSx pour Lustre doté d'une classe de stockage SSD ou HDD est proportionnel à sa capacité de stockage. Les systèmes de fichiers Amazon FSx for Lustre s'adaptent à un débit multiple TBps et à des millions d'IOPS. Amazon FSx for Lustre prend également en charge l'accès simultané au même fichier ou répertoire à partir de milliers d'instances de calcul. Cet accès permet de vérifier rapidement les données de la mémoire de l'application au stockage, une technique courante dans le calcul haute performance (HPC). Vous pouvez augmenter la quantité de stockage et la capacité de débit selon vos besoins à tout moment après avoir créé le système de fichiers. Pour de plus amples informations, veuillez consulter Gestion de la capacité de stockage.

FSx pour les systèmes de fichiers Lustre, fournissent un débit de lecture en rafale en utilisant un mécanisme I/O de crédit réseau pour allouer la bande passante réseau en fonction de l'utilisation moyenne de la bande passante. Les systèmes de fichiers accumulent des crédits lorsque leur utilisation de la bande passante réseau est inférieure à leurs limites de base, et peuvent utiliser ces crédits lorsqu'ils effectuent des transferts de données réseau.

Les tableaux suivants présentent les performances FSx pour lesquelles les options de déploiement de Lustre utilisant les classes de stockage SSD et HDD sont conçues.

Performances du système de fichiers pour les options de stockage SSD

Type de déploiement	Débit réseau (MBps/TiB de stockage provisionné)		IOPS réseau (IOPS/TiB de stockage provisionné)	Stockage en cache (GiB RAM/TiB de stockage provisionné)	Latences du disque par opération de fichier (millisecondes, P50)	Débit du disque (MBps/TiB de stockage ou cache SSD provisionné)	
	Base de référence	Éclater				Base de référence	Éclater
SCRATCH_2	200	1300	Base de référence de dizaines de milliers Des centaines de milliers de personnes éclatent	6.7	Métadonnées : sub-ms Données : sub-ms	200 (lire) 100 (écrire)	-
PERSISTENT-125	320	1300		3.4		125	500
PERSISTENT-250	640	1300		6.8		250	500
PERSISTENT-500	1300	-		13,7		500	-
PERSISTENT-1000	2600	-		27,3		1 000	-

Performances du système de fichiers pour les options de stockage sur disque dur

Type de déploiement	Débit réseau (MBps/TiB de stockage ou cache SSD provisionné)		IOPS réseau (IOPS/TiB de stockage provisionné)	Stockage en cache (GiB RAM/TiB de stockage provisionné)	Latences du disque par opération de fichier (millisec ondes, P50)	Débit du disque (MBps/TiB de stockage ou cache SSD provisionné)	
	Base de référence	Éclater				Base de référence	Éclater
PERSISTENT-12							
Stockage sur disque dur	40	375*	Base de référence de dizaines de milliers Des centaines de milliers de personnes éclatent	0,4 mémoire	Métadonnées : sub-ms Données : ms à un chiffre	12	80 (lire) 50 (écrire)
Cache de lecture SSD	200	1 900		200 disques SSD en cache	Données : sub-ms	200	-
PERSISTENT-40							
Stockage sur disque dur	150	1 300*	Base de référence de dizaines de milliers Des centaines	1.5	Métadonnées : sub-ms Données : ms à un chiffre	40	250 (lire) 150 (écrire)

Performances du système de fichiers pour les options de stockage SSD de génération précédente

Type de déploiement	Débit réseau (MBps par TiB de stockage provisionné)		IOPS réseau (IOPS par TiB de stockage provisionné)	Stockage en cache (GiB par TiB de stockage provisionné)	Latences du disque par opération de fichier (millisec ondes, P50)	Débit du disque (MBps par TiB de stockage ou de cache SSD provisionné)	
	Base de référence	Éclater				Base de référence	Éclater
PERSISTENT-50	250	1 300*	Base de référence de dizaines de milliers	2,2 RAM	Métadonnées : sub-ms	50	240
PERSISTENT-100	500	1 300*		4,4 RAM	Données : sub-ms	100	240
PERSISTENT-200	750	1 300*	Des centaines de milliers de personnes éclatent	8,8 RAM		200	240

> **Note**
>
> * Les systèmes de fichiers persistants suivants Régions AWS fournissent des rafales de réseau allant jusqu'à 530 MBps par TiB de stockage : Afrique (Le Cap), Asie-Pacifique (Hong Kong), Asie-Pacifique (Osaka), Asie-Pacifique (Singapour), Canada (centre), Europe (Francfort), Europe (Londres), Europe (Milan), Europe (Stockholm), Moyen-Orient (Bahreïn), Amérique du Sud (São Paulo), Chine, et US West (Los Angeles).

Exemple : base de référence agrégée et débit en rafale

L'exemple suivant illustre l'impact de la capacité de stockage et du débit du disque sur les performances du système de fichiers.

Un système de fichiers persistant doté d'une capacité de stockage de 4,8 TiB et d'un débit de 50 MBps TiB par unité de stockage fournit un débit de base agrégé de 240 MBps et un débit de disque en rafale de 1,152. GBps

Quelle que soit la taille du système de fichiers, Amazon FSx for Lustre fournit des latences constantes inférieures à la milliseconde pour les opérations sur les fichiers.

Caractéristiques de performance de la classe de stockage Intelligent-Tiering

La classe de stockage FSx for Lustre Intelligent-Tiering offre un stockage élastique et optimisé en termes de coûts pour les charges de travail qui s'exécutent traditionnellement sur des systèmes de fichiers de stockage de fichiers hautes performances basés sur des disques durs ou mixtes HDD/SDD. Les systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering utilisent un stockage régional entièrement élastique et intelligemment hiérarchisé, qui augmente et diminue automatiquement pour s'adapter à l'évolution de votre charge de travail. Pour plus d'informations sur la manière dont il hiérarchise les données, consultezComment la classe de stockage Intelligent-Tiering hiérarchise les données.

Le débit pris en charge par un système de fichiers FSx pour Lustre doté d'une classe de stockage Intelligent-Tiering est indépendant de son stockage. Les systèmes de fichiers à hiérarchisation intelligente s'adaptent à un débit multiple et à TBps des millions d'IOPS. Les systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering fournissent également un cache de lecture SSD provisionné en option pour un accès à faible latence aux données fréquemment consultées. Par

défaut, Amazon FSx for Lustre fournit un cache de lecture SSD pour les métadonnées fréquemment consultées. Comme la plupart des charges de travail ont tendance à être gourmandes en lecture et à ne travailler activement qu'avec un petit sous-ensemble de l'ensemble de données à un moment donné, le modèle hybride du stockage à hiérarchisation intelligente et des caches de lecture SSD permet aux systèmes de fichiers utilisant la classe de stockage intelligente de fournir un stockage dont les performances sont comparables à celles des systèmes de fichiers SSD pour la plupart des charges de travail, tout en réduisant les coûts de stockage par rapport aux classes de stockage SSD et HDD.

Lors de la lecture et de l'écriture de données dans un système de fichiers à hiérarchisation intelligente, en particulier des données qui n'ont pas été consultées récemment ou assez fréquemment pour se trouver dans le cache en mémoire du serveur de fichiers, les performances dépendent de la taille du cache de lecture du SSD. L'accès aux données depuis le stockage à hiérarchisation intelligente comporte des time-to-first-byte latences d'environ plusieurs dizaines de millisecondes ainsi que des coûts par demande, tandis que les accès depuis le cache de lecture SSD génèrent un temps de latence inférieur à la milliseconde et aucun coût par demande.

Lorsque vous configurez la taille du cache de lecture SSD pour votre système de fichiers, vous devez tenir compte à la fois de la taille du jeu de données fréquemment consulté au sein de la charge de travail et de la sensibilité de la charge de travail à une latence plus élevée lors de la lecture de données moins fréquemment consultées. Vous pouvez passer d'un mode de dimensionnement du cache de lecture SSD à un autre une fois votre système de fichiers créé et augmenter ou diminuer le cache. Pour plus d'informations sur la modification du cache de lecture de votre SSD, consultezGestion du cache de lecture SSD provisionné.

Une demande d'écriture se produit lorsque FSx Lustre écrit un bloc de données dans un stockage à hiérarchisation intelligente. Lorsque vous écrivez des données dans le système de fichiers, les demandes d'écriture sont agrégées et écrites dans un stockage à hiérarchisation intelligente, ce qui augmente le débit et réduit les coûts des demandes. Les lectures peuvent être effectuées à partir du cache en mémoire du serveur de fichiers, du cache de lecture SSD ou directement à partir du stockage Intelligent-Tiering. Lorsqu'une lecture est effectuée à partir du stockage à hiérarchisation intelligente, une demande de lecture est envoyée pour chaque bloc de données récupérées. Lorsque vous lisez des données de manière séquentielle, FSx for Lustre les préextrait afin d'améliorer les performances.

Les données du cache en mémoire des systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering sont transmises directement au client demandeur sous forme d'E/S réseau. Lorsqu'un client accède à des données qui ne se trouvent pas dans le cache en mémoire, elles sont

lues à partir du cache de lecture SSD ou du stockage à hiérarchisation intelligente sous forme d'E/S disque, puis transmises au client sous forme d'E/S réseau.

Performances du système de fichiers pour la hiérarchisation intelligente

Le tableau suivant montre les performances FSx pour lesquelles les systèmes de fichiers Lustre Intelligent-Tiering sont conçus.

Capacité de débit allouée () MBps	Débit réseau () MBps		IOPS du réseau	Stockage en mémoire cache (Go)	Débit maximal du disque cache SSD () MBps	Nombre maximal d'IOPS par seconde sur disque cache SSD	
	Base de référence	Éclater				Base de référence	Éclater
Tous les 4 000	12500	-	Des centaines de milliers	76,8	4000	160000	-

Conseils sur les performances

Lorsque vous utilisez Amazon FSx pour Lustre, tenez compte des conseils de performance suivants. Pour les limites de service, voirQuotas de service pour Amazon FSx pour Lustre.

- I/O Taille moyenne : Amazon FSx for Lustre étant un système de fichiers réseau, chaque opération sur les fichiers fait l'objet d'un aller-retour entre le client et Amazon FSx for Lustre, ce qui entraîne une faible latence. En raison de cette latence par opération, le débit global augmente généralement à mesure que la I/O taille moyenne augmente, car les frais généraux sont amortis sur une plus grande quantité de données.
- Modèle de demande — En activant 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 sur Amazon for Lustre de manière asynchrone. FSx 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 les écritures synchrones envoie des demandes synchrones à Amazon FSx pour Lustre. Chaque opération fait l'objet d'un aller-retour entre le client et Amazon FSx for Lustre.

  > **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.

- Limiter la taille des répertoires : pour obtenir des performances de métadonnées optimales sur les systèmes de fichiers Persistent 2 FSx for Lustre, limitez chaque répertoire à moins de 100 000 fichiers. La limitation du nombre de fichiers dans un répertoire réduit le temps nécessaire au système de fichiers pour verrouiller le répertoire parent.
- Instances Amazon EC2 : les applications qui effectuent un grand nombre d'opérations de lecture et d'écriture ont probablement besoin de plus de mémoire ou de capacité de calcul que les applications qui n'en exécutent pas. Lorsque vous lancez vos instances Amazon EC2 pour votre charge de travail gourmande en ressources informatiques, choisissez des types d'instances dotés de la quantité de ressources dont votre application a besoin. Les caractéristiques de performance des systèmes de fichiers Amazon FSx for Lustre ne dépendent pas de l'utilisation d'instances optimisées pour Amazon EBS.
- Réglage recommandé des instances clientes pour des performances optimales

1. Pour les types d'instances clientes dont la mémoire est supérieure à 64 GiB, nous recommandons d'appliquer les réglages suivants :

```
sudo lctl set_param ldlm.namespaces.*.lru_max_age=600000
sudo lctl set_param ldlm.namespaces.*.lru_size=<100 * number_of_CPUs>
```

2. Pour les types d'instances clientes comportant plus de 64 cœurs de vCPU, nous recommandons d'appliquer les réglages suivants :

```
echo "options ptlrpc ptlrpcd_per_cpt_max=32" >> /etc/modprobe.d/modprobe.conf
echo "options ksocklnd credits=2560" >> /etc/modprobe.d/modprobe.conf

# reload all kernel modules to apply the above two settings
sudo reboot
```

   Une fois le client monté, les réglages suivants doivent être appliqués :

```
sudo lctl set_param osc.*OST*.max_rpcs_in_flight=32
sudo lctl set_param mdc.*.max_rpcs_in_flight=64
sudo lctl set_param mdc.*.max_mod_rpcs_in_flight=50
```

3. Pour optimiser les performances de la liste des annuaires (ls), les réglages suivants doivent être appliqués :

```
sudo lctl set_param llite.*.statahead_max=512
sudo lctl set_param llite.*.statahead_agl=1
if sudo lctl get_param llite.*.statahead_xattr > /dev/null 2>&1; then
    sudo lctl set_param llite.*.statahead_xattr=1
else
    echo "Warning: Xattr statahead is not supported on this Lustre client. Please
 upgrade to the latest Lustre 2.15 client to apply this tuning"
fi
```

   Notez qu'il `lctl set_param` est connu pour ne pas persister après le redémarrage. Comme ces paramètres ne peuvent pas être définis de façon permanente du côté client, il est recommandé d'implémenter une tâche cron de démarrage pour définir la configuration avec les réglages recommandés.

- Équilibre global de la charge de travail OSTs : dans certains cas, votre charge de travail ne détermine pas le débit global que votre système de fichiers peut fournir (200 MBps par TiB de

stockage). Si tel est le cas, vous pouvez utiliser CloudWatch des métriques pour déterminer si les performances sont affectées par un déséquilibre dans les I/O modèles de votre charge de travail. Pour déterminer si cela en est la cause, consultez la CloudWatch métrique maximale pour Amazon FSx for Lustre.

Dans certains cas, cette statistique indique une charge égale ou supérieure à 240 MBps de débit (la capacité de débit d'un seul disque Amazon for Lustre de 1,2 To). FSx Dans de tels cas, votre charge de travail n'est pas uniformément répartie sur vos disques. Dans ce cas, vous pouvez utiliser la `lfs setstripe` commande pour modifier le découpage des fichiers auxquels votre charge de travail accède le plus fréquemment. Pour des performances optimales, répartissez les fichiers OSTs présentant des exigences de débit élevées sur l'ensemble de votre système de fichiers.

Si vos fichiers sont importés depuis un référentiel de données, vous pouvez adopter une autre approche pour répartir vos fichiers haut débit de manière uniforme sur votre. OSTs Pour ce faire, vous pouvez modifier le `ImportedFileChunkSize` paramètre lors de la création de votre prochain système de fichiers Amazon FSx for Lustre.

Supposons, par exemple, que votre charge de travail utilise un système de fichiers de 7 To (composé de 6 fichiers de 1,17 To OSTs) et doive générer un débit élevé sur des fichiers de 2,4 Go. Dans ce cas, vous pouvez définir la `ImportedFileChunkSize` valeur de `(2.4 GiB / 6 OSTs) = 400 MiB` manière à ce que vos fichiers soient répartis uniformément sur le système de fichiers OSTs.

- Lustreclient pour les IOPS de métadonnées — Si votre système de fichiers possède une configuration de métadonnées spécifiée, nous vous recommandons d'installer un client Lustre 2.15 ou Lustre 2.12 avec l'une des versions du système d'exploitation suivantes : Amazon Linux 2023 ; Amazon Linux 2 ; Red Hat/Rocky Linux 8.9, 8.10 ou 9.x ; CentOS 8.9 ou 8.10 ; Ubuntu 22+ avec noyau 6.2, 6.5 ou 6.8 ; ou Ubuntu 20.

Considérations relatives aux performances liées à la hiérarchisation intelligente

Voici quelques considérations importantes relatives aux performances lorsque vous travaillez avec des systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering :

- Les charges de travail lisant des données de plus petite I/O taille nécessiteront une plus grande simultanéité et entraîneront des coûts de demande plus élevés pour atteindre le même débit que

les charges de travail utilisant de grandes I/O tailles en raison de la latence plus élevée due aux niveaux de stockage à hiérarchisation intelligente. Nous vous recommandons de configurer le cache de lecture de votre SSD suffisamment grand pour prendre en charge une simultanéité et un débit plus élevés lorsque vous travaillez avec des tailles d'E/S plus petites.

- Le nombre maximal d'IOPS sur disque que vos clients peuvent utiliser avec un système de fichiers à hiérarchisation intelligente dépend des modèles d'accès spécifiques à votre charge de travail et du fait que vous ayez ou non provisionné un cache de lecture SSD. Pour les charges de travail avec accès aléatoire, les clients peuvent généralement générer des IOPS beaucoup plus élevées si les données sont mises en cache dans le cache de lecture du SSD que si les données ne se trouvent pas dans le cache.
- La classe de stockage Intelligent-Tiering prend en charge la lecture anticipée afin d'optimiser les performances des demandes de lecture séquentielles. Nous vous recommandons de configurer votre modèle d'accès aux données de manière séquentielle lorsque cela est possible afin de permettre la préextraction des données et d'améliorer les performances.

Accès aux systèmes de fichiers

Avec Amazon FSx, vous pouvez transférer vos charges de travail gourmandes en ressources informatiques depuis votre site vers le cloud Amazon Web Services en important des données via un VPN. Direct Connect Vous pouvez accéder à votre système de FSx fichiers Amazon sur site, copier des données dans votre système de fichiers selon vos besoins et exécuter des charges de travail intensives sur des instances dans le cloud.

Dans la section suivante, vous découvrirez comment accéder à votre système de fichiers Amazon FSx for Lustre sur une instance Linux. En outre, vous découvrirez comment utiliser le fichier`fstab` pour remonter automatiquement votre système de fichiers après un redémarrage du système.

Avant de monter un système de fichiers, vous devez créer, configurer et lancer vos ressources AWS associées. Pour obtenir des instructions complètes, consultez Commencer à utiliser Amazon FSx pour Lustre. Vous pouvez ensuite installer et configurer le Lustre client sur votre instance de calcul.

Rubriques

- Lustrecompatibilité entre le système de fichiers et le noyau client
- Installation du Lustre client
- Montage à partir d'une instance Amazon Elastic Compute Cloud
- Configuration des clients EFA
- Montage depuis Amazon Elastic Container Service
- Montage de systèmes de FSx fichiers Amazon sur site ou depuis un Amazon VPC pair
- Montage automatique de votre système de FSx fichiers Amazon
- Montage de jeux de fichiers spécifiques
- Démontage des systèmes de fichiers
- Utilisation des instances Spot Amazon EC2

Lustrecompatibilité entre le système de fichiers et le noyau client

Nous vous recommandons vivement d'utiliser la Lustre version de votre système de fichiers FSx for Lustre compatible avec les versions du noyau Linux de vos instances clientes.

Clients Amazon Linux

Système d'exploitation	Version du système d'exploitation	Version minimale du noyau	Version maximale du noyau	Version client Lustre	Version du système de fichiers Lustre		
					2,10	2,12	2,15
Amazon L	6,12	*	*	2.15	non	oui	oui
	6.1	6,1,79-99,167	6,179-99,167 et versions ultérieures	2.15	non	oui	oui
Amazon Linux 2	5,10	5.10.144-127,601	5.10.144-127,601+	2,12	oui	oui	oui
			<5.10.144-127,601	2.10	oui	oui	non
	5.4	5,4.214-120,368	5.4.214-120,368+	2,12	oui	oui	oui
			<5.4.214-120,368	2.10	oui	oui	non
	4,14	4,14,294-220,533	4,14,294-220,533+	2,12	oui	oui	oui
			<4,14,294-220,533	2.10	oui	oui	non

Clients d'Ubuntu

Système d'exploitation	Version du système d'exploitation	Version minimale du noyau	Version maximale du noyau	Version client Lustre	Version du système de fichiers Lustre		
					2,10	2,12	2,15
Ubuntu	24	6,14,0-1012	6,14,0*	2.15	non	oui	oui
		6,8,0-1024	6,8,0*	2.15	non	oui	oui
	22	6,8,0-1017	6,8,0*	2.15	non	oui	oui
		6,5,0-1023	6,5,0*	2.15	non	oui	oui
		6,2,0-1017	6,2,0*	2.15	non	oui	oui
		5.15.0-1015-aws	5.15.0-1051-aws	2,12	oui	oui	oui
	20	5.15.0-1015-aws	5,15,0*	2,12	oui	oui	oui
		5.4.0-1011-aws	5.13.0-1031-aws	2.10	oui	oui	non

RHEL/CentOS/RockyClientèle Linux

Système d'exploitation	Version du système d'exploitation	Architecture	Version minimale du noyau	Version maximale du noyau	Version client Lustre	Version du système de fichiers Lustre		
						2,10	2,12	2,15
RHEL/ Rocky Linux	9,7	Arm + x86	5,14,0-6 1,5.1	5,14,0-6 1*	2.15	non	oui	oui
	9,6	Arm + x86	5,14.0-5 0,12.1	5,14,0-5 0*	2.15	non	oui	oui
	9,5	Arm + x86	5.14.0-5(3.19.1	5,14,0-5(3*	2.15	non	oui	oui
	9,4	Arm + x86	5,14,0-4 7,13.1	5,14,0-4 7*	2.15	non	oui	oui
	9.3	Arm + x86	5,14,0-3(2,18.1	5,14,0-3(2,18.1	2.15	non	oui	oui
	9.0	Arm + x86	5,14,0-7(,13.1	5,14,0-7(,30.1	2.15	non	oui	oui
RHEL/ Cent OS/ RockyLinux	8.10	Arm + x86	4,18,0-5 3	4,18,0-5 3*	2,12	oui	oui	oui
	8,9	Arm + x86	4,18,0-5 3*	4,18,0-5 3*	2,12	oui	oui	oui

Système d'exploitation	Version du système d'exploitation	Architecture	Version minimale du noyau	Version maximale du noyau	Version client Lustre	Version du système de fichiers Lustre		
	8,8	Arm + x86	4,18,0-47 7*	4,18,0-47 7*	2,12	oui	oui	oui
	8,7	Arm + x86	4,18,0-42 5*	4,18,0-42 5*	2,12	oui	oui	oui
	8,6	Arm + x86	4,18,0-37 2*	4,18,0-37 2*	2,12	oui	oui	oui
	8,5	Arm + x86	4,18,0-34 8*	4,18,0-34 8*	2,12	oui	oui	oui
	8,4	Arm + x86	4,18,0-30 5*	4,18,0-30 5*	2,12	oui	oui	oui
RHEL/ CentOS	8,3	Arm + x86	4,18,0-24 0*	4,18,0-24 0*	2.10	oui	oui	non
	8.2	Arm + x86	4,18,0-19 3*	4,18,0-19 3*	2.10	oui	oui	non
	7,9	x86	3,10,0-1160*	3,10,0-1160*	2,12	oui	oui	oui
	7.8	x86	3,10,0-1127*	3,10,0-1127*	2.10	oui	oui	non
	7.7	x86	3,10,0-1062*	3,10,0-1062*	2.10	oui	oui	non
CentOS	7,9	Arm	4,18,0-19 3*	4,18,0-19 3*	2,12	oui	oui	oui

Système d'exploitation	Version du système d'exploitation	Architecture	Version minimale du noyau	Version maximale du noyau	Version client Lustre	Version du système de fichiers Lustre		
	7.8	Arm	4,18,0-14 7*	4,18,0-14 7*	2,12	oui	oui	oui

Installation du Lustre client

Pour monter votre système de fichiers Amazon FSx for Lustre à partir d'une instance Linux, installez d'abord le Lustre client open source. Ensuite, en fonction de la version de votre système d'exploitation, appliquez l'une des procédures suivantes. Pour plus d'informations sur le support du noyau, consultezLustrecompatibilité entre le système de fichiers et le noyau client.

Si vous utilisez un client Lustre avec EFA (Elastic Fabric Adapter), consultezConfiguration des clients EFA.

Si votre instance de calcul n'exécute pas le noyau Linux spécifié dans les instructions d'installation et que vous ne pouvez pas modifier le noyau, vous pouvez créer votre propre Lustre client. Pour plus d'informations, consultez Compiler Lustre sur le Lustre Wiki.

Amazon Linux

Pour installer le Lustre client sur Amazon Linux 2023

1. Ouvrez un terminal sur votre client.
2. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance de calcul en exécutant la commande suivante.

   ```
   uname -r
   ```

3. Passez en revue la réponse du système et comparez-la à la configuration minimale requise pour le noyau suivante pour installer le Lustre client sur Amazon Linux 2023 :

   - 6.12 Configuration minimale requise pour le noyau : 6,12*
   - Configuration minimale requise pour le noyau 6.1 : 6.1.79-99.167.amzn2023

Si votre instance EC2 répond à la configuration minimale requise pour le noyau, passez à l'étape suivante et installez le Lustre client.

Si la commande renvoie un résultat inférieur à la configuration minimale requise pour le noyau, mettez à jour le noyau et redémarrez votre instance Amazon EC2 en exécutant la commande suivante.

```
sudo dnf -y update kernel && sudo reboot
```

Vérifiez que le noyau a été mis à jour à l'aide de la uname -r commande.

4. Téléchargez et installez le Lustre client à l'aide de la commande suivante.

```
sudo dnf install -y lustre-client
```

Pour installer le Lustre client sur Amazon Linux 2

1. Ouvrez un terminal sur votre client.
2. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance de calcul en exécutant la commande suivante.

```
uname -r
```

3. Passez en revue la réponse du système et comparez-la aux exigences minimales de noyau suivantes pour l'installation du Lustre client sur Amazon Linux 2 :

   - Configuration minimale du noyau 5.10 : 5.10.144-127.601.amzn2
   - 5.4 Configuration minimale requise pour le noyau : 5.4.214-120.368.amzn2
   - Configuration minimale du noyau 4.14 : 4.14.294-220.533.amzn2

   Si votre instance EC2 répond aux exigences minimales du noyau, passez à l'étape suivante et installez le Lustre client.

   Si la commande renvoie un résultat inférieur à la configuration minimale requise pour le noyau, mettez à jour le noyau et redémarrez votre instance Amazon EC2 en exécutant la commande suivante.

```
sudo yum -y update kernel && sudo reboot
```

Vérifiez que le noyau a été mis à jour à l'aide de la uname -r commande.

4. Téléchargez et installez le Lustre client à l'aide de la commande suivante.

```
sudo amazon-linux-extras install -y lustre
```

Si vous ne parvenez pas à mettre à niveau le noyau selon la configuration minimale requise, vous pouvez installer l'ancien client 2.10 à l'aide de la commande suivante.

```
sudo amazon-linux-extras install -y lustre2.10
```

Pour installer le Lustre client sur Amazon Linux

1. Ouvrez un terminal sur votre client.
2. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance de calcul en exécutant la commande suivante. Le Lustre client nécessite le noyau Amazon Linux `4.14, version 104` ou supérieur.

```
uname -r
```

3. Effectuez l'une des actions suivantes :

   - Si la commande renvoie une version 4.14 `4.14.104-78.84.amzn1.x86_64` ou supérieure, téléchargez et installez le Lustre client à l'aide de la commande suivante.

     ```
     sudo yum install -y lustre-client
     ```

   - Si la commande renvoie un résultat inférieur à`4.14.104-78.84.amzn1.x86_64`, mettez à jour le noyau et redémarrez votre instance Amazon EC2 en exécutant la commande suivante.

     ```
     sudo yum -y update kernel && sudo reboot
     ```

     Vérifiez que le noyau a été mis à jour à l'aide de la uname -r commande. Téléchargez et installez ensuite le Lustre client comme décrit précédemment.

CentOS, Rocky Linux et Red Hat

Pour installer le Lustre client sur Red Hat et Rocky Linux 9.0 ou 9.3—9.7

Vous pouvez installer et mettre à jour des packages Lustre clients compatibles avec Red Hat Enterprise Linux (RHEL) et Rocky Linux depuis le référentiel de packages yum du FSx Lustre client Amazon. Ces packages sont signés pour garantir qu'ils n'ont pas été falsifiés avant ou pendant le téléchargement. L'installation du référentiel échoue si vous n'installez pas la clé publique correspondante sur votre système.

Pour ajouter le référentiel de packages yum du FSx Lustre client Amazon

1. Ouvrez un terminal sur votre client.
2. Installez la clé publique Amazon FSx rpm à l'aide de la commande suivante.

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
   ```

3. Importez la clé à l'aide de la commande suivante.

   ```
   sudo rpm --import /tmp/fsx-rpm-public-key.asc
   ```

4. Ajoutez le référentiel et mettez à jour le gestionnaire de packages à l'aide de la commande suivante.

   ```
   sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/9/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
   ```

Pour configurer le référentiel yum FSx Lustre du client Amazon

Le référentiel de packages yum du FSx Lustre client Amazon est configuré par défaut pour installer le Lustre client compatible avec la version du noyau initialement fournie avec les dernières versions prises en charge de Rocky Linux et RHEL 9. Pour installer un Lustre client compatible avec la version du noyau que vous utilisez, vous pouvez modifier le fichier de configuration du référentiel.

Cette section explique comment déterminer le noyau que vous utilisez, si vous devez modifier la configuration du référentiel et comment modifier le fichier de configuration.

1. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance de calcul à l'aide de la commande suivante.

   ```
   uname -r
   ```

2. Effectuez l'une des actions suivantes :

   - Si la commande revient`5.14.0-611*`, il n'est pas nécessaire de modifier la configuration du référentiel. Passez à la procédure Pour installer le Lustre client.
   - Si la commande revient`5.14.0-570*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour la version 9.6 de Rocky Linux et RHEL.
   - Si la commande revient`5.14.0-503*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions Rocky Linux et RHEL 9.5.
   - Si la commande revient`5.14.0-427*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions Rocky Linux et RHEL 9.4.
   - Si la commande revient`5.14.0-362.18.1`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions Rocky Linux et RHEL 9.3.
   - Si la commande revient`5.14.0-70*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions Rocky Linux et RHEL 9.0.

3. Modifiez le fichier de configuration du référentiel pour qu'il pointe vers une version spécifique de RHEL à l'aide de la commande suivante. *`specific_RHEL_version`*Remplacez-le par la version RHEL que vous devez utiliser.

   ```
   sudo sed -i 's#9#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
   ```

   Par exemple, pour pointer vers la version 9.6, *`specific_RHEL_version`* remplacez-la par `9.6` dans la commande, comme dans l'exemple suivant.

   ```
   sudo sed -i 's#9#9.6#' /etc/yum.repos.d/aws-fsx.repo
   ```

4. Utilisez la commande suivante pour effacer le cache yum.

   ```
   sudo yum clean all
   ```

Pour installer le client Lustre

- Installez les packages depuis le référentiel à l'aide de la commande suivante.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informations supplémentaires (Rocky Linux et Red Hat 9.0 et versions ultérieures)

Les commandes précédentes installent les deux packages nécessaires au montage et à l'interaction avec votre système de FSx fichiers Amazon. Le référentiel inclut des Lustre packages supplémentaires, tels qu'un package contenant le code source et des packages contenant des tests, que vous pouvez éventuellement installer. Pour répertorier tous les packages disponibles dans le référentiel, utilisez la commande suivante.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Pour télécharger le fichier source rpm, qui contient une archive du code source en amont et l'ensemble des correctifs que nous avons appliqués, utilisez la commande suivante.

```
 sudo yumdownloader --source kmod-lustre-client
```

Lorsque vous exécutez yum update, une version plus récente du module est installée si elle est disponible et la version existante est remplacée. Pour éviter que la version actuellement installée ne soit supprimée lors de la mise à jour, ajoutez une ligne comme celle-ci à votre `/etc/yum.conf` fichier.

```
installonlypkgs=kernel, kernel-PAE, installonlypkg(kernel), installonlypkg(kernel-
module),
              installonlypkg(vm), multiversion(kernel), kmod-lustre-client
```

Cette liste inclut les packages d'installation uniquement par défaut, spécifiés dans la page `yum.conf` de manuel, ainsi que le `kmod-lustre-client` package.

Pour installer le Lustre client sur CentOS et Red Hat 8.2—8.10 ou sur Rocky Linux 8.4—8.10

Vous pouvez installer et mettre à jour des packages Lustre clients compatibles avec Red Hat Enterprise Linux (RHEL), Rocky Linux et CentOS à partir du référentiel de packages yum du client FSx Lustre Amazon. Ces packages sont signés pour garantir qu'ils n'ont pas été falsifiés avant ou

pendant le téléchargement. L'installation du référentiel échoue si vous n'installez pas la clé publique correspondante sur votre système.

Pour ajouter le référentiel de packages yum du FSx Lustre client Amazon

1. Ouvrez un terminal sur votre client.
2. Installez la clé publique Amazon FSx rpm à l'aide de la commande suivante.

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Importez la clé à l'aide de la commande suivante.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Ajoutez le référentiel et mettez à jour le gestionnaire de packages à l'aide de la commande suivante.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/8/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Pour configurer le référentiel yum FSx Lustre du client Amazon

Le référentiel de packages yum du FSx Lustre client Amazon est configuré par défaut pour installer le Lustre client compatible avec la version du noyau initialement fournie avec les dernières versions supportées de CentOS, Rocky Linux et RHEL 8. Pour installer un Lustre client compatible avec la version du noyau que vous utilisez, vous pouvez modifier le fichier de configuration du référentiel.

Cette section explique comment déterminer le noyau que vous utilisez, si vous devez modifier la configuration du référentiel et comment modifier le fichier de configuration.

1. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance de calcul à l'aide de la commande suivante.

```
uname -r
```

2. Effectuez l’une des actions suivantes :

   - Si la commande est renvoyée`4.18.0-553*`, il n'est pas nécessaire de modifier la configuration du référentiel. Passez à la procédure Pour installer le Lustre client.

- Si la commande est renvoyée`4.18.0-513*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS, Rocky Linux et RHEL 8.9.
- Si la commande est renvoyée`4.18.0-477*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS, Rocky Linux et RHEL 8.8.
- Si la commande est renvoyée`4.18.0-425*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS, Rocky Linux et RHEL 8.7.
- Si la commande est renvoyée`4.18.0-372*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS, Rocky Linux et RHEL 8.6.
- Si la commande est renvoyée`4.18.0-348*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS, Rocky Linux et RHEL 8.5.
- Si la commande est renvoyée`4.18.0-305*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS, Rocky Linux et RHEL 8.4.
- Si la commande est renvoyée`4.18.0-240*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS et RHEL 8.3.
- Si la commande est renvoyée`4.18.0-193*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS et RHEL 8.2.

3. Modifiez le fichier de configuration du référentiel pour qu'il pointe vers une version spécifique de RHEL à l'aide de la commande suivante.

```
sudo sed -i 's#8#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
```

Par exemple, pour pointer vers la version 8.9, *`specific_RHEL_version`* remplacez-la par `8.9` dans la commande.

```
sudo sed -i 's#8#8.9#' /etc/yum.repos.d/aws-fsx.repo
```

4. Utilisez la commande suivante pour effacer le cache yum.

```
sudo yum clean all
```

Pour installer le client Lustre

- Installez les packages depuis le référentiel à l'aide de la commande suivante.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informations supplémentaires (CentOS, Rocky Linux et Red Hat 8.2 et versions ultérieures)

Les commandes précédentes installent les deux packages nécessaires au montage et à l'interaction avec votre système de FSx fichiers Amazon. Le référentiel inclut des Lustre packages supplémentaires, tels qu'un package contenant le code source et des packages contenant des tests, que vous pouvez éventuellement installer. Pour répertorier tous les packages disponibles dans le référentiel, utilisez la commande suivante.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Pour télécharger le fichier source rpm, qui contient une archive du code source en amont et l'ensemble des correctifs que nous avons appliqués, utilisez la commande suivante.

```
 sudo yumdownloader --source kmod-lustre-client
```

Lorsque vous exécutez yum update, une version plus récente du module est installée si elle est disponible et la version existante est remplacée. Pour éviter que la version actuellement installée ne soit supprimée lors de la mise à jour, ajoutez une ligne comme celle-ci à votre `/etc/yum.conf` fichier.

```
installonlypkgs=kernel, kernel-PAE, installonlypkg(kernel), installonlypkg(kernel-
module),
              installonlypkg(vm), multiversion(kernel), kmod-lustre-client
```

Cette liste inclut les packages d'installation uniquement par défaut, spécifiés dans la page `yum.conf` de manuel, ainsi que le `kmod-lustre-client` package.

Pour installer le Lustre client sur CentOS et Red Hat 7.7, 7.8 ou 7.9 (instances x86_64)

Vous pouvez installer et mettre à jour des packages Lustre clients compatibles avec Red Hat Enterprise Linux (RHEL) et CentOS à partir du référentiel de packages yum du client FSx Lustre Amazon. Ces packages sont signés pour garantir qu'ils n'ont pas été falsifiés avant ou pendant

le téléchargement. L'installation du référentiel échoue si vous n'installez pas la clé publique correspondante sur votre système.

Pour ajouter le référentiel de packages yum du FSx Lustre client Amazon

1. Ouvrez un terminal sur votre client.
2. Installez la clé publique Amazon FSx rpm à l'aide de la commande suivante.

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Importez la clé à l'aide de la commande suivante.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Ajoutez le référentiel et mettez à jour le gestionnaire de packages à l'aide de la commande suivante.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/7/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Pour configurer le référentiel yum FSx Lustre du client Amazon

Le référentiel de packages yum du FSx Lustre client Amazon est configuré par défaut pour installer le Lustre client compatible avec la version du noyau initialement fournie avec les dernières versions de CentOS et RHEL 7 prises en charge. Pour installer un Lustre client compatible avec la version du noyau que vous utilisez, vous pouvez modifier le fichier de configuration du référentiel.

Cette section explique comment déterminer le noyau que vous utilisez, si vous devez modifier la configuration du référentiel et comment modifier le fichier de configuration.

1. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance de calcul à l'aide de la commande suivante.

```
uname -r
```

2. Effectuez l’une des actions suivantes :

   - Si la commande est renvoyée`3.10.0-1160*`, il n'est pas nécessaire de modifier la configuration du référentiel. Passez à la procédure Pour installer le Lustre client.

- Si la commande est renvoyée`3.10.0-1127*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS et RHEL 7.8.
- Si la commande est renvoyée`3.10.0-1062*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client pour les versions CentOS et RHEL 7.7.

3. Modifiez le fichier de configuration du référentiel pour qu'il pointe vers une version spécifique de RHEL à l'aide de la commande suivante.

   ```
   sudo sed -i 's#7#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
   ```

   Pour pointer vers la version 7.8, *`specific_RHEL_version`* remplacez-la par `7.8` dans la commande.

   ```
   sudo sed -i 's#7#7.8#' /etc/yum.repos.d/aws-fsx.repo
   ```

   Pour pointer vers la version 7.7, *`specific_RHEL_version`* remplacez-la par `7.7` dans la commande.

   ```
   sudo sed -i 's#7#7.7#' /etc/yum.repos.d/aws-fsx.repo
   ```

4. Utilisez la commande suivante pour effacer le cache yum.

   ```
   sudo yum clean all
   ```

Pour installer le client Lustre

- Installez les packages Lustre clients depuis le référentiel à l'aide de la commande suivante.

  ```
  sudo yum install -y kmod-lustre-client lustre-client
  ```

Informations supplémentaires (CentOS et Red Hat 7.7 et versions ultérieures)

Les commandes précédentes installent les deux packages nécessaires au montage et à l'interaction avec votre système de FSx fichiers Amazon. Le référentiel inclut des Lustre packages supplémentaires, tels qu'un package contenant le code source et des packages contenant des tests, que vous pouvez éventuellement installer. Pour répertorier tous les packages disponibles dans le référentiel, utilisez la commande suivante.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Pour télécharger le fichier source rpm contenant une archive du code source en amont et de l'ensemble des correctifs que nous avons appliqués, utilisez la commande suivante.

```
 sudo yumdownloader --source kmod-lustre-client
```

Lorsque vous exécutez yum update, une version plus récente du module est installée si elle est disponible, et la version existante est remplacée. Pour éviter que la version actuellement installée ne soit supprimée lors de la mise à jour, ajoutez une ligne comme celle-ci à votre `/etc/yum.conf` fichier.

```
installonlypkgs=kernel, kernel-big-mem, kernel-enterprise, kernel-smp,
              kernel-debug, kernel-unsupported, kernel-source, kernel-devel, kernel-
PAE,
              kernel-PAE-debug, kmod-lustre-client
```

Cette liste inclut les packages d'installation uniquement par défaut, spécifiés dans la page `yum.conf` de manuel, ainsi que le `kmod-lustre-client` package.

Pour installer le Lustre client sur CentOS 7.8 ou 7.9 (instances basées sur ARM basées sur Graviton AWS)

Vous pouvez installer et mettre à jour des packages Lustre clients à partir du référentiel de packages Amazon FSx Lustre client yum compatibles avec CentOS 7 pour les instances EC2 AWS basées sur ARM basées sur Graviton. Ces packages sont signés pour garantir qu'ils n'ont pas été falsifiés avant ou pendant le téléchargement. L'installation du référentiel échoue si vous n'installez pas la clé publique correspondante sur votre système.

Pour ajouter le référentiel de packages yum du FSx Lustre client Amazon

1. Ouvrez un terminal sur votre client.
2. Installez la clé publique Amazon FSx rpm à l'aide de la commande suivante.

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-
   key.asc -o /tmp/fsx-rpm-public-key.asc
   ```

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.cn/fsx-rpm-public-
key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Importez la clé à l'aide de la commande suivante.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Ajoutez le référentiel et mettez à jour le gestionnaire de packages à l'aide de la commande suivante.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/centos/7/fsx-lustre-
client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Pour configurer le référentiel yum FSx Lustre du client Amazon

Le référentiel de packages yum du FSx Lustre client Amazon est configuré par défaut pour installer le Lustre client compatible avec la version du noyau initialement fournie avec la dernière version de CentOS 7 prise en charge. Pour installer un Lustre client compatible avec la version du noyau que vous utilisez, vous pouvez modifier le fichier de configuration du référentiel.

Cette section explique comment déterminer le noyau que vous utilisez, si vous devez modifier la configuration du référentiel et comment modifier le fichier de configuration.

1. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance de calcul à l'aide de la commande suivante.

```
uname -r
```

2. Effectuez l’une des actions suivantes :

   - Si la commande est renvoyée`4.18.0-193*`, il n'est pas nécessaire de modifier la configuration du référentiel. Passez à la procédure Pour installer le Lustre client.
   - Si la commande est renvoyée`4.18.0-147*`, vous devez modifier la configuration du référentiel afin qu'elle pointe vers le Lustre client de la version 7.8 de CentOS.

3. Modifiez le fichier de configuration du référentiel pour qu'il pointe vers la version CentOS 7.8 à l'aide de la commande suivante.

```
sudo sed -i 's#7#7.8#' /etc/yum.repos.d/aws-fsx.repo
```

4. Utilisez la commande suivante pour effacer le cache yum.

```
sudo yum clean all
```

Pour installer le client Lustre

- Installez les packages depuis le référentiel à l'aide de la commande suivante.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informations supplémentaires (CentOS 7.8 ou 7.9 pour les instances EC2 basées sur ARM et alimentées par AWS Graviton)

Les commandes précédentes installent les deux packages nécessaires au montage et à l'interaction avec votre système de FSx fichiers Amazon. Le référentiel inclut des Lustre packages supplémentaires, tels qu'un package contenant le code source et des packages contenant des tests, que vous pouvez éventuellement installer. Pour répertorier tous les packages disponibles dans le référentiel, utilisez la commande suivante.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Pour télécharger le fichier source rpm, qui contient une archive du code source en amont et l'ensemble des correctifs que nous avons appliqués, utilisez la commande suivante.

```
 sudo yumdownloader --source kmod-lustre-client
```

Lorsque vous exécutez yum update, une version plus récente du module est installée si elle est disponible, et la version existante est remplacée. Pour éviter que la version actuellement installée ne soit supprimée lors de la mise à jour, ajoutez une ligne comme celle-ci à votre `/etc/yum.conf` fichier.

```
installonlypkgs=kernel, kernel-big-mem, kernel-enterprise, kernel-smp,
              kernel-debug, kernel-unsupported, kernel-source, kernel-devel, kernel-
PAE,
              kernel-PAE-debug, kmod-lustre-client
```

Cette liste inclut les packages d'installation uniquement par défaut, spécifiés dans la page `yum.conf` de manuel, ainsi que le `kmod-lustre-client` package.

Ubuntu avec taille de page par défaut (4 Ko)

Pour installer le Lustre client sur Ubuntu 18.04, 20.04, 22.04 ou 24.04 avec la taille de page par défaut (4 Ko)

Vous pouvez obtenir Lustre des packages depuis le référentiel Amazon FSx Ubuntu. Pour vérifier que le contenu du dépôt n'a pas été altéré avant ou pendant le téléchargement, une signature GNU Privacy Guard (GPG) est appliquée aux métadonnées du dépôt. L'installation du dépôt échoue à moins que la bonne clé GPG publique ne soit installée sur votre système.

1. Ouvrez un terminal sur votre client.
2. Suivez ces étapes pour ajouter le référentiel Amazon FSx Ubuntu :

   a. Si vous n'avez pas encore enregistré de référentiel Amazon FSx Ubuntu sur votre instance cliente, téléchargez et installez la clé publique requise. Utilisez la commande suivante de l'.

   ```
   wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
   ```

   b. Ajoutez le référentiel de FSx packages Amazon à votre gestionnaire de packages local à l'aide de la commande suivante.

   ```
   sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu $(lsb_release -cs) main" > /etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
   ```

3. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance cliente et mettez-le à jour si nécessaire. Pour obtenir la liste des noyaux requis pour le Lustre client sur Ubuntu pour les instances EC2 basées sur x86 et les instances EC2 basées sur ARM alimentées par des processeurs Graviton, voir. AWS Clients d'Ubuntu

   a. Exécutez la commande suivante pour déterminer quel noyau est en cours d'exécution.

   ```
   uname -r
   ```

b. Exécutez la commande suivante pour mettre à jour le noyau et la dernière Lustre version d'Ubuntu, puis redémarrez.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Si la version de votre noyau est supérieure à la version minimale du noyau pour les instances EC2 basées sur x86 et les instances EC2 basées sur Graviton, et que vous ne souhaitez pas effectuer la mise à jour vers la dernière version du noyau, vous pouvez effectuer l'installation Lustre pour le noyau actuel à l'aide de la commande suivante.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Les deux Lustre packages nécessaires au montage et à l'interaction avec votre système de fichiers FSx for Lustre sont installés. Vous pouvez éventuellement installer des packages connexes supplémentaires, tels qu'un package contenant le code source et des packages contenant des tests inclus dans le référentiel.

c. Répertoriez tous les packages disponibles dans le référentiel à l'aide de la commande suivante.

```
sudo apt-cache search ^lustre
```

d. (Facultatif) Si vous souhaitez que la mise à niveau de votre système mette également toujours à niveau les modules Lustre clients, assurez-vous que le `lustre-client-modules-aws` package est installé à l'aide de la commande suivante.

```
sudo apt install -y lustre-client-modules-aws
```

> **Note**
>
> Si un `Module Not Found` message d'erreur s'affiche, consultezPour résoudre les erreurs de module manquantes.

Pour résoudre les erreurs de module manquantes

Si un `Module Not Found` message d'erreur s'affiche lors de l'installation sur n'importe quelle version d'Ubuntu, procédez comme suit :

Rétrogradez votre noyau vers la dernière version prise en charge. Répertoriez toutes les versions disponibles lustre-client-modules du package et installez le noyau correspondant. Pour ce faire, exécutez la commande suivante.

```
sudo apt-cache search lustre-client-modules
```

Par exemple, si la dernière version incluse dans le référentiel est `lustre-client-modules-5.4.0-1011-aws` la suivante :

1. Installez le noyau pour lequel ce package a été conçu à l'aide des commandes suivantes.

   ```
   sudo apt-get install -y linux-image-5.4.0-1011-aws
   ```

   ```
   sudo sed -i 's/GRUB_DEFAULT=.\+/GRUB\_DEFAULT="Advanced options for Ubuntu>Ubuntu,
    with Linux 5.4.0-1011-aws"/' /etc/default/grub
   ```

   ```
   sudo update-grub
   ```

2. Redémarrez votre instance à l'aide de la commande suivante.

   ```
   sudo reboot
   ```

3. Installez le Lustre client à l'aide de la commande suivante.

   ```
   sudo apt-get install -y lustre-client-modules-$(uname -r)
   ```

Ubuntu avec une taille de page de 64 Ko

Pour installer le Lustre client sur Ubuntu24.04 (ARM64) avec une taille de page de 64 Ko

Vous pouvez obtenir Lustre des packages depuis le référentiel Amazon FSx Ubuntu. Pour vérifier que le contenu du dépôt n'a pas été altéré avant ou pendant le téléchargement, une signature GNU Privacy Guard (GPG) est appliquée aux métadonnées du dépôt. L'installation du dépôt échoue à moins que la bonne clé GPG publique ne soit installée sur votre système.

1. Ouvrez un terminal sur votre client.
2. Vérifiez que votre instance utilise une taille de page de 64 Ko. Le résultat doit être`65536`.

```
getconf PAGESIZE
```

3. Suivez ces étapes pour ajouter le référentiel Amazon FSx Ubuntu :

   a. Si vous n'avez pas encore enregistré de référentiel Amazon FSx Ubuntu sur votre instance cliente, téléchargez et installez la clé publique requise. Utilisez la commande suivante de l'.

   ```
   wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
   ```

   b. Ajoutez le référentiel de FSx packages Amazon à votre gestionnaire de packages local à l'aide de la commande suivante.

   ```
   sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu $(lsb_release -cs) main" > /etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
   ```

4. Déterminez quel noyau est actuellement en cours d'exécution sur votre instance cliente et mettez-le à jour si nécessaire. La version de votre noyau Ubuntu 24 doit être `6.14.0-1018-aws-64k` ou ultérieure.

   a. Exécutez la commande suivante pour déterminer quel noyau est en cours d'exécution.

   ```
   uname -r
   ```

   b. Exécutez la commande suivante pour effectuer la mise à jour vers la dernière version du noyau Ubuntu et de Lustre, puis redémarrez.

   ```
   sudo apt install -y linux-aws-64k lustre-client-modules-aws-64k && sudo reboot
   ```

   Si la version de votre noyau est supérieure à celle `6.14.0-1018-aws-64k` des instances EC2 basées sur Graviton et que vous ne souhaitez pas passer à la dernière version du noyau, vous pouvez effectuer l'installation Lustre pour le noyau actuel à l'aide de la commande suivante.

   ```
   sudo apt install -y lustre-client-modules-$(uname -r)
   ```

Les deux Lustre packages nécessaires au montage et à l'interaction avec votre système de fichiers FSx for Lustre sont installés. Vous pouvez éventuellement installer des packages connexes supplémentaires, tels qu'un package contenant le code source et des packages contenant des tests inclus dans le référentiel.

c. Répertoriez tous les packages disponibles dans le référentiel à l'aide de la commande suivante.

```
sudo apt-cache search ^lustre
```

d. (Facultatif) Si vous souhaitez que la mise à niveau de votre système mette également toujours à niveau les modules Lustre clients, assurez-vous que le `lustre-client-modules-aws-64k` package est installé à l'aide de la commande suivante.

```
sudo apt install -y lustre-client-modules-aws-64k
```

SUSE Linux

Pour installer le Lustre client sur SUSE Linux 12 SP3 SP4, ou SP5

Pour installer le Lustre client sur SUSE Linux 12 SP3

1. Ouvrez un terminal sur votre client.
2. Installez la clé publique Amazon FSx rpm à l'aide de la commande suivante.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importez la clé à l'aide de la commande suivante.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Ajoutez le référentiel pour le Lustre client à l'aide de la commande suivante.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Téléchargez et installez le Lustre client à l'aide des commandes suivantes.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
sudo sed -i 's#SLES-12#SP3#' /etc/zypp/repos.d/aws-fsx.repo
sudo zypper refresh
sudo zypper in lustre-client
```

Pour installer le Lustre client sur SUSE Linux 12 SP4

1. Ouvrez un terminal sur votre client.
2. Installez la clé publique Amazon FSx rpm à l'aide de la commande suivante.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-
public-key.asc
```

3. Importez la clé à l'aide de la commande suivante.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Ajoutez le référentiel pour le Lustre client à l'aide de la commande suivante.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-
lustre-client.repo
```

5. Effectuez l’une des actions suivantes :

   - Si vous l'avez installé SP4 directement, téléchargez et installez le Lustre client à l'aide des commandes suivantes.

     ```
     sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
     sudo sed -i 's#SLES-12#SP4#' /etc/zypp/repos.d/aws-fsx.repo
     sudo zypper refresh
     sudo zypper in lustre-client
     ```

   - Si vous avez migré SP3 vers SP4 et ajouté le FSx référentiel Amazon pour SP3, téléchargez et installez le Lustre client à l'aide des commandes suivantes.

     ```
     sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
     sudo sed -i 's#SP3#SP4#' /etc/zypp/repos.d/aws-fsx.repo
     sudo zypper ref
     sudo zypper up --force-resolution lustre-client-kmp-default
     ```

Pour installer le Lustre client sur SUSE Linux 12 SP5

1. Ouvrez un terminal sur votre client.
2. Installez la clé publique Amazon FSx rpm à l'aide de la commande suivante.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importez la clé à l'aide de la commande suivante.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Ajoutez le référentiel pour le Lustre client à l'aide de la commande suivante.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Effectuez l'une des actions suivantes :

   - Si vous l'avez installé SP5 directement, téléchargez et installez le Lustre client à l'aide des commandes suivantes.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
sudo zypper refresh
sudo zypper in lustre-client
```

   - Si vous avez migré SP4 vers SP5 et ajouté le FSx référentiel Amazon pour SP4, téléchargez et installez le Lustre client à l'aide des commandes suivantes.

```
sudo sed -i 's#SP4#SLES-12' /etc/zypp/repos.d/aws-fsx.repo
sudo zypper ref
sudo zypper up --force-resolution lustre-client-kmp-default
```

> **Note**
>
> Vous devrez peut-être redémarrer votre instance de calcul pour que le client termine l'installation.

Montage à partir d'une instance Amazon Elastic Compute Cloud

Vous pouvez monter votre système de fichiers à partir d'une instance Amazon EC2.

Pour monter votre système de fichiers depuis Amazon EC2

1. Connectez-vous à votre instance EC2 Amazon.
2. Créez un répertoire sur votre système de fichiers FSx for Lustre pour le point de montage à l'aide de la commande suivante.

   ```
   $ sudo mkdir -p /fsx
   ```

3. Montez le système de fichiers Amazon FSx for Lustre dans le répertoire que vous avez créé. Utilisez la commande suivante et remplacez les éléments suivants :

   - Remplacez *file_system_dns_name* par le nom DNS réel du système de fichiers.
   - Remplacez *mountname* par le nom de montage du système de fichiers. Ce nom de montage est renvoyé dans la réponse à l'opération de l'`CreateFileSystem`API. Il est également renvoyé dans la réponse de la describe-file-systems AWS CLI commande et dans le fonctionnement de l'DescribeFileSystemsAPI.

   ```
   sudo mount -t lustre -o relatime,flock file_system_dns_name@tcp:/mountname /fsx
   ```

   Cette commande permet de monter votre système de fichiers avec deux options, `-o relatime` et `flock` :

   - `relatime`— Bien que l'`atime`option conserve `atime` (temps d'accès aux inodes) les données pour chaque accès à un fichier, elle conserve également les `relatime` `atime` données, mais pas pour chaque accès à un fichier. Lorsque l'`relatime`option est activée, les `atime` données sont écrites sur le disque uniquement si le fichier a été modifié depuis la dernière mise à jour des `atime` données (`mtime`), ou si le dernier accès au fichier remonte à un certain temps (6 heures par défaut). L'utilisation de l'`atime`option `relatime` ou optimisera les processus de publication des fichiers.

> **Note**
>
> Si votre charge de travail nécessite un temps d'accès précis, vous pouvez utiliser l'option de `atime` montage. Cela peut toutefois avoir un impact sur les performances de la charge de travail en augmentant le trafic réseau requis pour maintenir des valeurs de temps d'accès précises.
> Si votre charge de travail ne nécessite pas de temps d'accès aux métadonnées, l'utilisation de l'option de `noatime` montage pour désactiver les mises à jour du temps d'accès peut apporter un gain de performances. Sachez que les processus `atime` ciblés tels que la publication de fichiers ou la publication de la validité des données seront inexacts lors de leur publication.

- `flock`— Active le verrouillage des fichiers pour votre système de fichiers. Si vous ne souhaitez pas activer le verrouillage des fichiers, utilisez la `mount` commande sans`flock`.

4. Vérifiez que la commande mount a réussi en répertoriant le contenu du répertoire dans lequel vous avez monté le système de fichiers, /mnt/fsx, à l'aide de la commande suivante.

```
$ ls /fsx
import-path  lustre
$
```

Vous pouvez également utiliser la `df` commande suivante.

```
$ df
Filesystem                     1K-blocks    Used  Available Use% Mounted on
devtmpfs                         1001808       0    1001808   0% /dev
tmpfs                            1019760       0    1019760   0% /dev/shm
tmpfs                            1019760     392    1019368   1% /run
tmpfs                            1019760       0    1019760   0% /sys/fs/cgroup
/dev/xvda1                       8376300 1263180    7113120  16% /
123.456.789.0@tcp:/mountname 3547698816   13824 3547678848   1% /fsx
tmpfs                             203956       0     203956   0% /run/user/1000
```

Les résultats montrent que le système de FSx fichiers Amazon est monté sur /fsx.

Configuration des clients EFA

Utilisez les procédures suivantes pour configurer votre client Lustre afin qu'il accède à un système de fichiers FSx pour Lustre via Elastic Fabric Adapter (EFA).

EFA est pris en charge sur les clients Lustre exécutant les systèmes d'exploitation suivants :

- Amazon Linux 2023 (AL2023)
- Red Hat Enterprise Linux (RHEL) 9.5 ou version ultérieure
- Ubuntu 22.04 ou version ultérieure avec la version 6.8+ du noyau

L'EFA est pris en charge sur les clients Lustre listés ci-dessous. Pour de plus amples informations, veuillez consulter Installation du Lustre client.

L'EFA est pris en charge sur les EC2 instances Nitro v4 (ou supérieures) compatibles avec EFA, à l'exception de la famille d'instances trn2. Consultez la section Types d'instances pris en charge dans le guide de EC2 l'utilisateur Amazon.

Rubriques

- Étape 1 : Installation des pilotes requis
- Étape 2 : Configuration de l'EFA pour le client Lustre
- Étape 3 : interfaces EFA

Étape 1 : Installation des pilotes requis

> **Note**
>
> Si vous utilisez une AMI Deep Learning, vous pouvez ignorer cette étape car le client Lustre, le pilote EFA et le pilote NVIDIA GPUDirect Storage (GDS) sont préinstallés.

Installation du client Lustre et du pilote EFA

Pour installer rapidement le client Lustre et le pilote EFA

1. Téléchargez et décompressez le fichier contenant le script d'installation :

```
curl -O https://docs.aws.amazon.com/fsx/latest/LustreGuide/samples/install-fsx-lustre-client.zip
unzip install-fsx-lustre-client.zip
```

2. Accédez au `install-fsx-lustre-client` dossier et exécutez le script d'installation :

```
cd install-fsx-lustre-client
sudo ./bin/install-fsx-lustre-client.sh --install-lustre --install-efa
```

Le script effectue automatiquement les opérations suivantes :

- Installe le client Lustre
- Installe le pilote EFA
- Vérifie l'installation du client Lustre et du pilote EFA

Pour obtenir la liste des options et des exemples d'utilisation que vous pouvez utiliser avec le `install-fsx-lustre-client.sh` script, consultez le `README.md` fichier dans le fichier zip.

Installez le pilote GDS (facultatif)

Cette étape n'est requise que si vous prévoyez d'utiliser le GPUDirect stockage NVIDIA (GDS) avec FSx for Lustre.

Prérequis:

- Instance Amazon EC2 P5, P5e, P5en ou P6-B200
- Pilote NVIDIA GDS version 2.24.2 ou supérieure

Pour installer le pilote GPUDirect de stockage NVIDIA sur votre instance cliente

1. Clonez le référentiel NVIDIA GDS :

```
git clone https://github.com/NVIDIA/gds-nvidia-fs.git
```

2. Compilez et installez le pilote :

```
cd gds-nvidia-fs/src/
```

```
export NVFS_MAX_PEER_DEVS=128
export NVFS_MAX_PCI_DEPTH=16
sudo -E make
sudo insmod nvidia-fs.ko
```

Étape 2 : Configuration de l'EFA pour le client Lustre

Pour accéder à un système de fichiers FSx pour Lustre à l'aide d'une interface EFA, vous devez installer les modules Lustre EFA et configurer les interfaces EFA.

Configuration rapide

Pour configurer rapidement votre client Lustre

1. Connectez-vous à votre EC2 instance Amazon.
2. Téléchargez et décompressez le fichier contenant le script de configuration :

   ```
   curl -O https://docs.aws.amazon.com/fsx/latest/LustreGuide/samples/configure-efa-fsx-lustre-client.zip
   unzip configure-efa-fsx-lustre-client.zip
   ```

3. Accédez au `configure-efa-fsx-lustre-client` dossier et exécutez le script de configuration :

   ```
   cd configure-efa-fsx-lustre-client
   # for regular IO
   sudo ./setup.sh

   # for NVIDIA GPUDirect Storage (GDS) IO
   sudo ./setup.sh --optimized-for-gds
   ```

   Le script effectue automatiquement les opérations suivantes :

   - Importe des modules Lustre
   - Configure les interfaces TCP et EFA
   - Crée un service systemd pour la configuration automatique au redémarrage

   Pour obtenir la liste des options et des exemples d'utilisation que vous pouvez utiliser avec le `setup.sh` script, consultez le `README.md` fichier dans le fichier zip.

Gestion manuelle du service Systemd

Le fichier de service systemd est créé dans/etc/systemd/system/configure- efa-fsx-lustre-client .service. Voici quelques commandes utiles liées au système :

```
# Check status
sudo systemctl status configure-efa-fsx-lustre-client.service

# View logs
sudo journalctl -u configure-efa-fsx-lustre-client.service
# View warnings/errors from dmesg
sudo dmesg
```

Pour plus d'informations, consultez le `README.md` fichier dans le fichier zip.

Configuration de montage automatique (en option)

Pour plus d'informations sur le montage automatique de votre système de fichiers Amazon FSx for Lustre au démarrage, consultezMontage automatique de votre système de FSx fichiers Amazon.

Étape 3 : interfaces EFA

Chaque système de fichiers FSx for Lustre a une limite maximale de 1 024 connexions EFA pour toutes les instances clientes.

Le `configure-efa-fsx-lustre-client.sh` script configure automatiquement les interfaces EFA en fonction du type d'instance.

Type d'instance	Nombre d'interfaces EFA par défaut
p6e-gb200.36xlarge	8
p6-b200.48xlarge	8
p5en.48xlarge	8
p5e.48xlarge	8
p5.48xlarge	8

Type d'instance	Nombre d'interfaces EFA par défaut
Autres instances avec plusieurs cartes réseau	2
Autres instances avec une seule carte réseau	1

Chaque interface EFA configurée sur une instance client compte comme une connexion par rapport à la limite de 1024 connexions EFA lorsqu'elle est connectée à un système de fichiers FSx pour Lustre.

Gestion manuelle des interfaces EFA

Les instances dotées d'un plus grand nombre d'interfaces EFA prennent généralement en charge un débit plus élevé. Vous pouvez personnaliser le nombre d'interfaces afin d'optimiser les performances pour vos charges de travail spécifiques, à condition de respecter la limite totale de connexions EFA.

Vous pouvez gérer manuellement les interfaces EFA à l'aide des commandes suivantes :

1. Afficher les interfaces EFA disponibles :

   ```
   for interface in /sys/class/infiniband/*; do
       if [ ! -e "$interface/device/driver" ]; then continue; fi
       driver=$(basename "$(realpath "$interface/device/driver")")
       if [ "$driver" != "efa" ]; then continue; fi
       echo $(basename $interface)
   done
   ```

2. Afficher les interfaces actuellement configurées :

   ```
   sudo lnetctl net show
   ```

3. Ajoutez une interface EFA :

   ```
   sudo lnetctl net add --net efa --if device_name --peer-credits 32
   ```

   *device_name*Remplacez-le par un nom de périphérique réel figurant dans la liste de l'étape 1.

4. Supprimez une interface EFA :

```
sudo lnetctl net del --net efa --if device_name
```

*device_name*Remplacez-le par un nom de périphérique réel figurant dans la liste de l'étape 2.

Montage depuis Amazon Elastic Container Service

Vous pouvez accéder à votre système de fichiers FSx for Lustre depuis un conteneur Docker Amazon Elastic Container Service (Amazon ECS) sur une instance Amazon EC2. Vous pouvez le faire en utilisant l'une des options suivantes :

1. En montant votre système de fichiers FSx for Lustre à partir de l'instance Amazon EC2 qui héberge vos tâches Amazon ECS et en exportant ce point de montage vers vos conteneurs.
2. En montant le système de fichiers directement dans votre conteneur de tâches.

Pour plus d'informations sur Amazon ECS, consultez Qu'est-ce qu'Amazon Elastic Container Service ? dans le manuel Amazon Elastic Container Service Developer Guide.

Nous vous recommandons d'utiliser l'option 1 (Montage à partir d'une instance Amazon EC2 hébergeant des tâches Amazon ECS) car elle permet une meilleure utilisation des ressources, en particulier si vous démarrez de nombreux conteneurs (plus de cinq) sur la même instance EC2 ou si vos tâches sont de courte durée (moins de 5 minutes).

Utilisez l'option 2 (Montage à partir d'un conteneur Docker) si vous ne parvenez pas à configurer l'instance EC2 ou si votre application a besoin de la flexibilité du conteneur.

> **Note**
>
> Le montage FSx de Lustre sur un type de lancement AWS Fargate n'est pas pris en charge.

Les sections suivantes décrivent les procédures pour chacune des options de montage de votre système de fichiers FSx for Lustre à partir d'un conteneur Amazon ECS.

Rubriques

- Montage à partir d'une instance Amazon EC2 hébergeant des tâches Amazon ECS
- Montage à partir d'un conteneur Docker

Montage à partir d'une instance Amazon EC2 hébergeant des tâches Amazon ECS

Cette procédure explique comment configurer une instance Amazon ECS on EC2 pour monter localement votre système de fichiers FSx for Lustre. La procédure utilise `volumes` des propriétés de `mountPoints` conteneur pour partager la ressource et rendre ce système de fichiers accessible aux tâches exécutées localement. Pour plus d'informations, consultez la section Lancement d'une instance de conteneur Amazon ECS dans le manuel du développeur Amazon Elastic Container Service.

Cette procédure concerne une AMI Amazon Linux 2 optimisée pour Amazon ECS. Si vous utilisez une autre distribution Linux, consultezInstallation du Lustre client.

Pour monter votre système de fichiers depuis Amazon ECS sur une instance EC2

1. Lorsque vous lancez des instances Amazon ECS, manuellement ou à l'aide d'un groupe Auto Scaling, ajoutez les lignes de l'exemple de code suivant à la fin du champ User data. Remplacez les éléments suivants dans l'exemple :

   - Remplacez *`file_system_dns_name`* par le nom DNS réel du système de fichiers.
   - Remplacez *`mountname`* par le nom de montage du système de fichiers.
   - *`mountpoint`*Remplacez-le par le point de montage du système de fichiers, que vous devez créer.

   ```
   #!/bin/bash

   ...<existing user data>...

   fsx_dnsname=file_system_dns_name
   fsx_mountname=mountname
   fsx_mountpoint=mountpoint
   amazon-linux-extras install -y lustre
   mkdir -p "$fsx_mountpoint"
   mount -t lustre ${fsx_dnsname}@tcp:/${fsx_mountname} ${fsx_mountpoint} -o
    relatime,flock
   ```

2. Lorsque vous créez vos tâches Amazon ECS, ajoutez les propriétés suivantes `volumes` et les propriétés du `mountPoints` conteneur dans la définition JSON. *`mountpoint`*Remplacez-le par le point de montage du système de fichiers (tel que`/mnt/fsx`).

```
{
    "volumes": [
           {
                 "host": {
                      "sourcePath": "mountpoint"
                 },
                 "name": "Lustre"
           }
    ],
    "mountPoints": [
           {
                 "containerPath": "mountpoint",
                 "sourceVolume": "Lustre"
           }
    ],
}
```

Montage à partir d'un conteneur Docker

La procédure suivante montre comment configurer un conteneur de tâches Amazon ECS pour installer le `lustre-client` package et y monter votre système de fichiers FSx for Lustre. La procédure utilise une image Docker Amazon Linux (`amazonlinux`), mais une approche similaire peut fonctionner pour d'autres distributions.

Pour monter votre système de fichiers à partir d'un conteneur Docker

1. Sur votre conteneur Docker, installez le `lustre-client` package et montez votre système de fichiers FSx for Lustre avec la `command` propriété. Remplacez les éléments suivants dans l'exemple :

   - Remplacez *`file_system_dns_name`* par le nom DNS réel du système de fichiers.
   - Remplacez *`mountname`* par le nom de montage du système de fichiers.
   - Remplacez *`mountpoint`* par le point de Montage du système de fichiers.

```
"command": [
  "/bin/sh -c \"amazon-linux-extras install -y lustre; mount -t
 lustre file_system_dns_name@tcp:/mountname mountpoint -o relatime,flock;\""
```

```
],
```

2. Ajoutez `SYS_ADMIN` une fonctionnalité à votre conteneur pour l'autoriser à monter votre système de fichiers FSx for Lustre, à l'aide de la `linuxParameters` propriété.

```
"linuxParameters": {
  "capabilities": {
      "add": [
        "SYS_ADMIN"
      ]
   }
}
```

Montage de systèmes de FSx fichiers Amazon sur site ou depuis un Amazon VPC pair

Vous pouvez accéder à votre système de fichiers Amazon FSx de deux manières. L'une provient d'instances Amazon EC2 situées dans un Amazon VPC relié au VPC du système de fichiers. L'autre provient de clients locaux connectés au VPC de votre système de fichiers à l' Direct Connect aide d'un VPN.

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

Avant d'utiliser la procédure suivante, vous devez configurer une connexion d'appairage VPC ou une passerelle de transit VPC.

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

Une connexion d'appairage VPC est une connexion réseau entre deux. VPCs Ce type de connexion vous permet d'acheminer le trafic entre eux à l'aide d'adresses privées du protocole Internet version 4 (IPv4) ou du protocole Internet version 6 (IPv6). Vous pouvez utiliser le peering VPC

pour vous connecter au VPCs sein d'une même AWS région ou entre des régions. AWS Pour plus d'informations sur l'appairage VPC, consultez Qu'est-ce que l'appairage VPC ? dans le Guide d'appairage Amazon VPC.

Vous pouvez monter votre système de fichiers depuis l'extérieur de son VPC à l'aide de l'adresse IP de son interface réseau principale. L'interface réseau principale est la première interface réseau renvoyée lorsque vous exécutez la `aws fsx describe-file-systems` AWS CLI commande. Vous pouvez également obtenir cette adresse IP depuis la console de gestion Amazon Web Services.

Le tableau suivant illustre les exigences en matière d'adresse IP pour accéder aux systèmes de FSx fichiers Amazon à l'aide d'un client situé en dehors du VPC du système de fichiers.

Pour les clients situés à...	Accès aux systèmes de fichiers créés avant le 17 décembre 2020	Accès aux systèmes de fichiers créés le 17 décembre 2020 ou après cette date
Apparé à VPCs l'aide de l'appairage VPC ou AWS Transit Gateway	Clients dont les adresses IP se situent dans une plage d'adresses IP privées RFC 1918 : • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	✓
Réseaux pairés utilisant ou Direct Connect Site-to-Site VPN		✓

Si vous devez accéder à votre système de FSx fichiers Amazon créé avant le 17 décembre 2020 à l'aide d'une plage d'adresses IP non privées, vous pouvez créer un nouveau système de fichiers en restaurant une sauvegarde du système de fichiers. Pour de plus amples informations, veuillez consulter Protection de vos données grâce à des sauvegardes.

Pour récupérer l'adresse IP de l'interface réseau principale d'un système de fichiers

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, sélectionnez Systèmes de fichiers.
3. Choisissez votre système de fichiers dans le tableau de bord.
4. Sur la page de détails du système de fichiers, sélectionnez Réseau et sécurité.

5. Pour Network interface, choisissez l'ID de votre interface Elastic Network principale. Cela vous amène à la console Amazon EC2.
6. Dans l'onglet Détails, recherchez l' IPv4 adresse IP privée principale. Il s'agit de l'adresse IP de votre interface réseau principale.

> **Note**
>
> Vous ne pouvez pas utiliser la résolution de noms DNS (Domain Name System) lorsque vous montez un système de FSx fichiers Amazon en dehors du VPC auquel il est associé.

Montage automatique de votre système de FSx fichiers Amazon

Vous pouvez mettre à jour le `/etc/fstab` fichier dans votre instance Amazon EC2 après vous être connecté à l'instance pour la première fois afin qu'il monte votre système de FSx fichiers Amazon à chaque redémarrage.

Utilisation de /etc/fstab pour le montage automatique de Lustre FSx

Pour monter automatiquement le répertoire de votre système de fichiers Amazon FSx lorsque l'instance Amazon EC2 redémarre, vous pouvez utiliser le fichier. `fstab` Le fichier `fstab` contient des informations sur les systèmes de fichiers. La commande`mount -a`, qui s'exécute au démarrage de l'instance, monte les systèmes de fichiers répertoriés dans le `fstab` fichier.

> **Note**
>
> - Avant de mettre à jour le `/etc/fstab` fichier de votre instance EC2, assurez-vous d'avoir déjà créé votre système de FSx fichiers Amazon. Pour plus d'informations, reportez-vous Étape 1 : Créez votre système de fichiers FSx for Lustre à l'exercice Getting Started.
> - Pour les systèmes de fichiers compatibles EFA, la configuration de systemd est une condition préalable. Pour de plus amples informations, veuillez consulter Configuration rapide.

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

1. Connectez-vous à votre instance EC2, puis ouvrez le fichier `/etc/fstab` dans un éditeur.

2. Ajoutez la ligne suivante dans le fichier `/etc/fstab`.

   Montez le système de fichiers Amazon FSx for Lustre dans le répertoire que vous avez créé. Utilisez la commande suivante et remplacez la suivante :

   - *`/fsx`*Remplacez-le par le répertoire dans lequel vous souhaitez monter votre système de FSx fichiers Amazon.
   - Remplacez *`file_system_dns_name`* par le nom DNS réel du système de fichiers.
   - Remplacez *`mountname`* par le nom de montage du système de fichiers. Ce nom de montage est renvoyé dans la réponse à l'opération de l'`CreateFileSystem`API. Il est également renvoyé dans la réponse de la describe-file-systems AWS CLI commande et dans le fonctionnement de l'`DescribeFileSystems`API.

   Pour les systèmes de fichiers non EFA :

   ```
   file_system_dns_name@tcp:/mountname /fsx lustre defaults,relatime,flock,_netdev,x-systemd.automount,x-systemd.requires=network.service 0 0
   ```

   Pour les systèmes de fichiers compatibles avec EFA :

   ```
   file_system_dns_name@tcp:/mountname /fsx lustre defaults,relatime,flock,_netdev,x-systemd.automount,x-systemd.requires=configure-efa-fsx-lustre-client.service,x-systemd.after=configure-efa-fsx-lustre-client.service 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.

3. Enregistrez les Modifications dans le fichier.

Votre instance EC2 est désormais configurée pour monter le système de FSx fichiers Amazon à chaque redémarrage.

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

Les champs de la ligne de code que vous avez ajoutée au `/etc/fstab` fichier sont les suivants.

Champ	Description
file_system_dns_name `@tcp:/`	Le nom DNS de votre système de FSx fichiers Amazon, qui identifie le système de fichiers. Vous pouvez obtenir ce nom à partir de la console ou par programmation à partir du AWS CLI ou d'un AWS SDK.
mountname	Le nom de montage du système de fichiers. Vous pouvez obtenir ce nom à partir de la console ou par programmation à l' AWS CLI aide de la describe-file-systems commande ou de l' AWS API ou du SDK à l'aide de l'opération. `DescribeFileSystems`
/fsx	Point de montage du système de fichiers Amazon FSx sur votre instance EC2.
`lustre`	Le type de système de fichiers, Amazon FSx.
`mount options`	Options de montage pour le système de fichiers, présentées sous la forme d'une liste séparée par des virgules des options suivantes : • `defaults`— Cette valeur indique au système d'exploitation d'utiliser les options de montage par défaut. Vous pouvez répertorier les options de montage par défaut une fois le système de fichiers monté en consultant le résultat de la `mount` commande. • `relatime`— Cette option conserve les données `atime` (temps d'accès aux inodes), mais pas pour chaque accès à un fichier. Lorsque cette option est activée, les `atime` données sont écrites sur le disque uniquement si le fichier a été modifié depuis la dernière mise à jour des `atime` données (`mtime`) ou si le fichier a été consulté pour la dernière fois il y a plus d'un certain temps (un jour

Champ	Description
	par défaut). Si vous souhaitez désactiver les mises à jour de l'heure d'accès aux inodes, utilisez plutôt l'option `noatime` mount. • `flock`— monte votre système de fichiers avec le verrouillage des fichiers activé. Si vous ne souhaitez pas que le verrouillage des fichiers soit activé, utilisez plutôt l'option de `noflock` montage. • `_netdev`— La valeur indique au système d'exploitation que le système de fichiers réside sur un appareil nécessitant un 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.
`x-systemd.automount,x-systemd.requires=network.service`	Ces options pour les systèmes de fichiers non EFA garantissent que le dispositif de montage automatique ne fonctionne pas tant que la connectivité réseau n'est pas en ligne. **Note** Pour Amazon Linux 2023 et Ubuntu 22.04 et versions ultérieures, utilisez l'`x-systemd.requires=systemd-networkd-wait-online.service` option au lieu de l'`x-systemd.requires=network.service` option.
`x-systemd.automount,x-systemd.requires=configure-efa-fsx-lustre-client.service,x-systemd.after=configure-efa-fsx-lustre-client.service`	Ces options pour les systèmes de fichiers compatibles EFA garantissent que le dispositif de montage automatique ne s'exécute pas tant que la configuration du client EFA n'est pas terminée.
`0`	Valeur qui indique si le système de fichiers doit être sauvegardé pardump. Pour Amazon FSx, cette valeur doit être`0`.

Champ	Description
`0`	Valeur indiquant l'ordre dans lequel les systèmes de `fsck` fichiers sont vérifiés au démarrage. Pour les systèmes de FSx fichiers Amazon, cette valeur doit `0` indiquer qu'ils ne `fsck` doivent pas être exécutés au démarrage.

Montage de jeux de fichiers spécifiques

En utilisant la fonctionnalité de jeu Lustre de fichiers, vous ne pouvez monter qu'un sous-ensemble de l'espace de noms du système de fichiers, appelé ensemble de fichiers. Pour monter un ensemble de fichiers du système de fichiers, vous devez indiquer sur le client le chemin du sous-répertoire après le nom du système de fichiers. Le montage d'un ensemble de fichiers (également appelé montage de sous-répertoires) limite la visibilité de l'espace de noms du système de fichiers sur un client spécifique.

Exemple — Monter un ensemble de Lustre fichiers

1. Supposons que vous disposiez d'un système de fichiers FSx pour Lustre avec les répertoires suivants :

   ```
   team1/dataset1/
   team2/dataset2/
   ```

2. Vous montez uniquement le `team1/dataset1` jeu de fichiers, de sorte que seule cette partie du système de fichiers soit visible localement sur le client. Utilisez la commande suivante et remplacez les éléments suivants :

   - Remplacez *`file_system_dns_name`* par le nom DNS réel du système de fichiers.
   - Remplacez *`mountname`* par le nom de montage du système de fichiers. Ce nom de montage est renvoyé dans la réponse à l'opération de l'`CreateFileSystem`API. Il est également renvoyé dans la réponse de la describe-file-systems AWS CLI commande et dans le fonctionnement de l'DescribeFileSystemsAPI.

   ```
   mount -t lustre file_system_dns_name@tcp:/mountname/team1/dataset1 /fsx
   ```

Lorsque vous utilisez la fonctionnalité de Lustre jeu de fichiers, gardez à l'esprit les points suivants :

- Aucune contrainte n'empêche un client de remonter le système de fichiers à l'aide d'un autre jeu de fichiers, ou de ne pas le faire du tout.
- Lorsque vous utilisez un ensemble de fichiers, certaines commandes Lustre administratives nécessitant un accès au `.lustre/` répertoire peuvent ne pas fonctionner, comme la `lfs fid2path` commande.
- Si vous envisagez de monter plusieurs sous-répertoires à partir du même système de fichiers sur le même hôte, sachez que cela consomme plus de ressources qu'un seul point de montage et qu'il peut être plus efficace de monter le répertoire racine du système de fichiers une seule fois.

Pour plus d'informations sur la fonctionnalité de jeu de Lustre fichiers, consultez le manuel d'utilisation de Lustre sur le site Web de Lustre documentation.

Démontage des systèmes de fichiers

Avant de supprimer un système de fichiers FSx for Lustre, assurez-vous qu'il est démonté de toutes les instances Amazon EC2 qui l'ont monté, et avant d'arrêter ou de mettre fin à une instance Amazon EC2, assurez-vous que tous les systèmes de fichiers FSx montés pour Lustre sont démontés de cette instance.

FSx pour Lustre, les serveurs accordent des verrous de fichiers et de répertoires temporaires aux clients pendant les I/O opérations, et les clients doivent réagir rapidement lorsque les serveurs demandent aux clients de libérer leurs verrous pour débloquer I/O operations from other clients. If clients become non-responsive, they may be forcefully evicted after several minutes to allow other clients to proceed with their requested I/O des opérations. Pour éviter ces périodes d'attente, vous devez toujours démonter le système de fichiers des instances clientes avant de les arrêter ou de les arrêter, et avant de procéder à la suppression FSx pour les systèmes de fichiers Lustre.

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 FSx fichiers Amazon via AWS CLI AWS Management Console, le ou l'un des AWS SDK. Pour démonter un système de fichiers Amazon FSx connecté à une instance Amazon EC2 exécutant Linux, utilisez `umount` la commande suivante :

```
umount /mnt/fsx
```

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

Example— Identifiez l'état de montage d'un système de FSx fichiers Amazon et démontez-le

```
$ df -T
Filesystem Type 1K-blocks Used Available Use% Mounted on
file-system-id.fsx.aws-region.amazonaws.com@tcp:/mountname /fsx 3547708416 61440
 3547622400 1% /fsx
      /dev/sda1 ext4 8123812 1138920 6884644 15% /
```

```
$ umount /fsx
```

```
$ df -T
```

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

Utilisation des instances Spot Amazon EC2

FSx for Lustre peut être utilisé avec les instances Spot EC2 afin de réduire considérablement vos coûts liés à Amazon EC2. Une instance Spot est une instance EC2 non utilisée qui est disponible à un prix inférieur au prix à la demande. Amazon EC2 peut interrompre votre instance Spot lorsque le prix Spot dépasse votre prix maximum, lorsque la demande d'instances Spot augmente ou lorsque l'offre d'instances Spot diminue.

Lorsqu'Amazon EC2 interrompt une instance Spot, il communique un avis d'interruption d'instance Spot, ce qui avertit l'instance qu'Amazon EC2 va l'interrompe dans deux minutes. Pour plus d'informations, consultez la section Instances Spot dans le Guide de l'utilisateur Amazon EC2.

Pour garantir que les systèmes de fichiers Amazon FSx ne soient pas affectés par les interruptions des instances Spot EC2, nous vous recommandons de démonter les systèmes de fichiers Amazon

FSx avant de mettre fin aux instances Spot EC2 ou de les mettre en veille prolongée. Pour de plus amples informations, veuillez consulter Démontage des systèmes de fichiers.

Gestion des interruptions des instances Amazon EC2 Spot

FSx for Lustre est un système de fichiers distribué dans lequel les instances du serveur et du client coopèrent pour fournir un système de fichiers performant et fiable. Ils maintiennent un état distribué et cohérent entre les instances client et serveur. FSx pour les serveurs Lustre, déléguez des autorisations d'accès temporaires aux clients pendant qu'ils travaillent activement I/O et mettent en cache les données du système de fichiers. Les clients sont tenus de répondre dans un court laps de temps lorsque les serveurs leur demandent de révoquer leurs autorisations d'accès temporaires. Pour protéger le système de fichiers contre le mauvais comportement des clients, les serveurs peuvent expulser les Lustre clients qui ne répondent pas au bout de quelques minutes. Pour éviter d'avoir à attendre plusieurs minutes avant qu'un client ne réponde pas à la demande du serveur, il est important de démonter proprement les Lustre clients, en particulier avant de mettre fin aux instances Spot EC2.

EC2 Spot envoie des avis de résiliation 2 minutes à l'avance avant de fermer une instance. Nous vous recommandons d'automatiser le processus de démontage proprement des Lustre clients avant de mettre fin aux instances Spot EC2.

Example— Script pour démonter proprement les instances Spot EC2 résilientes

Cet exemple de script démonte proprement les instances Spot EC2 en cours de terminaison en procédant comme suit :

- Surveille les avis de résiliation de Spot.
- Lorsqu'il reçoit un avis de résiliation :
  - Arrêtez les applications qui accèdent au système de fichiers.
  - Démonte le système de fichiers avant la fermeture de l'instance.

Vous pouvez adapter le script en fonction de vos besoins, notamment pour arrêter votre application en douceur. Pour plus d'informations sur les meilleures pratiques relatives à la gestion des interruptions des instances Spot, consultez la section Meilleures pratiques pour la gestion des interruptions des instances Spot EC2.

```
#!/bin/bash
```

```
# TODO: Specify below the FSx mount point you are using
*FSXPATH=/fsx*

cd /

TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600")
if [ "$?" -ne 0 ]; then
    echo "Error running 'curl' command" >&2
    exit 1
fi

# Periodically check for termination
while sleep 5
do

    HTTP_CODE=$(curl -H "X-aws-ec2-metadata-token: $TOKEN" -s -w %{http_code} -o /dev/
null http://169.254.169.254/latest/meta-data/spot/instance-action)

    if [[ "$HTTP_CODE" -eq 401 ]] ; then
        # Refreshing Authentication Token
        TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 30")
        continue
    elif [[ "$HTTP_CODE" -ne 200 ]] ; then
        # If the return code is not 200, the instance is not going to be interrupted
        continue
    fi

    echo "Instance is getting terminated. Clean and unmount '$FSXPATH' ..."
    curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-
data/spot/instance-action
    echo

    # Gracefully stop applications accessing the filesystem
    #
    # TODO*: Replace with the proper command to stop your application if possible*

    # Kill every process still accessing Lustre filesystem
    echo "Kill every process still accessing Lustre filesystem..."
    fuser -kMm -TERM "${FSXPATH}"; sleep 2
    fuser -kMm -KILL "${FSXPATH}"; sleep 2

    # Unmount FSx For Lustre filesystem
```

```
    if ! umount -c "${FSXPATH}"; then
        echo "Error unmounting '$FSXPATH'. Processes accessing it:" >&2
        lsof "${FSXPATH}"

        echo "Retrying..."
        continue
    fi

    # Start a graceful shutdown of the host
    shutdown now

done
```

Administration des systèmes de fichiers

FSx for Lustre fournit un ensemble de fonctionnalités qui simplifient l'exécution de vos tâches administratives. Il s'agit notamment de la capacité d' point-in-timeeffectuer des sauvegardes, de gérer les quotas de stockage du système de fichiers, de gérer votre capacité de stockage et de débit, de gérer la compression des données et de définir des fenêtres de maintenance pour effectuer des correctifs logiciels de routine sur le système.

Vous pouvez administrer vos systèmes de fichiers FSx for Lustre à l'aide de l'Amazon FSx Management Console, AWS Command Line Interface (AWS CLI), de FSx l'API Amazon ou AWS SDKs.

Rubriques

- Utilisation de systèmes de fichiers compatibles avec EFA
- Utilisation Lustre quotas de stockage
- Gestion de la capacité de stockage
- Gestion du cache de lecture SSD provisionné
- Gestion des performances des métadonnées
- Gestion de la capacité de débit allouée
- Lustrecompression de données
- Lustrecourge-racine
- FSx pour l'état du système de fichiers Lustre
- Marquez vos ressources Amazon FSx for Lustre
- Fenêtres FSx de maintenance Amazon pour Lustre
- Gestion des versions de Lustre
- Suppression d’un système de fichiers

Utilisation de systèmes de fichiers compatibles avec EFA

Si vous créez un système de fichiers avec une capacité GBps de débit supérieure à 10 %, nous vous recommandons d'activer Elastic Fabric Adapter (EFA) afin d'optimiser le débit par instance client. EFA est une interface réseau haute performance qui utilise une technique de contournement du système d'exploitation personnalisée et le protocole réseau AWS Scalable Reliable Datagram (SRD) pour améliorer les performances. Pour plus d'informations sur l'EFA, consultez la section Elastic

Fabric Adapter for AI/ML and HPC workloads on Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Les systèmes de fichiers compatibles EFA prennent en charge deux fonctionnalités de performance supplémentaires : GPUDirect Storage (GDS) et ENA Express. La prise en charge du GDS s'appuie sur l'EFA pour améliorer encore les performances en permettant le transfert direct de données entre le système de fichiers et la mémoire du GPU, en contournant le processeur. Ce chemin direct élimine le besoin de copies de mémoire redondantes et l'implication du processeur dans les opérations de transfert de données. Grâce à la prise en charge de l'EFA et du GDS, vous pouvez obtenir un débit plus élevé pour les instances clientes individuelles compatibles EFA. ENA Express fournit une communication réseau optimisée pour les instances Amazon EC2 à l'aide d'un algorithme de sélection de chemin avancé et d'un mécanisme de contrôle de congestion amélioré. Grâce à la prise en charge d'ENA Express, vous pouvez obtenir un débit plus élevé pour les instances clientes individuelles compatibles ENA Express. Pour plus d'informations sur ENA Express, consultez la section Améliorer les performances du réseau entre les instances EC2 avec ENA Express dans le guide de l'utilisateur Amazon EC2.

Rubriques

- Considérations relatives à l'utilisation de systèmes de fichiers compatibles EFA
- Conditions préalables à l'utilisation de systèmes de fichiers compatibles avec EFA
- Création d'un système de fichiers compatible EFA

Considérations relatives à l'utilisation de systèmes de fichiers compatibles EFA

Voici quelques points importants à prendre en compte lors de la création de systèmes de fichiers compatibles EFA :

- Plusieurs options de connectivité : les systèmes de fichiers compatibles EFA peuvent communiquer avec les instances clientes via ENA, ENA Express et EFA.
- Type de déploiement : EFA est pris en charge sur les systèmes de fichiers Persistent 2 avec une configuration de métadonnées spécifiée, y compris les systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering.
- Mise à jour du paramètre EFA : vous pouvez choisir d'activer EFA lorsque vous créez un nouveau système de fichiers, mais vous ne pouvez pas activer ou désactiver EFA sur un système de fichiers existant.

- Adaptation du débit à la capacité de stockage : vous pouvez augmenter la capacité de stockage d'un système de fichiers SSD compatible EFA pour augmenter la capacité de débit, mais vous ne pouvez pas modifier le niveau de débit d'un système de fichiers compatible EFA.
- Régions AWS: Pour obtenir la liste des Régions AWS systèmes de fichiers Persistent 2 compatibles avec EFA, consultez. Disponibilité du type de déploiement

Conditions préalables à l'utilisation de systèmes de fichiers compatibles avec EFA

Les conditions requises pour utiliser les systèmes de fichiers compatibles EFA sont les suivantes :

Pour créer votre système de fichiers compatible avec EFA, procédez comme suit :

- Utilisez un groupe de sécurité compatible EFA. Pour de plus amples informations, veuillez consulter Groupes de sécurité compatibles avec EFA.
- Utilisez la même zone de disponibilité et le même CIDR /16 que vos instances clientes compatibles EFA au sein de votre Amazon VPC.
- Sur les systèmes de fichiers à hiérarchisation intelligente, l'EFA n'est pris en charge qu'avec une capacité de débit de 4 000 MBps ou par incréments de 4 000. MBps

Pour accéder à votre système de fichiers à l'aide d'Elastic Fabric Adapter (EFA) :

- Utilisez des instances EC2 Nitro v4 (ou supérieures) qui prennent en charge l'EFA, à l'exception de la famille d'instances trn2. Consultez la section Types d'instances pris en charge dans le guide de l'utilisateur Amazon EC2.
- Exécutez AL2023, RHEL 9.5 et versions ultérieures, ou Ubuntu 22+ avec la version 6.8 ou ultérieure du noyau. Pour de plus amples informations, veuillez consulter Installation du Lustre client.
- Installez les modules EFA et configurez les interfaces EFA sur vos instances clientes. Pour de plus amples informations, veuillez consulter Configuration des clients EFA.

Pour accéder à votre système de fichiers à l'aide du GPUDirect stockage (GDS) :

- Utilisez une instance client Amazon EC2 P5, P5e, P5en ou P6-B200.

- Installez le package NVIDIA Compute Unified Device Architecture (CUDA), le pilote NVIDIA open source et le pilote de GPUDirect stockage NVIDIA sur votre instance cliente. Pour de plus amples informations, veuillez consulter Installez le pilote GDS (facultatif).

Pour accéder à votre système de fichiers à l'aide d'ENA Express :

- Utilisez des instances Amazon EC2 compatibles avec ENA Express. Consultez la section Types d'instances pris en charge pour ENA Express dans le guide de l'utilisateur Amazon EC2.
- Mettez à jour les paramètres de votre instance Linux. Consultez la section Conditions requises pour les instances Linux dans le guide de l'utilisateur Amazon EC2.
- Activez ENA Express sur les interfaces réseau de vos instances clientes. Pour plus de détails, consultez la section Vérifier les paramètres ENA Express de votre instance EC2 dans le guide de l'utilisateur Amazon EC2.

Création d'un système de fichiers compatible EFA

Cette section contient des instructions sur la façon de créer un système FSx de fichiers compatible avec Lustre EFA à l'aide du. AWS CLI Pour plus d'informations sur la création d'un système de fichiers compatible EFA à l'aide de la FSx console Amazon, consultez. Étape 1 : Créez votre système de fichiers FSx for Lustre

Pour créer un système de fichiers compatible EFA (CLI)

Utilisez la commande create-file-systemCLI (ou l'opération CreateFileSystemAPI équivalente). L'exemple suivant crée un système de fichiers compatible FSx pour Lustre EFA avec un `PERSISTENT_2` type de déploiement.

```
aws fsx create-file-system\
   --storage-capacity 4800 \
   --storage-type SSD \
   --file-system-type LUSTRE \
   --file-system-type-version 2.15 \
   --subnet-ids subnet-01234567890 \
   --security-group-ids sg-0123456789abcdefg \
   --lustre-configuration '{"DeploymentType": "PERSISTENT_2", "EfaSupport": true}'
```

Après avoir créé le système de fichiers avec succès, Amazon FSx renvoie la description du système de fichiers au format JSON.

Utilisation Lustre quotas de stockage

Vous pouvez créer des quotas de stockage pour les utilisateurs, les groupes et les projets sur FSx les systèmes de fichiers Lustre. Les quotas de stockage vous permettent de limiter la quantité d'espace disque et le nombre de fichiers qu'un utilisateur, un groupe ou un projet peut consommer. Les quotas de stockage suivent automatiquement l'utilisation au niveau de l'utilisateur, au niveau du groupe et au niveau du projet afin que vous puissiez surveiller la consommation, que vous choisissiez ou non de définir des limites de stockage.

Amazon FSx applique les quotas et empêche les utilisateurs qui les ont dépassés d'écrire sur l'espace de stockage. Lorsque les utilisateurs dépassent leur quota, ils doivent supprimer suffisamment de fichiers pour atteindre les limites du quota afin de pouvoir à nouveau écrire dans le système de fichiers.

Rubriques

- Application des quotas
- Types de quotas
- Limites de quotas et délais de grâce
- Définition et affichage des quotas
- Quotas et compartiments liés à Amazon S3
- Quotas et restauration des sauvegardes

Application des quotas

L'application des quotas par utilisateur, groupe et projet est automatiquement activée sur tous FSx les systèmes de fichiers Lustre. Vous ne pouvez pas désactiver l'application des quotas.

Types de quotas

Les administrateurs système disposant des informations d'identification de l'utilisateur root du AWS compte peuvent créer les types de quotas suivants :

- Un quota d'utilisateurs s'applique à un utilisateur individuel. Un quota d'utilisateurs pour un utilisateur spécifique peut être différent de celui des autres utilisateurs.
- Un quota de groupe s'applique à tous les utilisateurs membres d'un groupe spécifique.

- Un quota de projet s'applique à tous les fichiers ou répertoires associés à un projet. Un projet peut inclure plusieurs répertoires ou des fichiers individuels situés dans différents répertoires d'un système de fichiers.

  > **Note**
  >
  > Les quotas de projet ne sont pris en charge que sur Lustre version 2.15 activée FSx pour les systèmes de fichiers Lustre.

- Un quota de blocs limite la quantité d'espace disque qu'un utilisateur, un groupe ou un projet peut utiliser. Vous configurez la taille de stockage en kilo-octets.
- Un quota d'inodes limite le nombre de fichiers ou de répertoires qu'un utilisateur, un groupe ou un projet peut créer. Vous configurez le nombre maximum d'inodes sous forme d'entier.

> **Note**
>
> Les quotas par défaut ne sont pas pris en charge.

Si vous définissez des quotas pour un utilisateur et un groupe particuliers, et que l'utilisateur est membre de ce groupe, l'utilisation des données de l'utilisateur s'applique aux deux quotas. Il est également limité par les deux quotas. Si l'une des limites de quota est atteinte, l'utilisateur n'est pas autorisé à écrire dans le système de fichiers.

> **Note**
>
> Les quotas définis pour l'utilisateur root ne sont pas appliqués. De même, l'écriture de données en tant qu'utilisateur root à l'aide de la `sudo` commande contourne l'application du quota.

Limites de quotas et délais de grâce

Amazon FSx applique les quotas d'utilisateurs, de groupes et de projets sous forme de limite stricte ou de limite souple avec une période de grâce configurable.

La limite stricte est la limite absolue. Si les utilisateurs dépassent leur limite stricte, l'allocation d'un bloc ou d'un inode échoue avec un message indiquant que le quota de disque est dépassé. Les

utilisateurs qui ont atteint la limite stricte de leur quota doivent supprimer suffisamment de fichiers ou de répertoires pour passer sous le quota avant de pouvoir à nouveau écrire dans le système de fichiers. Lorsqu'une période de grâce est définie, les utilisateurs peuvent dépasser la limite souple pendant la période de grâce s'ils sont inférieurs à la limite stricte.

Pour les limites souples, vous configurez un délai de grâce en secondes. La limite souple doit être inférieure à la limite stricte.

Vous pouvez définir différentes périodes de grâce pour les quotas d'inodes et de blocs. Vous pouvez également définir différentes périodes de grâce pour un quota d'utilisateurs, un quota de groupe et un quota de projet. Lorsque les quotas d'utilisateurs, de groupes et de projets ont des périodes de grâce différentes, la limite souple se transforme en limite stricte une fois la période de grâce de l'un de ces quotas expirée.

Lorsque les utilisateurs dépassent une limite souple, Amazon leur FSx permet de continuer à dépasser leur quota jusqu'à l'expiration du délai de grâce ou jusqu'à ce que la limite stricte soit atteinte. À la fin de la période de grâce, la limite souple est convertie en limite stricte, et les utilisateurs sont empêchés de poursuivre leurs opérations d'écriture jusqu'à ce que leur utilisation du stockage revienne en dessous du quota de blocs ou des limites de quota d'inode définies. Les utilisateurs ne reçoivent aucune notification ni aucun avertissement lorsque le délai de grâce commence.

Définition et affichage des quotas

Vous définissez des quotas de stockage à l'aide de Lustre `lfs`commandes du système de fichiers dans votre terminal Linux. La `lfs setquota` commande définit les limites de quota et affiche les `lfs quota` informations relatives aux quotas.

Pour plus d'informations sur Lustre commandes de quota, consultez le manuel d'utilisation de Lustre sur Lustre site Web de documentation.

Définition des quotas d'utilisateurs, de groupes et de projets

La syntaxe de la `setquota` commande permettant de définir les quotas d'utilisateur, de groupe ou de projet est la suivante.

```
lfs setquota {-u|--user|-g|--group|-p|--project} username|groupname|projectid
             [-b block_softlimit] [-B block_hardlimit]
             [-i inode_softlimit] [-I inode_hardlimit]
             /mount_point
```

Où :

- `-u`ou `--user` indique un utilisateur pour lequel définir un quota.
- `-g`ou `--group` indique un groupe pour lequel définir un quota.
- `-p`ou `--project` indique un projet pour lequel définir un quota.
- `-b`définit un quota de blocs avec une limite souple. `-B`définit un quota de blocs avec une limite stricte. Les deux *`block_softlimit`* *`block_hardlimit`* sont exprimés en kilo-octets, et la valeur minimale est de 1024 Ko.
- `-i`définit un quota d'inodes avec une limite souple. `-I`définit un quota d'inodes avec une limite stricte. Les deux *`inode_softlimit`* *`inode_hardlimit`* sont exprimés en nombre d'inodes, et la valeur minimale est de 1024 inodes.
- *`mount_point`*est le répertoire dans lequel le système de fichiers a été monté.

Exemple de quota utilisateur : la commande suivante définit une limite de blocs souples de 5 000 Ko, une limite de blocs fixes de 8 000 Ko, une limite d'inodes souples de 2 000 et un quota de limite de 3 000 inodes durs pour le système de fichiers `user1` sur lequel est monté le système de fichiers. `/mnt/fsx`

```
sudo lfs setquota -u user1 -b 5000 -B 8000 -i 2000 -I 3000 /mnt/fsx
```

Exemple de quota de groupe : la commande suivante définit une limite de blocs fixes de 100 000 Ko pour le groupe nommé `group1` sur le système de fichiers sur lequel le système de fichiers est monté`/mnt/fsx`.

```
sudo lfs setquota -g group1 -B 100000 /mnt/fsx
```

Exemple de quota de projet : assurez-vous d'abord que vous avez utilisé la `project` commande pour associer les fichiers et répertoires souhaités au projet. Par exemple, la commande suivante associe tous les fichiers et sous-répertoires du `/mnt/fsxfs/dir1` répertoire au projet dont l'ID de projet est`100`.

```
sudo lfs project -p 100 -r -s /mnt/fsxfs/dir1
```

Utilisez ensuite la `setquota` commande pour définir le quota du projet. La commande suivante définit une limite de bloc souple de 307 200 Ko, une limite de bloc rigide de 309 200 Ko, une limite de

10 000 inodes souples et un quota de 11 000 inodes durs pour le projet sur le système de fichiers sur lequel est monté le projet250. /mnt/fsx

```
sudo lfs setquota -p 250 -b 307200 -B 309200 -i 10000 -I 11000 /mnt/fsx
```

Définition des délais de grâce

Le délai de grâce par défaut est d'une semaine. Vous pouvez ajuster le délai de grâce par défaut pour les utilisateurs, les groupes ou les projets à l'aide de la syntaxe suivante.

```
lfs setquota -t {-u|-g|-p}
             [-b block_grace]
             [-i inode_grace]
             /mount_point
```

Où :

- `-t`indique qu'un délai de grâce sera défini.
- `-u`définit un délai de grâce pour tous les utilisateurs.
- `-g`définit un délai de grâce pour tous les groupes.
- `-p`fixe un délai de grâce pour tous les projets.
- `-b`définit un délai de grâce pour les quotas par bloc. `-i`définit un délai de grâce pour les quotas d'inodes. Les deux *`block_grace`* *`inode_grace`* sont exprimés en secondes entières ou au `XXwXXdXXhXXmXXs` format.
- *`mount_point`*est le répertoire dans lequel le système de fichiers a été monté.

La commande suivante définit des périodes de grâce de 1 000 secondes pour les quotas de blocage des utilisateurs et de 1 semaine et 4 jours pour les quotas d'inode des utilisateurs.

```
sudo lfs setquota -t -u -b 1000 -i 1w4d /mnt/fsx
```

Afficher les quotas

La `quota` commande affiche des informations sur les quotas d'utilisateurs, les quotas de groupe, les quotas de projet et les périodes de grâce.

Afficher la commande de quota	Informations sur les quotas affichées
`lfs quota /mount_point`	Informations générales sur les quotas (utilisation du disque et limites) pour l'utilisateur exécutant la commande et le groupe principal de l'utilisateur.
`lfs quota -u username /mount_point`	Informations générales sur les quotas pour un utilisateur spécifique. Les utilisateurs disposant des informations d'identification utilisateur root du AWS compte peuvent exécuter cette commande pour n'importe quel utilisateur, mais les utilisateurs non root ne peuvent pas exécuter cette commande pour obtenir des informations sur les quotas d'autres utilisateurs.
`lfs quota -u username -v /mount_point`	Informations générales sur les quotas pour un utilisateur spécifique et statistiques détaillées sur les quotas pour chaque cible de stockage d'objets (OST) et cible de métadonnées (MDT). Les utilisateurs disposant des informations d'identification utilisateur root du AWS compte peuvent exécuter cette commande pour n'importe quel utilisateur, mais les

Afficher la commande de quota	Informations sur les quotas affichées
	utilisateurs non root ne peuvent pas exécuter cette commande pour obtenir des informations sur les quotas d'autres utilisateurs.
`lfs quota -g groupname /mount_point`	Informations générales sur les quotas pour un groupe spécifique.
`lfs quota -p projectid /mount_point`	Informations générales sur les quotas pour un projet spécifiqu e.
`lfs quota -t -u /mount_point`	Bloquez et annulez les délais de grâce pour les quotas d'utilisateurs.
`lfs quota -t -g /mount_point`	Bloquez et annulez les délais de grâce pour les quotas de groupe.
`lfs quota -t -p /mount_point`	Bloquez et annulez les délais de grâce pour les quotas de projet.

Quotas et compartiments liés à Amazon S3

Vous pouvez lier votre système de fichiers FSx for Lustre à un référentiel de données Amazon S3. Pour de plus amples informations, veuillez consulter Lier votre système de fichiers à un compartiment Amazon S3.

Vous pouvez éventuellement choisir un dossier ou un préfixe spécifique dans un compartiment S3 lié comme chemin d'importation vers votre système de fichiers. Lorsqu'un dossier dans Amazon S3 est spécifié et importé dans votre système de fichiers depuis S3, seules les données de ce dossier sont

prises en compte dans le quota. Les données de l'ensemble du bucket ne sont pas prises en compte dans les limites du quota.

Les métadonnées des fichiers d'un compartiment S3 lié sont importées dans un dossier dont la structure correspond au dossier importé depuis Amazon S3. Ces fichiers sont pris en compte dans les quotas d'inodes des utilisateurs et des groupes propriétaires des fichiers.

Lorsqu'un utilisateur effectue un chargement `hsm_restore` différé ou qu'il charge un fichier, la taille totale du fichier est prise en compte dans le quota de blocs associé au propriétaire du fichier. Par exemple, si l'utilisateur A charge paresseusement un fichier appartenant à l'utilisateur B, la quantité de stockage et l'utilisation des inodes sont prises en compte dans le quota de l'utilisateur B. De même, lorsqu'un utilisateur utilise l' FSx API Amazon pour publier un fichier, les données sont libérées des quotas de bloc de l'utilisateur ou du groupe propriétaire du fichier.

Comme les restaurations HSM et le chargement différé sont effectués avec un accès root, ils contournent l'application des quotas. Une fois les données importées, elles sont comptabilisées pour l'utilisateur ou le groupe en fonction de la propriété définie dans S3, ce qui peut amener les utilisateurs ou les groupes à dépasser leurs limites de blocage. Dans ce cas, ils devront libérer des fichiers pour pouvoir à nouveau écrire dans le système de fichiers.

De même, les systèmes de fichiers sur lesquels l'importation automatique est activée créeront automatiquement de nouveaux inodes pour les objets ajoutés à S3. Ces nouveaux inodes sont créés avec un accès root et contournent l'application des quotas lors de leur création. Ces nouveaux inodes seront pris en compte dans le calcul des utilisateurs et des groupes, en fonction du propriétaire de l'objet dans S3. Si ces utilisateurs et groupes dépassent leurs quotas d'inodes en fonction de l'activité d'importation automatique, ils devront supprimer des fichiers afin de libérer de la capacité supplémentaire et de dépasser leurs limites de quota.

Quotas et restauration des sauvegardes

Lorsque vous restaurez une sauvegarde, les paramètres de quota du système de fichiers d'origine sont implémentés dans le système de fichiers restauré. Par exemple, si des quotas sont définis dans le système de fichiers A et que le système de fichiers B est créé à partir d'une sauvegarde du système de fichiers A, les quotas du système de fichiers A sont appliqués dans le système de fichiers B.

Gestion de la capacité de stockage

Vous pouvez augmenter la capacité de stockage SSD ou HDD configurée sur votre système de fichiers FSx for Lustre si vous avez besoin de stockage et de débit supplémentaires. Comme le débit d'un système de fichiers FSx pour Lustre évolue de manière linéaire avec la capacité de stockage, vous bénéficiez également d'une augmentation comparable de la capacité de débit. Pour augmenter la capacité de stockage, vous pouvez utiliser la FSx console Amazon, le AWS Command Line Interface (AWS CLI) ou l' FSx API Amazon.

Lorsque vous demandez une mise à jour de la capacité de stockage de votre système de fichiers, Amazon ajoute FSx automatiquement de nouveaux serveurs de fichiers réseau et adapte votre serveur de métadonnées. Lors de l'augmentation de la capacité de stockage, le système de fichiers peut être indisponible pendant quelques minutes. Les opérations sur les fichiers effectuées par les clients alors que le système de fichiers n'est pas disponible seront réessayées de manière transparente et finiront par réussir une fois le dimensionnement du stockage terminé. Lorsque le système de fichiers n'est pas disponible, l'état du système de fichiers est défini sur`UPDATING`. Une fois le dimensionnement du stockage terminé, l'état du système de fichiers est défini sur`AVAILABLE`.

Amazon exécute FSx ensuite un processus d'optimisation du stockage qui rééquilibre de manière transparente les données entre les serveurs de fichiers existants et récemment ajoutés. Le rééquilibrage est effectué en arrière-plan sans impact sur la disponibilité du système de fichiers. Lors du rééquilibrage, vous pouvez constater une baisse des performances du système de fichiers car les ressources sont consommées pour le déplacement des données. Pour la plupart des systèmes de fichiers, l'optimisation du stockage prend de quelques heures à quelques jours. Vous pouvez accéder à votre système de fichiers et l'utiliser pendant la phase d'optimisation.

Vous pouvez suivre la progression de l'optimisation du stockage à tout moment à l'aide de la FSx console, de la CLI et de l'API Amazon. Pour de plus amples informations, veuillez consulter Surveillance de l'augmentation de la capacité de stockage.

Rubriques

- Considérations relatives à l'augmentation de la capacité de stockage
- Quand augmenter la capacité de stockage
- Comment le dimensionnement du stockage et les demandes de sauvegarde simultanés sont gérés
- Augmenter la capacité de stockage
- Surveillance de l'augmentation de la capacité de stockage

Considérations relatives à l'augmentation de la capacité de stockage

Voici quelques points importants à prendre en compte lors de l'augmentation de la capacité de stockage :

- Augmenter uniquement : vous pouvez uniquement augmenter la capacité de stockage d'un système de fichiers ; vous ne pouvez pas diminuer la capacité de stockage.
- Augmenter les incréments : lorsque vous augmentez la capacité de stockage, utilisez les incréments répertoriés dans la boîte de dialogue Augmenter la capacité de stockage.
- Délai entre les augmentations : vous ne pouvez pas augmenter davantage la capacité de stockage d'un système de fichiers jusqu'à 6 heures après la dernière demande d'augmentation.
- Capacité de débit — Vous augmentez automatiquement la capacité de débit lorsque vous augmentez la capacité de stockage. Pour les systèmes de fichiers HDD persistants dotés d'un cache SSD, la capacité de stockage du cache de lecture est également augmentée de la même manière afin de conserver un cache SSD dimensionné à 20 % de la capacité de stockage du disque dur. Amazon FSx calcule les nouvelles valeurs pour les unités de capacité de stockage et de débit et les répertorie dans la boîte de dialogue Augmenter la capacité de stockage.

  > **Note**
  >
  > Vous pouvez modifier indépendamment la capacité de débit d'un système de fichiers SSD persistant sans avoir à mettre à jour la capacité de stockage du système de fichiers. Pour de plus amples informations, veuillez consulter Gestion de la capacité de débit allouée.

- Type de déploiement : vous pouvez augmenter la capacité de stockage de tous les types de déploiement, à l'exception des systèmes de fichiers Scratch 1.

Quand augmenter la capacité de stockage

Augmentez la capacité de stockage de votre système de fichiers lorsque la capacité de stockage disponible est insuffisante. Utilisez cette `FreeStorageCapacity` CloudWatch métrique pour contrôler la quantité de stockage gratuit disponible sur le système de fichiers. Vous pouvez créer une CloudWatch alarme Amazon sur cette métrique et être averti lorsqu'elle tombe en dessous d'un seuil spécifique. Pour de plus amples informations, veuillez consulter Surveillance avec Amazon CloudWatch.

Vous pouvez utiliser CloudWatch des métriques pour surveiller les niveaux d'utilisation continue du débit de votre système de fichiers. Si vous déterminez que votre système de fichiers a besoin d'une capacité de débit supérieure, vous pouvez utiliser les informations métriques pour vous aider à déterminer dans quelle mesure augmenter la capacité de stockage. Pour plus d'informations sur la manière de déterminer le débit actuel de votre système de fichiers, consultezComment utiliser les CloudWatch métriques Amazon FSx for Lustre. Pour plus d'informations sur l'impact de la capacité de stockage sur la capacité de débit, consultezAmazon FSx pour les performances de Lustre.

Vous pouvez également consulter la capacité de stockage et le débit total de votre système de fichiers dans le panneau Résumé de la page de détails du système de fichiers.

Comment le dimensionnement du stockage et les demandes de sauvegarde simultanés sont gérés

Vous pouvez demander une sauvegarde juste avant le début d'un flux de travail de dimensionnement du stockage ou pendant qu'il est en cours. La séquence dans laquelle Amazon FSx traite les deux demandes est la suivante :

- Si un flux de travail de dimensionnement du stockage est en cours (l'état du dimensionnement du stockage est défini `IN_PROGRESS` et l'état du système de fichiers l'est`UPDATING`) et que vous demandez une sauvegarde, la demande de sauvegarde est mise en file d'attente. La tâche de sauvegarde est lancée lorsque le dimensionnement du stockage est en phase d'optimisation du stockage (l'état du dimensionnement du stockage est `UPDATED_OPTIMIZING` celui du système de fichiers`AVAILABLE`).
- Si la sauvegarde est en cours (l'état de la sauvegarde est définie`CREATING`) et que vous demandez un dimensionnement du stockage, la demande de dimensionnement du stockage est mise en file d'attente. Le flux de travail de dimensionnement du stockage démarre lorsqu'Amazon FSx transfère la sauvegarde vers Amazon S3 (le statut de la sauvegarde est`TRANSFERRING`).

Si une demande de dimensionnement du stockage est en attente et qu'une demande de sauvegarde du système de fichiers est également en attente, la priorité de la tâche de sauvegarde est plus élevée. La tâche de dimensionnement du stockage ne démarre pas tant que la tâche de sauvegarde n'est pas terminée.

Augmenter la capacité de stockage

Vous pouvez augmenter la capacité de stockage d'un système de fichiers à l'aide de la FSx console Amazon AWS CLI, de ou de l' FSx API Amazon.

Pour augmenter la capacité de stockage d'un système de fichiers (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de Lustre fichiers pour lequel vous souhaitez augmenter la capacité de stockage.
3. Pour Actions, choisissez Mettre à jour la capacité de stockage. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté de la capacité de stockage du système de fichiers pour afficher la boîte de dialogue Augmenter la capacité de stockage.
4. Pour la capacité de stockage souhaitée, fournissez une nouvelle capacité de stockage en GiB supérieure à la capacité de stockage actuelle du système de fichiers :

   - Pour un SSD persistant ou un système de fichiers Scratch 2, cette valeur doit être exprimée en multiples de 2 400 GiB.
   - Pour un système de fichiers HDD persistant, cette valeur doit être exprimée en multiples de 6 000 GiB pour 12 systèmes de MBps/TiB fichiers et de 1 800 GiB pour les systèmes de fichiers MBps 40/TiB.
   - Pour un système de fichiers compatible EFA, cette valeur doit être exprimée en multiples de 38400 GiB pour 125 systèmes de fichiers, de 19200 GiB pour 250 systèmes de MBps/TiB fichiers, de multiples de 9600 GiB pour 500 MBps/TiB systèmes de fichiers et de multiples de 4800 GiB pour 1 000 systèmes de MBps/TiB fichiers. MBps/TiB

   > **Note**
   >
   > Vous ne pouvez pas augmenter la capacité de stockage des systèmes de fichiers Scratch 1.

5. Choisissez Mettre à jour pour lancer la mise à jour de la capacité de stockage.
6. Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers dans l'onglet Mises à jour.

Pour augmenter la capacité de stockage d'un système de fichiers (CLI)

1. Pour augmenter la capacité de stockage d'un système de fichiers FSx pour Lustre, utilisez la AWS CLI commande update-file-system. Définissez les paramètres suivants :

   Définissez `--file-system-id` l'ID du système de fichiers que vous mettez à jour.

`--storage-capacity`Défini sur une valeur entière correspondant au montant, en GiB, de l'augmentation de la capacité de stockage. Pour un SSD persistant ou un système de fichiers Scratch 2, cette valeur doit être exprimée en multiples de 2 400. Pour un système de fichiers HDD persistant, cette valeur doit être exprimée en multiples de 6 000 pour 12 systèmes de MBps/TiB fichiers et de 1 800 pour 40 systèmes de MBps/TiB fichiers. La nouvelle valeur cible doit être supérieure à la capacité de stockage actuelle du système de fichiers.

Cette commande spécifie une valeur cible de capacité de stockage de 9 600 GiB pour un SSD persistant ou un système de fichiers Scratch 2.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --storage-capacity 9600
```

2. Vous pouvez suivre la progression de la mise à jour à l'aide de la AWS CLI commande describe-file-systems. Recherchez le `administrative-actions` dans la sortie.

   Pour de plus amples informations, veuillez consulter AdministrativeAction.

Surveillance de l'augmentation de la capacité de stockage

Vous pouvez suivre la progression d'une augmentation de capacité de stockage à l'aide de la FSx console Amazon, de l'API ou du AWS CLI.

Surveillance des augmentations dans la console

Dans l'onglet Mises à jour de la page de détails du système de fichiers, vous pouvez consulter les 10 mises à jour les plus récentes pour chaque type de mise à jour.

Vous pouvez consulter les informations suivantes :

Type de mise à jour

Les types pris en charge sont la capacité de stockage et l'optimisation du stockage.

Valeur cible

La valeur souhaitée pour mettre à jour la capacité de stockage du système de fichiers.

Statut

L'état actuel de la capacité de stockage est mis à jour. Les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon traite FSx la demande de mise à jour.
- Mise à jour ; optimisation — Amazon FSx a augmenté la capacité de stockage du système de fichiers. Le processus d'optimisation du stockage rééquilibre désormais les données entre les serveurs de fichiers.
- Terminé — L'augmentation de la capacité de stockage s'est terminée avec succès.
- Échec — L'augmentation de la capacité de stockage a échoué. Choisissez le point d'interrogation (?) pour connaître les raisons de l'échec de la mise à jour du stockage.

% de progression

Affiche la progression du processus d'optimisation du stockage sous forme de pourcentage d'achèvement.

Heure de la demande

Heure à laquelle Amazon FSx a reçu la demande d'action de mise à jour.

La surveillance des augmentations avec l'API AWS CLI and

Vous pouvez afficher et surveiller les demandes d'augmentation de la capacité de stockage du système de fichiers à l'aide de la describe-file-systems AWS CLI commande et de l'action de l'DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous augmentez la capacité de stockage d'un système de fichiers, deux `AdministrativeActions` sont générés : une action `FILE_SYSTEM_UPDATE` et une `STORAGE_OPTIMIZATION` action.

L'exemple suivant montre un extrait de la réponse d'une commande describe-file-systems CLI. Le système de fichiers a une capacité de stockage de 4 800 Go, et une action administrative est en cours pour augmenter la capacité de stockage à 9 600 Go.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 4800,
```

```
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 9600
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "PENDING",
                }
            ]
```

Amazon FSx exécute `FILE_SYSTEM_UPDATE` d'abord l'action en ajoutant de nouveaux serveurs de fichiers au système de fichiers. Lorsque le nouveau stockage est disponible pour le système de fichiers, l'`FILE_SYSTEM_UPDATE`état passe à`UPDATED_OPTIMIZING`. La capacité de stockage indique la nouvelle valeur supérieure, et Amazon FSx commence à traiter l'action `STORAGE_OPTIMIZATION` administrative. Cela est illustré dans l'extrait suivant de la réponse d'une commande describe-file-systems CLI.

La `ProgressPercent` propriété affiche la progression du processus d'optimisation du stockage. Une fois le processus d'optimisation du stockage terminé avec succès, le statut de l'`FILE_SYSTEM_UPDATE`action passe à`COMPLETED`, et l'`STORAGE_OPTIMIZATION`action n'apparaît plus.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 9600,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
```

```
                    "StorageCapacity": 9600
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

Si l'augmentation de la capacité de stockage échoue, le statut de l'`FILE_SYSTEM_UPDATE`action passe à`FAILED`. La `FailureDetails` propriété fournit des informations sur l'échec, comme indiqué dans l'exemple suivant.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 4800,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 9600
                }
            ]
```

Gestion du cache de lecture SSD provisionné

Lorsque vous créez un système de fichiers avec la classe de stockage Intelligent-Tiering, vous avez également la possibilité de fournir un cache de lecture SSD qui fournit des latences SSD pour les lectures de vos données fréquemment consultées, jusqu'à 3 IOPS par GiB.

Vous pouvez configurer le cache de lecture de votre SSD pour les données fréquemment consultées à l'aide de l'une des options de mode de dimensionnement suivantes :

- Automatique (proportionnel à la capacité de débit). Avec Automatic, Amazon FSx for Lustre sélectionne automatiquement la taille du cache de lecture des données SSD en fonction de la capacité de débit allouée.
- Personnalisé (fourni par l'utilisateur). Avec Custom, vous pouvez personnaliser la taille du cache de lecture de votre SSD et l'augmenter ou le réduire à tout moment en fonction des besoins de votre charge de travail.
- Choisissez No Cache si vous ne souhaitez pas utiliser de cache de lecture de données SSD avec votre système de fichiers.

En mode automatique (proportionnel à la capacité de débit), Amazon provisionne FSx automatiquement la taille de cache de lecture par défaut suivante en fonction de la capacité de débit de votre système de fichiers.

Capacité de débit allouée () MBps	Cache de lecture SSD en mode automatique (proportionnel à la capacité de débit) (GiB)	Taille du cache de lecture SSD prise en charge	
		minimum (GiB)	maximum (GiB)
Tous les 4 000	20 000	32	131072

Une fois votre système de fichiers créé, vous pouvez modifier le mode de dimensionnement et la capacité de stockage de votre cache de lecture à tout moment.

Rubriques

- Considérations relatives à la mise à jour du cache de lecture SSD
- Mettre à jour le cache de lecture d'un SSD provisionné
- Surveillance des mises à jour du cache de lecture du SSD

Considérations relatives à la mise à jour du cache de lecture SSD

Voici quelques points importants à prendre en compte lors de la modification du cache de lecture des données de votre SSD :

- Chaque fois que vous modifiez le cache de lecture du SSD, tout son contenu est effacé. Cela signifie que vous pouvez constater une baisse des niveaux de performance jusqu'à ce que le cache de lecture du SSD soit à nouveau rempli.
- Vous pouvez augmenter ou diminuer la capacité du cache de lecture d'un SSD. Cependant, vous ne pouvez le faire qu'une fois toutes les six heures. Il n'y a aucune limite de temps lors de l'ajout ou de la suppression d'un cache de lecture SSD dans votre système de fichiers.
- Vous devez augmenter ou diminuer la taille du cache de lecture de votre SSD d'au moins 10 % chaque fois que vous le modifiez.

Mettre à jour le cache de lecture d'un SSD provisionné

Vous pouvez mettre à jour le cache de lecture des données de votre SSD à l'aide de la FSx console Amazon AWS CLI, de l'API Amazon ou de l' FSx API Amazon.

Pour mettre à jour le cache de lecture SSD pour un système de fichiers à hiérarchisation intelligente (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers. Dans la liste des systèmes de fichiers, choisissez le système de fichiers Lustre FSx pour lequel vous souhaitez mettre à jour le cache de lecture SSD.
3. SSD Dans le panneau récapitulatif, choisissez Mettre à jour à côté de la valeur du cache de lecture SSD du système de fichiers.

La boîte de dialogue Mettre à jour le cache de lecture SSD apparaît.

4. Sélectionnez le nouveau mode de dimensionnement que vous souhaitez pour votre cache de lecture de données, comme suit :

   - Choisissez Automatique (proportionnel à la capacité de débit) pour que votre cache de lecture de données soit automatiquement dimensionné en fonction de votre capacité de débit.
   - Choisissez Personnalisé (fourni par l'utilisateur) si vous connaissez la taille approximative de votre ensemble de données et souhaitez personnaliser votre cache de lecture des données. Si vous sélectionnez Personnalisé, vous devez également spécifier la capacité de cache de lecture souhaitée en GiB.
   - Choisissez Aucun si vous ne souhaitez pas utiliser de cache de lecture de données SSD avec votre système de fichiers Intelligent-Tiering.

5. Choisissez Mettre à jour.

Pour mettre à jour le cache de lecture SSD pour un système de fichiers à hiérarchisation intelligente (CLI)

Pour mettre à jour le cache de lecture des données SSD pour un système de fichiers à hiérarchisation intelligente, utilisez la AWS CLI commande update-file-systemou l'action API équivalente UpdateFileSystem . Définissez les paramètres suivants :

- `--file-system-id`Défini sur l'ID du système de fichiers que vous mettez à jour.
- Pour modifier le cache de lecture de votre SSD, utilisez la `--lustre-configuration` `DataReadCacheConfiguration` propriété. Cette propriété comporte deux paramètres, à `SizeGiB` savoir `SizingMode` :
  - SizeGiB - Définit la taille du cache de lecture de votre SSD en GiB lors de l'utilisation `USER_PROVISIONED` du mode.
  - SizingMode- Définit le mode de dimensionnement du cache de lecture de votre SSD.
    - Définissez cette valeur `NO_CACHE` si vous ne souhaitez pas utiliser de cache de lecture SSD avec votre système de fichiers Intelligent-Tiering.
    - Réglez sur `USER_PROVISIONED` pour spécifier la taille exacte du cache de lecture de votre SSD.
    - Configurez `PROPORTIONAL_TO_THROUGHPUT_CAPACITY` pour que le cache de lecture des données de votre SSD soit automatiquement dimensionné en fonction de votre capacité de débit.

L'exemple suivant met à jour le cache de lecture SSD en `USER_PROVISIONED` mode et définit la taille à 524288 GiB.

```
aws fsx update-file-system \
   --file-system-id fs-0123456789abcdef0 \
   --lustre-configuration
 'DataReadCacheConfiguration={SizeGiB=524288,SizingMode=USER_PROVISIONED}'
```

Pour suivre la progression de la mise à jour, utilisez la describe-file-systems AWS CLI commande. Recherchez la `AdministrativeActions` section dans le résultat.

Pour plus d'informations, consultez AdministrativeActionle Amazon FSx API Reference.

Surveillance des mises à jour du cache de lecture du SSD

Vous pouvez suivre la progression d'une mise à jour du cache de lecture SSD à l'aide de la FSx console Amazon, de l'API ou du AWS CLI.

Surveillance des mises à jour dans la console

Vous pouvez surveiller les mises à jour du système de fichiers dans l'onglet Mises à jour de la page de détails du système de fichiers.

Pour les mises à jour du cache de lecture SSD, vous pouvez consulter les informations suivantes :

Type de mise à jour

Les types pris en charge sont le mode de dimensionnement du cache de lecture SSD et la taille du cache de lecture SSD.

Valeur cible

La valeur mise à jour pour le mode de dimensionnement du cache de lecture SSD ou la taille du cache de lecture SSD du système de fichiers.

Statut

État actuel de la mise à jour. Les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon traite FSx la demande de mise à jour.
- Terminé — La mise à jour s'est terminée avec succès.

- Échec : la demande de mise à jour a échoué. Choisissez le point d'interrogation (?) pour connaître les raisons de l'échec de la demande.

Heure de la demande

Heure à laquelle Amazon FSx a reçu la demande d'action de mise à jour.

Surveillance des mises à jour du cache de lecture du SSD avec l'API AWS CLI and

Vous pouvez afficher et surveiller les demandes de mise à jour du cache de lecture du SSD du système de fichiers à l'aide de la describe-file-systems AWS CLI commande et de l'DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous mettez à jour le cache de lecture SSD d'un système de fichiers, un `FILE_SYSTEM_UPDATE` `AdministrativeActions` est généré.

L'exemple suivant montre un extrait de la réponse d'une commande `describe-file-systems` CLI. Le système de fichiers a une action administrative en attente pour changer le mode de dimensionnement du cache de lecture SSD en 524288 `USER_PROVISIONED` et la taille du cache de lecture SSD en 524288.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "DataReadCacheConfiguration": {
                     "SizingMode": "USER_PROVISIONED"
                     "SizeGiB": 524288,
                }
            }
        }
    }
]
```

Lorsque la nouvelle configuration du cache de lecture SSD est disponible pour le système de fichiers, l'`FILE_SYSTEM_UPDATE`état passe à`COMPLETED`. Si la demande de mise à jour du cache de lecture SSD échoue, le statut de l'`FILE_SYSTEM_UPDATE`action passe à`FAILED`.

Gestion des performances des métadonnées

Vous pouvez mettre à jour la configuration des métadonnées de votre système de fichiers FSx for Lustre sans perturber vos utilisateurs finaux ou vos applications en utilisant la FSx console Amazon, FSx l'API Amazon ou AWS Command Line Interface (AWS CLI). La procédure de mise à jour augmente le nombre d'IOPS de métadonnées provisionnées pour votre système de fichiers.

> **Note**
>
> Les métadonnées améliorées ne sont disponibles que pour les systèmes de fichiers 2.15. Vous pouvez augmenter les performances des métadonnées uniquement sur FSx les systèmes de fichiers Lustre créés avec le type de déploiement Persistent 2 et une configuration de métadonnées spécifiée. Vous ne pouvez pas ajouter ou mettre à jour la configuration des métadonnées FSx pour un système de fichiers pour Lustre si la configuration des métadonnées n'est pas spécifiée au moment de la création du système de fichiers. Cela s'applique également aux systèmes de fichiers restaurés à partir de sauvegardes de systèmes de fichiers 2.12 qui ne permettaient pas d'améliorer les performances des métadonnées, ou à partir de systèmes de fichiers 2.15 pour lesquels aucune configuration de métadonnées n'était spécifiée.

Les performances accrues des métadonnées de votre système de fichiers peuvent être utilisées en quelques minutes. Vous pouvez mettre à jour les performances des métadonnées à tout moment, à condition que les demandes d'augmentation des performances des métadonnées soient espacées d'au moins 6 heures. Lors du dimensionnement des performances des métadonnées, le système de fichiers peut être indisponible pendant quelques minutes. Les opérations sur les fichiers effectuées par les clients alors que le système de fichiers n'est pas disponible seront réessayées de manière transparente et finiront par réussir une fois le dimensionnement des performances des métadonnées terminé. La nouvelle augmentation des performances des métadonnées vous sera facturée une fois qu'elles seront disponibles.

Vous pouvez suivre la progression d'une augmentation des performances des métadonnées à tout moment à l'aide de la FSx console, de la CLI et de l'API Amazon. Pour de plus amples informations, veuillez consulter Surveillance des mises à jour de configuration des métadonnées.

Rubriques

- Lustreconfiguration des performances des métadonnées

- Considérations relatives à l'amélioration des performances des métadonnées
- Quand améliorer les performances des métadonnées
- Améliorer les performances des métadonnées
- Modification du mode de configuration des métadonnées
- Surveillance des mises à jour de configuration des métadonnées

Lustreconfiguration des performances des métadonnées

Le nombre d'IOPS de métadonnées provisionnées détermine le taux maximal d'opérations de métadonnées pouvant être prises en charge par le système de fichiers.

Lorsque vous créez le système de fichiers, vous choisissez un mode de configuration des métadonnées :

- Pour les systèmes de fichiers SSD, vous pouvez choisir le mode automatique si vous souhaitez qu'Amazon FSx provisionne et adapte automatiquement les IOPS de métadonnées sur votre système de fichiers en fonction de la capacité de stockage de ce dernier. Notez que les systèmes de fichiers à hiérarchisation intelligente ne prennent pas en charge le mode automatique.
- Pour les systèmes de fichiers SSD, vous pouvez choisir Provisionné par l'utilisateur si vous souhaitez spécifier le nombre d'IOPS de métadonnées à allouer à votre système de fichiers.
- Pour les systèmes de fichiers à hiérarchisation intelligente, vous devez choisir le mode provisionné par l'utilisateur. Avec le mode provisionné par l'utilisateur, vous pouvez spécifier le nombre d'IOPS de métadonnées à allouer à votre système de fichiers.

Sur les systèmes de fichiers SSD, vous pouvez passer du mode automatique au mode provisionné par l'utilisateur à tout moment. Vous pouvez également passer du mode provisionné par l'utilisateur au mode automatique si le nombre d'IOPS de métadonnées provisionnées sur votre système de fichiers correspond au nombre d'IOPS de métadonnées par défaut provisionnées en mode automatique. Les systèmes de fichiers à hiérarchisation intelligente ne prennent en charge que le mode provisionné par l'utilisateur, vous ne pouvez donc pas changer de mode de configuration des métadonnées.

Les valeurs IOPS des métadonnées valides sont les suivantes :

- Pour les systèmes de fichiers SSD, les valeurs d'IOPS de métadonnées valides sont 1 500, 3 000, 6 000 et des multiples de 12 000 jusqu'à un maximum de 192 000.

- Pour les systèmes de fichiers à hiérarchisation intelligente, les valeurs d'IOPS de métadonnées valides sont 6 000 et 12 000.

Si les performances des métadonnées de votre charge de travail dépassent le nombre d'IOPS de métadonnées provisionnées en mode automatique, vous pouvez utiliser le mode provisionné par l'utilisateur pour augmenter la valeur d'IOPS des métadonnées pour votre système de fichiers.

Vous pouvez consulter la valeur actuelle de la configuration du serveur de métadonnées du système de fichiers comme suit :

- Utilisation de la console : dans le panneau Résumé de la page de détails du système de fichiers, le champ IOPS des métadonnées indique la valeur actuelle des IOPS de métadonnées provisionnées et le mode de configuration des métadonnées actuel du système de fichiers.
- Utilisation de la CLI ou de l'API : utilisez la commande describe-file-systemsCLI ou l'opération DescribeFileSystemsAPI et recherchez la `MetadataConfiguration` propriété.

Considérations relatives à l'amélioration des performances des métadonnées

Voici quelques points importants à prendre en compte pour améliorer les performances de vos métadonnées :

- Amélioration des performances des métadonnées uniquement : vous pouvez uniquement augmenter le nombre d'IOPS de métadonnées pour un système de fichiers ; vous ne pouvez pas diminuer le nombre d'IOPS de métadonnées.
- La spécification d'IOPS de métadonnées en mode automatique n'est pas prise en charge : vous ne pouvez pas spécifier le nombre d'IOPS de métadonnées sur un système de fichiers en mode automatique. Vous devrez passer en mode provisionné par l'utilisateur, puis effectuer la demande. Pour de plus amples informations, veuillez consulter Modification du mode de configuration des métadonnées.
- IOPS de métadonnées pour les données écrites avant le dimensionnement : lorsque vous redimensionnez les IOPS de métadonnées au-delà de 12 000, Lustre ajoute FSx de nouveaux serveurs de métadonnées à votre système de fichiers. Les nouvelles métadonnées sont automatiquement distribuées sur tous les serveurs pour améliorer les performances. Toutefois, les métadonnées et les sous-répertoires existants créés avant le dimensionnement restent sur les serveurs d'origine, sans augmentation des IOPS des métadonnées.

- Délai entre deux augmentations : vous ne pouvez pas augmenter davantage les performances des métadonnées sur un système de fichiers jusqu'à 6 heures après la dernière demande d'augmentation.
- Amélioration simultanée des performances des métadonnées et du stockage SSD : vous ne pouvez pas adapter simultanément les performances des métadonnées et la capacité de stockage du système de fichiers.

Quand améliorer les performances des métadonnées

Augmentez le nombre d'IOPS de métadonnées lorsque vous devez exécuter des charges de travail nécessitant des niveaux de performance de métadonnées supérieurs à ceux fournis par défaut sur votre système de fichiers. Vous pouvez surveiller les performances de vos métadonnées sur le en AWS Management Console utilisant le `Metadata IOPS Utilization` graphique qui indique le pourcentage des performances du serveur de métadonnées provisionné que vous consommez sur votre système de fichiers.

Vous pouvez également surveiller les performances de vos métadonnées à l'aide de CloudWatch mesures plus détaillées. CloudWatch les métriques incluent `DiskReadOperations` et`DiskWriteOperations`, qui fournissent le volume d'opérations du serveur de métadonnées nécessitant des E/S sur disque, ainsi que des métriques granulaires pour les opérations de métadonnées, notamment la création de fichiers et de répertoires, les statistiques, les lectures et les suppressions. Pour de plus amples informations, veuillez consulter FSx pour les métriques de métadonnées Lustre.

Améliorer les performances des métadonnées

Vous pouvez améliorer les performances des métadonnées d'un système de fichiers en utilisant la FSx console Amazon AWS CLI, ou l' FSx API Amazon.

Pour améliorer les performances des métadonnées d'un système de fichiers (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers. Dans la liste des systèmes de fichiers, choisissez le système de fichiers Lustre FSx pour lequel vous souhaitez améliorer les performances des métadonnées.
3. Pour Actions, choisissez Mettre à jour les IOPS des métadonnées. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté du champ IOPS des métadonnées du système de fichiers.

La boîte de dialogue Mettre à jour les métadonnées IOPS s'affiche.

4. Choisissez Provisioned par l'utilisateur.
5. Pour les IOPS de métadonnées souhaitées, choisissez la nouvelle valeur d'IOPS de métadonnées. La valeur que vous entrez doit être supérieure ou égale à la valeur IOPS actuelle des métadonnées.

   - Pour les systèmes de fichiers SSD, les valeurs valides sont `15003000`,`6000`,`12000`, et des multiples `12000` allant jusqu'à un maximum de`192000`.
   - Pour les systèmes de fichiers à hiérarchisation intelligente, les valeurs valides sont et. `6000` `12000`
6. Choisissez Mettre à jour.

Pour améliorer les performances des métadonnées d'un système de fichiers (CLI)

Pour améliorer les performances des métadonnées d'un système de fichiers FSx pour Lustre, utilisez la AWS CLI commande update-file-system(UpdateFileSystem c'est l'action d'API équivalente). Définissez les paramètres suivants :

- Définissez `--file-system-id` l'ID du système de fichiers que vous mettez à jour.
- Pour améliorer les performances de vos métadonnées, utilisez la `--lustre-configuration` `MetadataConfiguration` propriété. Cette propriété possède deux paramètres, `Mode` et`Iops`.

  1. Si votre système de fichiers est en mode USER_PROVISIONED, l'utilisation `Mode` est facultative (si elle est utilisée, définie sur`Mode`). `USER_PROVISIONED`

     Si votre système de fichiers SSD est en mode AUTOMATIQUE, réglez-le sur `USER_PROVISIONED` (ce qui fait `Mode` passer le mode du système de fichiers à USER_PROVISIONED en plus d'augmenter la valeur IOPS des métadonnées).
  2. Pour les systèmes de fichiers SSD, définissez `Iops` une valeur de`1500`,`3000`, `600012000`, ou des multiples `12000` allant jusqu'à un maximum de`192000`. Pour les systèmes de fichiers à hiérarchisation intelligente, définissez sur `Iops` ou. `6000` `12000` La valeur que vous entrez doit être supérieure ou égale à la valeur IOPS actuelle des métadonnées.

L'exemple suivant met à jour les IOPS de métadonnées provisionnées à 12 000.

```
aws fsx update-file-system \
```

```
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration 'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=12000}'
```

Modification du mode de configuration des métadonnées

Pour les systèmes de fichiers SSD, vous pouvez modifier le mode de configuration des métadonnées d'un système de fichiers existant à l'aide de la AWS console et de la CLI, comme expliqué dans les procédures suivantes.

Lorsque vous passez du mode automatique au mode provisionné par l'utilisateur, vous devez fournir une valeur d'IOPS de métadonnées supérieure ou égale à la valeur d'IOPS de métadonnées actuelle du système de fichiers.

Si vous demandez à passer du mode provisionné par l'utilisateur au mode automatique et que la valeur actuelle des IOPS des métadonnées est supérieure à la valeur automatique par défaut, Amazon FSx rejette la demande, car la réduction de la taille des IOPS des métadonnées n'est pas prise en charge. Pour débloquer le changement de mode, vous devez augmenter la capacité de stockage pour qu'elle corresponde à vos IOPS de métadonnées actuelles en mode automatique afin de réactiver le changement de mode.

Vous pouvez modifier le mode de configuration des métadonnées d'un système de fichiers à l'aide de la FSx console Amazon AWS CLI, de ou de l' FSx API Amazon.

Pour modifier le mode de configuration des métadonnées d'un système de fichiers (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers. Dans la liste des systèmes de fichiers, choisissez le système de fichiers FSx pour Lustre dont vous souhaitez modifier le mode de configuration des métadonnées.
3. Pour Actions, choisissez Mettre à jour les IOPS des métadonnées. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté du champ IOPS des métadonnées du système de fichiers.

   La boîte de dialogue Mettre à jour les métadonnées IOPS s'affiche.
4. Effectuez l’une des actions suivantes :

   - Pour passer du mode provisionné par l'utilisateur au mode automatique, choisissez Automatique.

- Pour passer du mode automatique au mode provisionné par l'utilisateur, choisissez Provisioned par l'utilisateur. Ensuite, pour les IOPS de métadonnées souhaitées, indiquez une valeur d'IOPS de métadonnées supérieure ou égale à la valeur d'IOPS de métadonnées actuelle du système de fichiers.

5. Choisissez Mettre à jour.

Pour modifier le mode de configuration des métadonnées d'un système de fichiers SSD (CLI)

Pour modifier le mode de configuration des métadonnées d'un SSD FSx pour le système de fichiers Lustre, utilisez la AWS CLI commande update-file-system(UpdateFileSystem c'est l'action d'API équivalente). Définissez les paramètres suivants :

- Définissez `--file-system-id` l'ID du système de fichiers que vous mettez à jour.
- Pour modifier le mode de configuration des métadonnées sur les systèmes de fichiers SSD, utilisez la `--lustre-configuration MetadataConfiguration` propriété. Cette propriété possède deux paramètres, `Mode` et`Iops`.
  - Pour faire passer votre système de fichiers SSD du mode AUTOMATIQUE au mode USER_PROVISIONED, définissez une valeur `Mode` d'`USER_PROVISIONED`IOPS de métadonnées supérieure ou égale `Iops` à la valeur d'IOPS des métadonnées du système de fichiers actuel. Par exemple :

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration
 'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=96000}'
```

  - Pour passer du mode USER_PROVISIONED au mode AUTOMATIC, définissez le `Mode` paramètre `AUTOMATIC` et ne l'utilisez pas. `Iops` Par exemple :

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration 'MetadataConfiguration={Mode=AUTOMATIC}'
```

Surveillance des mises à jour de configuration des métadonnées

Vous pouvez suivre la progression des mises à jour de configuration des métadonnées à l'aide de la FSx console Amazon, de l'API ou du AWS CLI.

Surveillance des mises à jour de configuration des métadonnées (console)

Vous pouvez surveiller les mises à jour de configuration des métadonnées dans l'onglet Mises à jour de la page de détails du système de fichiers.

Pour les mises à jour de configuration des métadonnées, vous pouvez consulter les informations suivantes :

Type de mise à jour

Les types pris en charge sont les IOPS de métadonnées et le mode de configuration des métadonnées.

Valeur cible

La valeur mise à jour pour les IOPS de métadonnées ou le mode de configuration des métadonnées du système de fichiers.

Statut

État actuel de la mise à jour. Les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon traite FSx la demande de mise à jour.
- Terminé — La mise à jour s'est terminée avec succès.
- Échec : la demande de mise à jour a échoué. Choisissez le point d'interrogation (?) pour connaître les raisons de l'échec de la demande.

Heure de la demande

Heure à laquelle Amazon FSx a reçu la demande d'action de mise à jour.

Surveillance des mises à jour de configuration des métadonnées (CLI)

Vous pouvez afficher et surveiller les demandes de mise à jour de configuration des métadonnées à l'aide de la describe-file-systems AWS CLI commande et de l'opération DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous mettez à jour les performances ou le mode de configuration des métadonnées d'un système de fichiers, un `FILE_SYSTEM_UPDATE` `AdministrativeActions` est généré.

L'exemple suivant montre un extrait de la réponse d'une commande `describe-file-systems` CLI. Le système de fichiers a une action administrative en attente pour augmenter le nombre d'IOPS de métadonnées à 96 000 et le mode de configuration des métadonnées à USER_PROVISIONED.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1678840205.853,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "MetadataConfiguration": {
                    "Iops": 96000,
                    "Mode": USER_PROVISIONED
                }
            }
        }
    }
]
```

Amazon FSx traite l'`FILE_SYSTEM_UPDATE`action en modifiant les IOPS de métadonnées et le mode de configuration des métadonnées du système de fichiers. Lorsque les nouvelles ressources de métadonnées sont disponibles pour le système de fichiers, le `FILE_SYSTEM_UPDATE` statut passe à`COMPLETED`.

Si la demande de mise à jour de la configuration des métadonnées échoue, le statut de l'`FILE_SYSTEM_UPDATE`action passe à`FAILED`, comme indiqué dans l'exemple suivant. La `FailureDetails` propriété fournit des informations sur l'échec.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1678840205.853,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "MetadataConfiguration": {
                    "Iops": 96000,
                    "Mode": USER_PROVISIONED
                }
            }
        },
```

```
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Gestion de la capacité de débit allouée

Chaque système de fichiers FSx for Lustre possède une capacité de débit qui est configurée lorsque vous créez le système de fichiers. Pour les systèmes de fichiers utilisant un stockage SSD ou HDD, la capacité de débit est mesurée en mégaoctets par seconde par tebioctet (MBps/TiB). For file systems using Intelligent-Tiering storage, the throughput capacity is measured in megabytes per second (MBps) for the file system. Throughput capacity is one factor that determines the speed at which the file server hosting the file system can serve file data. Higher levels of throughput capacity also come with higher levels of I/Oopérations par seconde (IOPS) et en plus de mémoire pour la mise en cache des données sur le serveur de fichiers. Pour de plus amples informations, veuillez consulter Amazon FSx pour les performances de Lustre.

Vous pouvez modifier le niveau de débit d'un système de fichiers SSD persistant en augmentant ou en diminuant la valeur du débit du système de fichiers par unité de stockage. Les valeurs valides dépendent du type de déploiement du système de fichiers, comme suit :

- Pour les types de déploiement basés sur un SSD Persistent 1, les valeurs valides sont 50, 100 et 200 /TiB. MBps
- Pour les types de déploiement basés sur SSD Persistent 2, les valeurs valides sont 125, 250, 500 et 1000 /TiB. MBps

Vous pouvez modifier la capacité de débit d'un système de fichiers à hiérarchisation intelligente en augmentant la valeur de la capacité de débit totale du système de fichiers. Les valeurs valides sont 4 000 MBps ou des incréments de 4 000 MBps, jusqu'à un maximum de 2 MBps 000 000.

Vous pouvez consulter la valeur actuelle de la capacité de débit du système de fichiers comme suit :

- Utilisation de la console : dans le panneau Résumé de la page de détails du système de fichiers, le champ Débit par unité de stockage indique la valeur actuelle pour les systèmes de fichiers SSD, tandis que le champ Capacité de débit indique la valeur actuelle pour les systèmes de fichiers à hiérarchisation intelligente.

- Utilisation de la CLI ou de l'API : utilisez la commande describe-file-systemsCLI ou l'opération DescribeFileSystemsAPI et recherchez la `PerUnitStorageThroughput` propriété.

Lorsque vous modifiez la capacité de débit de votre système de fichiers, Amazon FSx remplace en arrière-plan les serveurs de fichiers du système de fichiers par des systèmes de fichiers SSD ou ajoute de nouveaux serveurs de fichiers sur des systèmes de fichiers à hiérarchisation intelligente. Votre système de fichiers sera indisponible pendant une heure au maximum pendant le dimensionnement de la capacité de débit. La nouvelle capacité de débit vous est facturée une fois qu'elle est disponible pour votre système de fichiers.

Rubriques

- Considérations relatives à la mise à jour de la capacité de débit
- Quand modifier la capacité de débit
- Modification de la capacité de débit
- Surveillance des variations de capacité de débit

Considérations relatives à la mise à jour de la capacité de débit

Voici quelques points importants à prendre en compte lors de la mise à jour de la capacité de débit :

- Augmenter ou diminuer : vous pouvez augmenter ou diminuer la capacité de débit d'un système de fichiers SSD. Vous pouvez uniquement augmenter la capacité de débit d'un système de fichiers à hiérarchisation intelligente.
- Mettre à jour les incréments : lorsque vous modifiez la capacité de débit, utilisez les incréments répertoriés dans la boîte de dialogue Mettre à jour le niveau de débit pour les systèmes de fichiers SSD ou dans la boîte de dialogue Mettre à jour la capacité de débit pour les systèmes de fichiers à hiérarchisation intelligente.
- Délai entre les augmentations : vous ne pouvez pas apporter d'autres modifications de capacité de débit sur un système de fichiers jusqu'à ce que 6 heures après la dernière demande ou avant la fin du processus d'optimisation du débit, selon le délai le plus long.
- Dimensionnement automatique du cache de lecture SSD — Pour le mode par défaut du cache de lecture SSD (proportionnel à la capacité de débit), Amazon FSx fournit automatiquement 5 GiB de stockage de données pour MBps chaque capacité de débit que vous fournissez. Au fur et à mesure que vous augmentez la capacité de débit de votre système de fichiers, Amazon adapte

FSx automatiquement le cache de données de votre SSD en attachant un espace de stockage de cache supplémentaire à tout serveur de fichiers nouvellement ajouté.

- Type de déploiement : vous ne pouvez mettre à jour la capacité de débit que pour les types de déploiement basés sur des SSD persistants ou basés sur la hiérarchisation intelligente. Vous ne pouvez pas modifier la capacité de débit des systèmes de fichiers SSD compatibles EFA.

Quand modifier la capacité de débit

Amazon FSx s'intègre à Amazon CloudWatch, ce qui vous permet de surveiller les niveaux d'utilisation continue du débit de votre système de fichiers. Les performances (débit et IOPS) que vous pouvez optimiser dans votre système de fichiers dépendent des caractéristiques spécifiques de votre charge de travail, en plus de la capacité de débit, de la capacité de stockage et de la classe de stockage de votre système de fichiers. Pour plus d'informations sur la manière de déterminer le débit actuel de votre système de fichiers, consultezComment utiliser les CloudWatch métriques Amazon FSx for Lustre. Pour plus d'informations sur CloudWatch les métriques, consultezSurveillance avec Amazon CloudWatch.

Modification de la capacité de débit

Vous pouvez modifier la capacité de débit d'un système de fichiers FSx pour Lustre à l'aide de la FSx console Amazon, du AWS Command Line Interface (AWS CLI) ou de l' FSx API Amazon.

Pour modifier la capacité de débit d'un système de fichiers SSD (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système FSx de fichiers Lustre dont vous souhaitez modifier la capacité de débit.
3. Pour Actions, choisissez Mettre à jour le niveau de débit. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté du débit du système de fichiers par unité de stockage.

   La fenêtre Mettre à jour le niveau de débit apparaît.
4. Choisissez la nouvelle valeur du débit souhaité par unité de stockage dans la liste.
5. Choisissez Mettre à jour pour lancer la mise à jour de la capacité de débit.

> **Note**
>
> Votre système de fichiers peut connaître une très brève période d'indisponibilité lors de la mise à jour.

Pour modifier la capacité de débit (CLI) d'un système de fichiers SSD

- Pour modifier la capacité de débit d'un système de fichiers, utilisez la commande update-file-systemCLI (ou une opération UpdateFileSystemAPI équivalente). Définissez les paramètres suivants :
  - `--file-system-id`Défini sur l'ID du système de fichiers que vous mettez à jour.
  - `--lustre-configuration PerUnitStorageThroughput`Défini sur une valeur de `50`100, ou `200` MBps/TiB pour les systèmes de fichiers SSD persistants 1, ou sur une valeur de`125`, `250`500, ou `1000` MBps/TiB pour les systèmes de fichiers SSD persistants 2.

  Cette commande indique que la capacité de débit doit être définie sur MBps 1000/TiB pour le système de fichiers.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration PerUnitStorageThroughput=1000
```

Pour modifier la capacité de débit d'un système de fichiers à hiérarchisation intelligente (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système FSx de fichiers Lustre dont vous souhaitez modifier la capacité de débit.
3. Pour Actions, choisissez Mettre à jour la capacité de débit. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté de la capacité de débit du système de fichiers.

   La boîte de dialogue Mettre à jour la capacité de débit apparaît.
4. Choisissez la nouvelle valeur pour la capacité de débit souhaitée dans la liste.

Amazon FSx redimensionnera automatiquement votre cache de lecture de données pour éviter d'en effacer le contenu.

5. Choisissez Mettre à jour pour lancer la mise à jour de la capacité de débit.

> **Note**
>
> Votre système de fichiers peut connaître une très brève période d'indisponibilité lors de la mise à jour.

Pour modifier la capacité de débit (CLI) d'un système de fichiers à hiérarchisation intelligente

- Pour modifier la capacité de débit d'un système de fichiers, utilisez la commande update-file-systemCLI (ou une opération UpdateFileSystemAPI équivalente). Définissez les paramètres suivants :

  - `--file-system-id`Défini sur l'ID du système de fichiers que vous mettez à jour.
  - Si votre cache de lecture de données est configuré en mode proportionnel à la capacité de débit, définissez `--lustre-configuration ThroughputCapacity` un niveau de débit par incréments de `4000` MBps, jusqu'à un maximum de. `2000000` MBps

    Si votre cache de lecture de données est configuré en mode provisionné par l'utilisateur, vous devez également utiliser la `--lustre-configuration DataReadCacheConfiguration` propriété pour spécifier le cache de lecture de données. Vous devez conserver le même ratio de stockage cache par serveur et spécifier le nouveau SizeGi B, sinon la demande sera rejetée.

  Cette commande indique que la capacité de débit doit être définie sur 8 000 MBps pour un système de fichiers qui utilise un cache de lecture configuré en mode proportionnel à la capacité de débit.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration '{
      "ThroughputCapacity": 8000
      }'
```

Cette commande indique que la capacité de débit doit être définie sur 8 000 MBps pour un système de fichiers qui utilise un cache de lecture configuré en mode provisionné par l'utilisateur.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration {
        "ThroughputCapacity": 8000,
        "DataReadCacheConfiguration": '{
             "SizingMode":"USER_PROVISIONED"
             "SizeGiB":1000
             # New size should be cache storage allocated per server multiplied by
 number of file servers
         }
}'
```

Surveillance des variations de capacité de débit

Vous pouvez suivre la progression d'une modification de capacité de débit à l'aide de la FSx console Amazon, de l'API et du AWS CLI.

Surveillance des variations de capacité de débit (console)

- Dans l'onglet Mises à jour de la page des détails du système de fichiers, vous pouvez consulter les 10 actions de mise à jour les plus récentes pour chaque type d'action de mise à jour.

  Pour les actions de mise à jour de la capacité de débit, vous pouvez consulter les informations suivantes.

  Type de mise à jour

  Le type pris en charge est Débit de stockage par unité.

  Valeur cible

  La valeur souhaitée pour modifier le débit du système de fichiers par unité de stockage.

  Statut

  État actuel de la mise à jour. Pour les mises à jour de la capacité de débit, les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon traite FSx la demande de mise à jour.
- Mise à jour ; optimisation — Amazon FSx a mis à jour les I/O, CPU, and memory resources. The new disk I/O performance level is available for write operations. Your read operations will see disk I/O performances réseau du système de fichiers entre le niveau précédent et le nouveau niveau jusqu'à ce que votre système de fichiers ne soit plus dans cet état.
- Terminé — La mise à jour de la capacité de débit s'est terminée avec succès.
- Échec : la mise à jour de la capacité de débit a échoué. Choisissez le point d'interrogation (?) pour en savoir plus sur les raisons de l'échec de la mise à jour du débit.

Heure de la demande

Heure à laquelle Amazon FSx a reçu la demande de mise à jour.

Surveillance des mises à jour du système de fichiers (CLI)

- Vous pouvez afficher et surveiller les demandes de modification de la capacité du débit du système de fichiers à l'aide de la commande describe-file-systemsCLI et de l'action DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous modifiez la capacité de débit d'un système de fichiers, une action `FILE_SYSTEM_UPDATE` administrative est générée.

  L'exemple suivant montre l'extrait de réponse d'une commande `describe-file-systems` CLI. Le système de fichiers a un débit cible par unité de stockage de MBps 500/TiB.

```
.
.
.
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "LustreConfiguration": {
            "PerUnitStorageThroughput": 500
```

```
          }
        }
    }
]
```

Lorsque Amazon FSx traite l'action avec succès, le statut passe à`COMPLETED`. La nouvelle capacité de débit est alors disponible pour le système de fichiers et apparaît dans la `PerUnitStorageThroughput` propriété.

Si la modification de la capacité de débit échoue, le statut passe à`FAILED`, et la `FailureDetails` propriété fournit des informations sur la panne.

Lustrecompression de données

Vous pouvez utiliser la fonction de compression Lustre des données pour réaliser des économies sur vos systèmes de fichiers et de stockage de sauvegarde Amazon FSx for Lustre à hautes performances. Lorsque la compression des données est activée, Amazon FSx for Lustre compresse automatiquement les fichiers nouvellement écrits avant qu'ils ne soient écrits sur le disque et les décompresse automatiquement lorsqu'ils sont lus.

La compression des données utilise l' LZ4 algorithme, qui est optimisé pour fournir des niveaux de compression élevés sans nuire aux performances du système de fichiers. LZ4 est un algorithme Lustre fiable par la communauté et axé sur les performances qui fournit un équilibre entre la vitesse de compression et la taille du fichier compressé. L'activation de la compression des données n'a généralement pas d'impact mesurable sur la latence.

La compression des données réduit la quantité de données transférées entre les serveurs de fichiers Amazon FSx for Lustre et le stockage. Si vous n'utilisez pas encore de formats de fichiers compressés, vous constaterez une augmentation de la capacité de débit globale du système de fichiers lors de la compression des données. Les augmentations de capacité de débit liées à la compression des données seront plafonnées une fois que vous aurez saturé vos cartes d'interface réseau frontales.

Par exemple, si votre système de fichiers est un type de déploiement SSD PERSISTENT-50, le débit de votre réseau a une base de référence de 250 par MBps TiB de stockage. Le débit de votre disque a une valeur de référence de 50 MBps par TiB. Avec la compression des données, le débit de votre disque peut passer de 50 MBps par TiB à un maximum de 250 MBps par TiB, ce qui est la limite de débit réseau de base. Pour plus d'informations sur les limites de débit du réseau et du

disque, consultez les tableaux de performances des systèmes de fichiers dansCaractéristiques de performance des classes de stockage SSD et HDD. Pour plus d'informations sur les performances de compression des données, consultez le billet Dépensez moins tout en augmentant les performances grâce à la compression Amazon FSx for Lustre des données sur le blog sur le AWS stockage.

Rubriques

- Gestion de la compression des données
- Compression de fichiers déjà écrits
- Affichage de la taille des fichiers
- Utilisation de CloudWatch métriques

Gestion de la compression des données

Vous pouvez activer ou désactiver la compression des données lors de la création d'un nouveau système de fichiers Amazon FSx for Lustre. La compression des données est désactivée par défaut lorsque vous créez un système de fichiers Amazon FSx for Lustre à partir de la console ou de l'API. AWS CLI

Pour activer la compression des données lors de la création d'un système de fichiers (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau système de fichiers décrite Étape 1 : Créez votre système de fichiers FSx for Lustre dans la section Démarrage.
3. Dans la section Détails du système de fichiers, pour Type de compression des données, sélectionnez LZ4.
4. Complétez l'assistant comme vous le faites lorsque vous créez un nouveau système de fichiers.
5. Choisissez Review and create.
6. Passez en revue les paramètres que vous avez choisis FSx pour votre système de fichiers Amazon for Lustre, puis choisissez Create file system.

Lorsque le système de fichiers est disponible, la compression des données est activée.

Pour activer la compression des données lors de la création d'un système de fichiers (CLI)

- Pour créer un système de fichiers FSx pour Lustre avec la compression des données activée, utilisez la commande Amazon FSx CLI `create-file-system`avec le

`DataCompressionType` paramètre, comme indiqué ci-dessous. L'opération d'API correspondante est CreateFileSystem.

```
$ aws fsx create-file-system \
      --client-request-token CRT1234 \
      --file-system-type LUSTRE \
      --file-system-type-version 2.12 \
      --lustre-configuration
 DeploymentType=PERSISTENT_1,PerUnitStorageThroughput=50,DataCompressionType=LZ4 \
      --storage-capacity 3600 \
      --subnet-ids subnet-123456 \
      --tags Key=Name,Value=Lustre-TEST-1 \
      --region us-east-2
```

Après avoir créé le système de fichiers avec succès, Amazon FSx renvoie la description du système de fichiers au format JSON, comme illustré dans l'exemple suivant.

```
{

    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.12",
            "Lifecycle": "CREATING",
            "StorageCapacity": 3600,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
```

```
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_1",
                "DataCompressionType": "LZ4",
                "PerUnitStorageThroughput": 50
            }
        }
    ]
}
```

Vous pouvez également modifier la configuration de compression des données de vos systèmes de fichiers existants. Lorsque vous activez la compression des données pour un système de fichiers existant, seuls les fichiers nouvellement écrits sont compressés et les fichiers existants ne le sont pas. Pour de plus amples informations, veuillez consulter Compression de fichiers déjà écrits.

Pour mettre à jour la compression des données sur un système de fichiers existant (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de Lustre fichiers pour lequel vous souhaitez gérer la compression des données.
3. Pour Actions, sélectionnez Mettre à jour le type de compression des données.
4. Dans la boîte de dialogue Mettre à jour le type de compression LZ4des données, choisissez d'activer la compression des données ou sélectionnez AUCUN pour la désactiver.
5. Choisissez Mettre à jour.
6. Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers dans l'onglet Mises à jour.

Pour mettre à jour la compression des données sur un système de fichiers existant (CLI)

Pour mettre à jour la configuration de compression des données pour un système de fichiers existant FSx pour Lustre, utilisez la AWS CLI commande update-file-system. Définissez les paramètres suivants :

- `--file-system-id`Défini sur l'ID du système de fichiers que vous mettez à jour.
- Réglez sur `--lustre-configuration DataCompressionType NONE` pour désactiver la compression des données ou `LZ4` pour activer la compression des données avec l' LZ4 algorithme.

Cette commande indique que la compression des données est activée avec l' LZ4 algorithme.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration DataCompressionType=LZ4
```

Configuration de la compression des données lors de la création d'un système de fichiers à partir d'une sauvegarde

Vous pouvez utiliser une sauvegarde disponible pour créer un nouveau système de fichiers Amazon FSx for Lustre. Lorsque vous créez un nouveau système de fichiers à partir d'une sauvegarde, il n'est pas nécessaire de le spécifier `DataCompressionType` ; le paramètre sera appliqué à l'aide du `DataCompressionType` paramètre de sauvegarde. Si vous choisissez de le spécifier `DataCompressionType` lors de la création à partir d'une sauvegarde, la valeur doit correspondre au `DataCompressionType` paramètre de la sauvegarde.

Pour consulter les paramètres d'une sauvegarde, sélectionnez-la dans l'onglet Sauvegardes de la FSx console Amazon. Les détails de la sauvegarde seront répertoriés sur la page de résumé de la sauvegarde. Vous pouvez également exécuter la `describe-backups` AWS CLI commande (l'action d'API équivalente est `DescribeBackups`).

Compression de fichiers déjà écrits

Les fichiers ne sont pas compressés s'ils ont été créés lorsque la compression des données a été désactivée sur le système de fichiers Amazon FSx for Lustre. L'activation de la compression des données ne compresse pas automatiquement vos données non compressées existantes.

Vous pouvez utiliser la `lfs_migrate` commande installée dans le cadre de l'installation du Lustre client pour compresser des fichiers existants. Pour un exemple, voir FSxL-Compression, disponible sur GitHub.

Affichage de la taille des fichiers

Vous pouvez utiliser les commandes suivantes pour afficher les tailles non compressées et compressées de vos fichiers et répertoires.

- duaffiche les tailles compressées.
- `du --apparent-size`affiche les tailles non compressées.
- `ls -l`affiche les tailles non compressées.

Les exemples suivants montrent le résultat de chaque commande avec le même fichier.

```
$ du -sh samplefile
272M samplefile
$ du -sh --apparent-size samplefile
1.0G samplefile
$ ls -lh samplefile
-rw-r--r-- 1 root root 1.0G May 10 21:16 samplefile
```

L'`-h`option est utile pour ces commandes car elle imprime les tailles dans un format lisible par l'homme.

Utilisation de CloudWatch métriques

Vous pouvez utiliser CloudWatch les métriques Amazon Logs pour consulter l'utilisation de votre système de fichiers. La `LogicalDiskUsage` métrique indique l'utilisation totale du disque logique (sans compression), et la `PhysicalDiskUsage` métrique indique l'utilisation totale du disque physique (avec compression). Ces deux mesures ne sont disponibles que si la compression des données est activée sur votre système de fichiers ou si elle était déjà activée.

Vous pouvez déterminer le taux de compression de votre système de fichiers en divisant le chiffre `Sum` de la `LogicalDiskUsage` statistique par celui `Sum` de la `PhysicalDiskUsage` statistique.

Pour plus d'informations sur la surveillance des performances de votre système de fichiers, consultezSurveillance des systèmes de fichiers Amazon FSx pour Lustre.

Lustrecourge-racine

Root squash est une fonctionnalité administrative qui ajoute une couche supplémentaire de contrôle d'accès aux fichiers en plus du contrôle d'accès basé sur le réseau actuel et des autorisations de fichiers POSIX. À l'aide de la fonctionnalité root squash, vous pouvez restreindre l'accès au niveau root aux clients qui tentent d'accéder à votre système de fichiers FSx for Lustre en tant que root.

Les autorisations de l'utilisateur root sont requises pour effectuer des actions administratives, telles que la gestion des autorisations sur FSx les systèmes de fichiers Lustre. Cependant, l'accès root fournit un accès illimité aux utilisateurs, leur permettant de contourner les contrôles d'autorisation pour accéder, modifier ou supprimer des objets du système de fichiers. À l'aide de la fonctionnalité root squash, vous pouvez empêcher l'accès non autorisé ou la suppression de données en spécifiant un ID utilisateur (UID) et un ID de groupe (GID) autres que root pour votre système de fichiers. Les utilisateurs root accédant au système de fichiers seront automatiquement convertis vers les

utilisateurs moins privilégiés spécifiés user/group avec des autorisations limitées définies par l'administrateur du stockage.

La fonctionnalité Root Squash vous permet également, en option, de fournir une liste de clients qui ne sont pas concernés par le paramètre Root squash. Ces clients peuvent accéder au système de fichiers en tant que root, avec des privilèges illimités.

Rubriques

- Comment fonctionne le courge-racine
- Gérer les courges-racines

Comment fonctionne le courge-racine

La fonctionnalité root squash fonctionne en remappant l'ID utilisateur (UID) et l'ID de groupe (GID) de l'utilisateur root à un UID et un GID spécifiés par l'administrateur système. Lustre La fonctionnalité root squash vous permet également de spécifier éventuellement un ensemble de clients pour lesquels le remappage UID/GID ne s'applique pas.

Lorsque vous créez un nouveau système de fichiers FSx pour Lustre, root squash est désactivé par défaut. Vous activez Root Squash en configurant un paramètre UID et GID root squash pour votre système de fichiers FSx for Lustre. Les valeurs UID et GID sont des nombres entiers pouvant aller de à : `0` `4294967294`

- Une valeur différente de zéro pour l'UID et le GID active Root squash. Les valeurs UID et GID peuvent être différentes, mais chacune doit être une valeur différente de zéro.
- Une valeur de `0` (zéro) pour l'UID et le GID indique root et désactive donc Root squash.

Lors de la création du système de fichiers, vous pouvez utiliser la FSx console Amazon pour fournir les valeurs UID et GID de root squash dans la propriété Root Squash, comme indiqué dans. Pour activer Root Squash lors de la création d'un système de fichiers (console) Vous pouvez également utiliser le `RootSquash` paramètre avec l'API AWS CLI or pour fournir les valeurs UID et GID, comme indiqué dans. Pour activer Root Squash lors de la création d'un système de fichiers (CLI)

Facultativement, vous pouvez également spécifier une liste NIDs de clients auxquels Root squash ne s'applique pas. Un NID client est un identifiant Lustre réseau utilisé pour identifier un client de manière unique. Vous pouvez spécifier le NID sous la forme d'une adresse unique ou d'une plage d'adresses :

- Une adresse unique est décrite au format Lustre NID standard en spécifiant l'adresse IP du client suivie de l'ID Lustre réseau (par exemple,`10.0.1.6@tcp`).
- Une plage d'adresses est décrite à l'aide d'un tiret pour séparer la plage (par exemple,`10.0.[2-10].[1-255]@tcp`).
- Si vous ne spécifiez aucun client NIDs, il n'y aura aucune exception pour Root Squash.

Lorsque vous créez ou mettez à jour votre système de fichiers, vous pouvez utiliser la propriété Exceptions to Root Squash dans la FSx console Amazon pour fournir la liste des clients NIDs. Dans l'API AWS CLI or, utilisez le `NoSquashNids` paramètre. Pour plus d'informations, consultez les procédures décrites dansGérer les courges-racines.

Gérer les courges-racines

Lors de la création du système de fichiers, le squash root est désactivé par défaut. Vous pouvez activer Root Squash lors de la création d'un nouveau système de fichiers Amazon FSx for Lustre à partir de la FSx console Amazon ou de l'API. AWS CLI

Pour activer Root Squash lors de la création d'un système de fichiers (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau système de fichiers décrite Étape 1 : Créez votre système de fichiers FSx for Lustre dans la section Démarrage.
3. Ouvrez la section Root Squash - facultative.
4. Pour Root Squash, indiquez l'utilisateur et le groupe IDs avec lesquels l'utilisateur root peut accéder au système de fichiers. Vous pouvez spécifier n'importe quel nombre entier compris entre `1` — `4294967294` :
    1. Pour ID utilisateur, spécifiez l'ID utilisateur que l'utilisateur root doit utiliser.
    2. Pour ID de groupe, spécifiez l'ID de groupe que l'utilisateur root doit utiliser.
5. (Facultatif) Pour les exceptions à la courge racine, procédez comme suit :
    1. Choisissez Ajouter une adresse client.
    2. Dans le champ Adresses des clients, spécifiez l'adresse IP d'un client auquel Root Squash ne s'applique pas. Pour plus d'informations sur le format de l'adresse IP, voirComment fonctionne le courge-racine.
    3. Répétez l'opération si nécessaire pour ajouter d'autres adresses IP de clients.

6. Complétez l'assistant comme vous le faites lorsque vous créez un nouveau système de fichiers.
7. Choisissez Review and create.
8. Passez en revue les paramètres que vous avez choisis FSx pour votre système de fichiers Amazon for Lustre, puis choisissez Create file system.

Lorsque le système de fichiers est disponible, Root Squash est activé.

Pour activer Root Squash lors de la création d'un système de fichiers (CLI)

- Pour créer un système de fichiers FSx for Lustre avec root squash activé, utilisez la commande Amazon FSx CLI `create-file-system`avec le `RootSquashConfiguration` paramètre. L'opération d'API correspondante est CreateFileSystem.

  Pour le `RootSquashConfiguration` paramètre, définissez les options suivantes :

  - `RootSquash`— Les valeurs UID:GID séparées par des virgules qui spécifient l'ID utilisateur et l'ID de groupe que l'utilisateur root doit utiliser. Vous pouvez spécifier n'importe quel nombre entier compris entre `0` — `4294967294` (0 correspond à la racine) pour chaque ID (par exemple,`65534:65534`).
  - `NoSquashNids`— Spécifiez les identifiants Lustre réseau (NIDs) des clients auxquels Root Squash ne s'applique pas. Pour plus d'informations sur le format NID du client, consultezComment fonctionne le courge-racine.

  L'exemple suivant crée un système de fichiers FSx for Lustre avec root squash activé :

```
$ aws fsx create-file-system \
      --client-request-token CRT1234 \
      --file-system-type LUSTRE \
      --file-system-type-version 2.15 \
      --lustre-configuration
 "DeploymentType=PERSISTENT_2,PerUnitStorageThroughput=250,DataCompressionType=LZ4,
\
          RootSquashConfiguration={RootSquash="65534:65534",\
          NoSquashNids=["10.216.123.47@tcp", "10.216.12.176@tcp"]}" \
      --storage-capacity 2400 \
      --subnet-ids subnet-123456 \
      --tags Key=Name,Value=Lustre-TEST-1 \
      --region us-east-2
```

Après avoir créé le système de fichiers avec succès, Amazon FSx renvoie la description du système de fichiers au format JSON, comme illustré dans l'exemple suivant.


```
{

    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.15",
            "Lifecycle": "CREATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_2",
                "DataCompressionType": "LZ4",
                "PerUnitStorageThroughput": 250,
                "RootSquashConfiguration": {
                    "RootSquash": "65534:65534",
                    "NoSquashNids": "10.216.123.47@tcp 10.216.29.176@tcp"
            }
        }
    ]
}
```

Vous pouvez également mettre à jour les paramètres root squash de votre système de fichiers existant à l'aide de la FSx console Amazon ou de l'API. AWS CLI Par exemple, vous pouvez modifier les valeurs UID et GID de root squash, ajouter ou supprimer un client NIDs ou désactiver root squash.

Pour mettre à jour les paramètres de root squash sur un système de fichiers existant (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de Lustre fichiers pour lequel vous souhaitez gérer Root Squash.
3. Pour Actions, choisissez Mettre à jour la courge rouge. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté du champ Root Squash du système de fichiers pour afficher la boîte de dialogue Mettre à jour les paramètres de Root Squash.
4. Pour Root Squash, mettez à jour l'utilisateur et le groupe IDs avec lesquels l'utilisateur root peut accéder au système de fichiers. Vous pouvez spécifier n'importe quel nombre entier compris entre `0` —`4294967294`. Pour désactiver la courge racine, spécifiez `0` (zéro) pour les deux IDs.
    1. Pour ID utilisateur, spécifiez l'ID utilisateur que l'utilisateur root doit utiliser.
    2. Pour ID de groupe, spécifiez l'ID de groupe que l'utilisateur root doit utiliser.
5. Pour les exceptions relatives à la courge rouge, procédez comme suit :
    1. Choisissez Ajouter une adresse client.
    2. Dans le champ Adresses des clients, spécifiez l'adresse IP d'un client auquel root squash ne s'applique pas,
    3. Répétez l'opération si nécessaire pour ajouter d'autres adresses IP de clients.
6. Choisissez Mettre à jour.

> **Note**
>
> Si Root squash est activé et que vous souhaitez le désactiver, choisissez Désactiver au lieu de suivre les étapes 4 à 6.

Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers dans l'onglet Mises à jour.

Pour mettre à jour les paramètres de root squash sur un système de fichiers existant (CLI)

Pour mettre à jour les paramètres de root squash pour un système de fichiers existant FSx pour Lustre, utilisez la AWS CLI commande update-file-system. L'opération d'API correspondante est UpdateFileSystem.

Définissez les paramètres suivants :

- `--file-system-id`Défini sur l'ID du système de fichiers que vous mettez à jour.
- Définissez les `--lustre-configuration RootSquashConfiguration` options comme suit :
  - `RootSquash`— Définissez les valeurs UID:GID séparées par des deux-points qui spécifient l'ID utilisateur et l'ID de groupe que l'utilisateur root doit utiliser. Vous pouvez spécifier n'importe quel nombre entier compris entre `0` — `4294967294` (0 correspond à la racine) pour chaque ID. Pour désactiver Root Squash, spécifiez `0:0` les valeurs UID:GID.
  - `NoSquashNids`— Spécifiez les identifiants Lustre réseau (NIDs) des clients auxquels Root Squash ne s'applique pas. `[]`À utiliser pour supprimer tous les clients NIDs, ce qui signifie qu'il n'y aura aucune exception à Root Squash.

Cette commande indique que root squash est activé en utilisant `65534` comme valeur l'ID utilisateur et l'ID de groupe de l'utilisateur root.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration RootSquashConfiguration={RootSquash="65534:65534", \
          NoSquashNids=["10.216.123.47@tcp", "10.216.12.176@tcp"]}
```

Si la commande aboutit, Amazon FSx for Lustre renvoie la réponse au format JSON.

Vous pouvez consulter les paramètres root squash de votre système de fichiers dans le panneau Résumé de la page de détails du système de fichiers sur la FSx console Amazon ou en réponse à une commande `describe-file-systems`CLI (l'action d'API équivalente est `DescribeFileSystems`).

FSx pour l'état du système de fichiers Lustre

Vous pouvez consulter l'état d'un système de FSx fichiers Amazon à l'aide de la FSx console Amazon, de la AWS CLI commande describe-file-systemsou de l'opération API DescribeFileSystems.

État du système de fichiers	Description
DISPONIBLE	Le système de fichiers est en bon état, accessible et prêt à être utilisé.
CREAtioN	Amazon FSx est en train de créer un nouveau système de fichiers.
SUPPRESSION	Amazon FSx est en train de supprimer un système de fichiers existant.
MISE À JOUR	Le système de fichiers est en cours de mise à jour à l'initiative du client.
MAL CONFIGURÉ	Le système de fichiers est dans un état défaillant mais récupérable.
ÉCHEC	Ce statut peut avoir l'une des significations suivantes : • Le système de fichiers est défaillant et Amazon ne FSx parvient pas à le récupérer. • Lors de la création d'un nouveau système de fichiers, Amazon FSx n'a pas pu créer le système de fichiers.

Marquez vos ressources Amazon FSx for Lustre

Pour vous aider à gérer vos systèmes de fichiers et les autres ressources Amazon FSx for Lustre, vous pouvez attribuer vos propres métadonnées à chaque ressource sous forme de balises. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Cette approche 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 balises et vous montre comment les créer.

Rubriques

- Principes de base des étiquettes
- Balisage de vos ressources
- Restrictions liées aux étiquettes
- Autorisations et étiquette

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 FSx for Lustre de votre compte afin de suivre le propriétaire et le niveau de pile de chaque instance.

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 tags n'ont aucune signification sémantique pour Amazon FSx et sont interprétés 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.

Si vous utilisez l'API Amazon FSx for Lustre, la AWS CLI ou un AWS SDK, vous pouvez utiliser l'action de l'`TagResource`API pour appliquer des balises aux ressources existantes. En outre, certaines actions de création de ressources vous permettent de spécifier des balises pour une ressource lors de la création de cette dernière. Si les balises ne peuvent pas être appliquées au cours de la création de ressources, nous restaurons le processus de création de ressources. Cela permet de s'assurer que les ressources sont créées avec des balises ou qu'elles ne sont pas créées du tout, et qu'aucune ressource ne demeurent sans balise à tout moment. En attribuant des balises aux ressources au moment de la création, vous pouvez supprimer la nécessité d'exécuter des scriptes de balisage personnalisés après la création de ressources. Pour plus d'informations sur la

façon de permettre aux utilisateurs de baliser des ressources lors de la création, consultez Accorder l'autorisation de baliser les ressources lors de la création.

Balisage de vos ressources

Vous pouvez étiqueter les ressources Amazon FSx for Lustre présentes sur votre compte. Si vous utilisez la FSx console Amazon, vous pouvez appliquer des balises aux ressources en utilisant l'onglet Tags sur l'écran des ressources concerné. Lorsque vous créez des ressources, vous pouvez appliquer la clé Nom avec une valeur, et vous pouvez appliquer les balises de votre choix lors de la création d'un nouveau système de fichiers. La console peut organiser les ressources en fonction de la balise Name, mais cette balise n'a aucune signification sémantique pour le service Amazon FSx for Lustre.

Vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans vos politiques IAM aux actions de l'API Amazon FSx for Lustre qui prennent en charge le balisage lors de la création afin de mettre en œuvre un contrôle granulaire sur les utilisateurs et les groupes autorisés à étiqueter les ressources lors de la création. Vos ressources sont correctement sécurisées depuis la création. Les balises sont appliquées immédiatement à vos ressources. Les autorisations de niveau ressource basées sur des balises sont donc effectives immédiatement. Vos ressources peuvent être suivies et signalées avec plus de précision. Vous pouvez appliquer l'utilisation du balisage sur les nouvelles ressources et contrôler que les clés et valeurs de balise sont définies sur vos ressources.

Vous pouvez également appliquer des autorisations au niveau des ressources aux actions de l'API `TagResource` `UntagResource` Amazon FSx for Lustre et à celles de l'API Amazon for Lustre dans vos politiques IAM afin de contrôler les clés et les valeurs de balise définies sur vos ressources existantes.

Pour plus d'informations sur l'étiquetage de vos ressources pour la facturation, consultez Utilisation des étiquettes de répartition des coûts dans le AWS Billing Guide de l'utilisateur.

Restrictions liées aux étiquettes

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

- Les caractères autorisés pour les balises Amazon FSx for Lustre sont les suivants : lettres, chiffres et espaces représentables en UTF-8, ainsi que les caractères suivants : + - =. _ :/@.
- Les clés et valeurs d'étiquette 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 supprimer une ressource uniquement en fonction de ses balises ; vous devez spécifier l'identifiant de la ressource. Par exemple, pour supprimer un système de fichiers que vous avez balisé avec une clé de balise appelée`DeleteMe`, vous devez utiliser l'`DeleteFileSystem`action avec l'identifiant de ressource du système de fichiers, tel que fs-1234567890abcdef0.

Lorsque vous balisez des ressources publiques ou partagées, les balises que vous attribuez ne sont disponibles que pour Compte AWS vous Compte AWS ; personne d'autre n'a accès à ces balises. 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.

Autorisations et étiquette

Pour plus d'informations sur les autorisations requises pour baliser les FSx ressources Amazon lors de leur création, consultezAccorder l'autorisation de baliser les ressources lors de la création. Pour plus d'informations sur l'utilisation de balises pour restreindre l'accès aux FSx ressources Amazon dans les politiques IAM, consultez. Utilisation de balises pour contrôler l'accès à vos FSx ressources Amazon

Fenêtres FSx de maintenance Amazon pour Lustre

Amazon FSx for Lustre applique des correctifs logiciels de routine aux Lustre logiciels qu'il gère. L'application de correctifs est peu fréquente, généralement une fois toutes les quelques semaines. La fenêtre de maintenance vous permet de contrôler le jour et l'heure de la semaine où ces correctifs logiciels ont lieu. Vous choisissez la fenêtre de maintenance lors de la création du système de fichiers. Si vous n'avez aucune préférence horaire, une fenêtre par défaut de 30 minutes est attribuée.

L'application de correctifs ne devrait nécessiter qu'une fraction de votre période de maintenance de 30 minutes. Pendant ces quelques minutes, votre système de fichiers sera temporairement

indisponible. Les opérations de fichiers effectuées par les clients alors que le système de fichiers n'est pas disponible seront réessayées de manière transparente et finiront par réussir une fois la maintenance terminée. Notez que le cache en mémoire sera effacé pendant la maintenance, ce qui entraînera des latences plus élevées jusqu'à la fin de la maintenance.

FSx for Lustre vous permet d'ajuster votre fenêtre de maintenance selon vos besoins en fonction de votre charge de travail et de vos exigences opérationnelles. Vous pouvez déplacer votre fenêtre de maintenance aussi souvent que nécessaire, à condition qu'une fenêtre de maintenance soit planifiée au moins une fois tous les 14 jours. Si un correctif est publié et que vous n'avez pas planifié de période de maintenance dans les 14 jours, FSx for Lustre procédera à la maintenance du système de fichiers afin de garantir sa sécurité et sa fiabilité.

Vous pouvez utiliser l'Amazon FSx Management Console AWS CLI, AWS l'API ou l'une des API AWS SDKs pour modifier la fenêtre de maintenance de vos systèmes de fichiers.

Pour modifier la fenêtre de maintenance à l'aide de la console

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez Systèmes de fichiers dans le volet de navigation.
3. Choisissez le système de fichiers dont vous souhaitez modifier la fenêtre de maintenance. La page de détails du système de fichiers apparaît.
4. Choisissez l'onglet Maintenance. Le panneau Paramètres de la fenêtre de maintenance apparaît.
5. Choisissez Modifier et entrez le nouveau jour et l'heure auxquels vous souhaitez que la fenêtre de maintenance commence.
6. Choisissez Save pour enregistrer les changements. La nouvelle heure de début de maintenance est affichée dans le panneau Paramètres.

Vous pouvez modifier la fenêtre de maintenance de votre système de fichiers à l'aide de la commande update-file-systemCLI. Exécutez la commande suivante en remplaçant l'ID du système de fichiers par l'ID de votre système de fichiers, ainsi que la date et l'heure auxquelles vous souhaitez ouvrir la fenêtre.

```
aws fsx update-file-system --file-system-id fs-01234567890123456 --lustre-configuration
 WeeklyMaintenanceStartTime=1:01:30
```

Gestion des versions de Lustre

FSx for Lustre prend actuellement en charge plusieurs versions de Lustre avec support à long terme (LTS) publiées par la communauté Lustre. Les nouvelles versions de LTS offrent des avantages tels que des améliorations de performances, de nouvelles fonctionnalités et la prise en charge des dernières versions du noyau Linux pour vos instances clientes. Vous pouvez mettre à niveau vos systèmes de fichiers vers des versions plus récentes de Lustre en quelques minutes à l'aide du AWS Management Console AWS CLI, ou AWS SDKs.

FSx for Lustre supporte actuellement les versions 2.10, 2.12 et 2.15 de Lustre LTS. Vous pouvez déterminer la version LTS de vos systèmes de fichiers FSx for Lustre à l'aide de la commande AWS Management Console ou à l'aide de la describe-file-systems AWS CLI commande.

Avant de procéder à une mise à niveau de la version Lustre, nous vous recommandons de suivre les étapes décrites dansBonnes pratiques pour les mises à niveau de la version Lustre.

Rubriques

- Bonnes pratiques pour les mises à niveau de la version Lustre
- Exécution de la mise à niveau

Bonnes pratiques pour les mises à niveau de la version Lustre

Nous vous recommandons de suivre les meilleures pratiques suivantes avant de mettre à niveau la version Lustre de votre système de fichiers FSx for Lustre :

- Test dans un environnement hors production : testez une mise à niveau de la version Lustre sur une copie de votre système de fichiers de production avant de procéder à la mise à niveau de votre système de fichiers de production. Cela garantit un processus de mise à niveau fluide pour votre charge de travail de production.
- Garantir la compatibilité avec le client : vérifiez que les versions du noyau Linux exécutées sur vos instances clientes sont compatibles avec la version de Lustre vers laquelle vous prévoyez de procéder à la mise à niveau. Consultez Lustrecompatibilité entre le système de fichiers et le noyau client pour plus de détails.
- Sauvegardez vos données :
  - Pour les systèmes de fichiers non liés à S3 : nous vous recommandons de créer une FSx sauvegarde avant de mettre à niveau la version Lustre afin de disposer d'un point de restauration

connu pour votre système de fichiers. Si les sauvegardes quotidiennes automatiques sont activées sur votre système de fichiers, Amazon FSx créera automatiquement une sauvegarde de votre système de fichiers avant la mise à niveau.

- Pour les systèmes de fichiers liés à S3, nous recommandons de vérifier que toutes les modifications ont été exportées vers S3 avant la mise à niveau. Si vous avez activé l'exportation automatique, vérifiez que la `AgeOfOldestQueuedMessage` AutoExportmétrique est égale à zéro pour confirmer que toutes les modifications ont été correctement exportées vers S3. Si vous n'avez pas activé l'exportation automatique, vous pouvez exécuter une tâche manuelle de référentiel de données (DRT) pour synchroniser votre système de fichiers avec le compartiment S3 avant la mise à niveau.

Exécution de la mise à niveau

Pour mettre à niveau votre système de fichiers FSx for Lustre vers une version plus récente, suivez les étapes indiquées :

1. Démonter tous les clients : avant de lancer la mise à niveau, vous devez démonter le système de fichiers de toutes les instances clientes accédant à votre système de fichiers. Vous pouvez vérifier que tous les clients sont correctement démontés en utilisant la `ClientConnections` métrique sur Amazon CloudWatch . Cette métrique ne doit afficher aucune connexion. Le processus de mise à niveau ne se poursuivra pas si des clients restent connectés au système de fichiers.

   Vous pouvez consulter la liste des identifiants de réseau client (NIDs) connectés au système de fichiers dans le `.fsx/clientConnections` fichier stocké à la racine de votre système de fichiers. Ce fichier est mis à jour toutes les 5 minutes. Vous pouvez utiliser la `cat` commande pour afficher le contenu du fichier, comme dans cet exemple :

   ```
   cat /test/.fsx/clientConnections
   ```

2. Mettre à niveau la version Lustre : vous pouvez mettre à niveau la version Lustre de votre système de fichiers FSx for Lustre à l'aide de la FSx console Amazon, de l' AWS CLI API Amazon ou de l' FSx API Amazon. Nous vous recommandons de mettre à niveau vos systèmes de fichiers vers la dernière version de Lustre prise en charge par FSx for Lustre.

   Pour mettre à jour la version Lustre d'un système de fichiers (console)

   a. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.

b. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers. Dans la liste des systèmes de fichiers, choisissez le système de fichiers FSx pour Lustre dont vous souhaitez mettre à jour la version de Lustre.

c. Pour Actions, sélectionnez Mettre à jour la version Lustre du système de fichiers. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté du champ de version Lustre du système de fichiers. La boîte de dialogue Mettre à jour la version Lustre du système de fichiers apparaît. La boîte de dialogue Mettre à jour la version Lustre du système de fichiers apparaît.

d. Dans le champ Sélectionnez une nouvelle version de Lustre, choisissez une version de Lustre. La valeur que vous choisissez doit être plus récente que la version actuelle de Lustre.

e. Choisissez Mettre à jour.

Pour mettre à jour la version Lustre d'un système de fichiers (CLI)

Pour mettre à jour la version Lustre d'un système de fichiers FSx pour Lustre, utilisez la AWS CLI commande update-file-system. (L'action d'API équivalente est UpdateFileSystem.) Définissez les paramètres suivants :

- `--file-system-id`Défini sur l'ID du système de fichiers que vous mettez à jour.
- Définissez une version `--file-system-type-version` de Lustre plus récente pour le système de fichiers que vous mettez à jour.

L'exemple suivant met à jour la version Lustre du système de fichiers de la version 2.12 à la version 2.15 :

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --file-system-type-version "2.15"
```

3. Montez tous les clients : vous pouvez suivre la progression des mises à jour des versions de Lustre en utilisant l'onglet Mises à jour de la FSx console Amazon ou `describe-file-systems` dans le AWS CLI. Une fois que l'état de mise à niveau de la version Lustre est indiqué`Completed`, vous pouvez remonter le système de fichiers en toute sécurité sur vos instances clientes et reprendre votre charge de travail.

Suppression d’un système de fichiers

Vous pouvez supprimer un système de fichiers Amazon FSx for Lustre à l'aide de la FSx console Amazon, du AWS CLI, et de l' FSx API Amazon. Avant de supprimer un système de fichiers FSx for Lustre, vous devez le démonter de chaque EC2 instance Amazon connectée. Sur les systèmes de fichiers liés à S3, pour vous assurer que toutes vos données sont réécrites dans S3 avant de supprimer votre système de fichiers, vous pouvez soit contrôler que la AgeOfOldestQueuedMessagemétrique soit nulle (si vous utilisez l'exportation automatique), soit exécuter une tâche de référentiel de données d'exportation. Si l'exportation automatique est activée et que vous souhaitez utiliser une tâche de référentiel de données d'exportation, vous devez désactiver l'exportation automatique avant d'exécuter la tâche d'exportation de référentiel de données.

Pour supprimer un système de fichiers après le démontage de chaque EC2 instance Amazon, procédez comme suit :

- Utilisation de la console : suivez la procédure décrite dansÉtape 5 : Nettoyer les ressources.
- Utilisation de l'API ou de la CLI : utilisez l'opération DeleteFileSystemAPI ou la commande delete-file-systemCLI.

Protection de vos données grâce à des sauvegardes

Avec Amazon FSx for Lustre, vous pouvez effectuer des sauvegardes quotidiennes automatiques et des sauvegardes initiées par l'utilisateur de systèmes de fichiers persistants qui ne sont pas liés à un référentiel de données durable Amazon S3. Les FSx sauvegardes Amazon sont file-system-consistent extrêmement durables et incrémentielles. Pour garantir une durabilité élevée, Amazon FSx for Lustre stocke les sauvegardes dans Amazon Simple Storage Service (Amazon S3) avec une durabilité de 99,999999999 % (11 9).

FSx pour Lustre, les sauvegardes du système de fichiers sont des sauvegardes incrémentielles basées sur des blocs, qu'elles soient générées à l'aide de la sauvegarde quotidienne automatique ou de la fonction de sauvegarde initiée par l'utilisateur. Cela signifie que lorsque vous effectuez une sauvegarde, Amazon FSx compare les données de votre système de fichiers à celles de votre sauvegarde précédente au niveau des blocs. Amazon FSx stocke ensuite une copie de toutes les modifications apportées au niveau des blocs dans la nouvelle sauvegarde. Les données au niveau des blocs qui restent inchangées depuis la sauvegarde précédente ne sont pas stockées dans la nouvelle sauvegarde. La durée du processus de sauvegarde dépend de la quantité de données modifiée depuis la dernière sauvegarde et est indépendante de la capacité de stockage du système de fichiers. La liste suivante illustre les durées de sauvegarde dans différentes circonstances :

- La sauvegarde initiale d'un tout nouveau système de fichiers contenant très peu de données ne prend que quelques minutes.
- La sauvegarde initiale d'un tout nouveau système de fichiers effectuée après le chargement TBs des données prend des heures.
- Une deuxième sauvegarde du système de fichiers contenant des données avec un minimum TBs de modifications apportées aux données au niveau du bloc (relativement peu de créations/modifications) prend quelques secondes.
- Une troisième sauvegarde du même système de fichiers après l'ajout et la modification d'une grande quantité de données prend des heures.

Lorsque vous supprimez une sauvegarde, seules les données propres à cette sauvegarde sont supprimées. Chaque sauvegarde FSx destinée à Lustre contient toutes les informations nécessaires pour créer un nouveau système de fichiers à partir de la sauvegarde, ce qui permet de restaurer efficacement un point-in-time instantané du système de fichiers.

La création de sauvegardes régulières pour votre système de fichiers est une bonne pratique qui complète la réplication qu'Amazon FSx for Lustre effectue pour votre système de fichiers. FSx Les sauvegardes Amazon vous aident à répondre à vos besoins en matière de conservation des sauvegardes et de conformité. Il est facile d'utiliser Amazon FSx pour les sauvegardes Lustre, qu'il s'agisse de créer des sauvegardes, de copier une sauvegarde, de restaurer un système de fichiers à partir d'une sauvegarde ou de supprimer une sauvegarde.

Les sauvegardes ne sont pas prises en charge sur les systèmes de fichiers Scratch, car ces systèmes de fichiers sont conçus pour le stockage temporaire et le traitement des données à court terme. Les sauvegardes ne sont pas prises en charge sur les systèmes de fichiers liés à un compartiment Amazon S3, car le compartiment S3 sert de référentiel de données principal et le système de Lustre fichiers ne contient pas nécessairement l'ensemble de données complet à un moment donné.

Rubriques

- Support de sauvegarde FSx pour Lustre
- Utilisation de sauvegardes quotidiennes automatiques
- Utilisation de sauvegardes initiées par l'utilisateur
- Utilisation AWS Backup avec Amazon FSx
- Copie de sauvegardes
- Copier des sauvegardes au sein d'un même Compte AWS
- Restauration des sauvegardes
- Suppression de sauvegardes

Support de sauvegarde FSx pour Lustre

Les sauvegardes ne sont prises en charge que sur FSx les systèmes de fichiers persistants Lustre qui ne sont pas liés à un référentiel de données Amazon S3.

Amazon FSx ne prend pas en charge les sauvegardes sur les systèmes de fichiers temporaires, car les systèmes de fichiers temporaires sont conçus pour le stockage temporaire et le traitement des données à court terme. Amazon FSx ne prend pas en charge les sauvegardes sur les systèmes de fichiers liés à un compartiment Amazon S3, car le compartiment S3 sert de référentiel de données principal et le système de fichiers ne contient pas nécessairement l'ensemble de données complet à un moment donné. Pour plus d’informations, consultez Options de déploiement et de classe de stockage et Utilisation de référentiels de données.

Utilisation de sauvegardes quotidiennes automatiques

Amazon FSx for Lustre peut effectuer une sauvegarde quotidienne automatique de votre système de fichiers. Ces sauvegardes quotidiennes automatiques ont lieu pendant la fenêtre de sauvegarde quotidienne établie lors de la création du système de fichiers. À un moment donné au cours de la fenêtre de sauvegarde quotidienne, le stockage I/O peut être suspendu brièvement pendant l'initialisation du processus de sauvegarde (généralement pendant moins de quelques secondes). Lorsque vous choisissez votre fenêtre de sauvegarde quotidienne, nous vous recommandons de choisir un moment de la journée qui vous convient. Cette durée se situe idéalement en dehors des heures de fonctionnement normales pour les applications qui utilisent le système de fichiers.

Les sauvegardes quotidiennes automatiques sont conservées pendant une certaine période, connue sous le nom de période de conservation. Vous pouvez définir une période de conservation comprise entre 0 et 90 jours. La définition de la période de rétention sur 0 (zéro) jour désactive les sauvegardes quotidiennes automatiques. La période de conservation par défaut pour les sauvegardes quotidiennes automatiques est de 0 jour. Les sauvegardes quotidiennes automatiques sont supprimées lorsque le système de fichiers est supprimé.

> **Note**
>
> Si vous définissez la période de conservation sur 0 jour, votre système de fichiers n'est jamais automatiquement sauvegardé. Nous vous recommandons vivement d'utiliser des sauvegardes quotidiennes automatiques pour les systèmes de fichiers associés à un niveau quelconque de fonctionnalités critiques.

Vous pouvez utiliser le AWS CLI ou l'un des AWS SDKs pour modifier la fenêtre de sauvegarde et la période de conservation des sauvegardes pour vos systèmes de fichiers. Utilisez l'opération `UpdateFileSystem`API ou la commande `update-file-system`CLI.

Utilisation de sauvegardes initiées par l'utilisateur

Amazon FSx for Lustre vous permet de sauvegarder manuellement vos systèmes de fichiers à tout moment. Vous pouvez le faire à l'aide de la console Amazon FSx for Lustre, de l'API ou de la AWS Command Line Interface (CLI). Vos sauvegardes des systèmes de FSx fichiers Amazon initiées par l'utilisateur n'expirent jamais et sont disponibles aussi longtemps que vous souhaitez les conserver. Les sauvegardes initiées par l'utilisateur sont conservées même après la suppression du système de

fichiers sauvegardé. Vous pouvez supprimer les sauvegardes initiées par l'utilisateur uniquement à l'aide de la console, de l'API ou de la CLI Amazon FSx for Lustre, et elles ne sont jamais supprimées automatiquement par Amazon FSx. Pour de plus amples informations, veuillez consulter Suppression de sauvegardes.

Création de sauvegardes initiées par l'utilisateur

La procédure suivante explique comment créer une sauvegarde initiée par l'utilisateur dans la FSx console Amazon pour un système de fichiers existant.

Pour créer une sauvegarde du système de fichiers initiée par l'utilisateur

1. Ouvrez la console Amazon FSx for Lustre à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord de la console, choisissez le nom du système de fichiers que vous souhaitez sauvegarder.
3. Dans Actions, sélectionnez Créer une sauvegarde.
4. Dans la boîte de dialogue Créer une sauvegarde qui s'ouvre, attribuez un nom à votre sauvegarde. Les noms de sauvegarde peuvent comporter au maximum 256 caractères Unicode, y compris des lettres, des espaces blancs, des chiffres et des caractères spéciaux. + - = _ :/
5. Choisissez Créer une sauvegarde.

Vous venez de créer la sauvegarde de votre système de fichiers. Vous trouverez un tableau de toutes vos sauvegardes dans la console Amazon FSx for Lustre en choisissant Sauvegardes dans la barre de navigation de gauche. Vous pouvez rechercher le nom que vous avez donné à votre sauvegarde, et le tableau filtre pour n'afficher que les résultats correspondants.

Lorsque vous créez une sauvegarde initiée par l'utilisateur comme décrit dans cette procédure, elle possède le type `USER_INITIATED` et le statut Création pendant qu'Amazon FSx crée la sauvegarde. Le statut passe à Transfert lorsque la sauvegarde est transférée vers Amazon S3, jusqu'à ce qu'elle soit entièrement disponible.

Utilisation AWS Backup avec Amazon FSx

AWS Backup est un moyen simple et économique de protéger vos données en sauvegardant vos systèmes de FSx fichiers Amazon. AWS Backup est un service de sauvegarde unifié conçu pour simplifier la création, la copie, 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 :

- Configurez et auditez les AWS ressources que vous souhaitez sauvegarder.
- Automatiser la planification des sauvegardes.
- Définir des politiques de conservation.
- Copiez les sauvegardes entre AWS les régions et les AWS comptes.
- Surveiller toutes les activités de sauvegarde et de restauration récentes.

AWS Backup utilise la fonctionnalité de sauvegarde intégrée d'Amazon FSx. Les sauvegardes effectuées depuis la AWS Backup console présentent le même niveau de cohérence et de performance du système de fichiers, ainsi que les mêmes options de restauration que les sauvegardes effectuées via la FSx console Amazon. Si vous gérez AWS Backup ces sauvegardes, vous bénéficiez de fonctionnalités supplémentaires, telles que des options de rétention illimitées et la possibilité de créer des sauvegardes planifiées toutes les heures. En outre, AWS Backup conserve vos sauvegardes immuables même après la suppression du système de fichiers source. Cela permet de se protéger contre les suppressions accidentelles ou malveillantes.

Les sauvegardes créées par AWS Backup ont un type de sauvegarde `AWS_BACKUP` et sont incrémentielles par rapport à toutes les autres FSx sauvegardes Amazon que vous effectuez de votre système de fichiers. Les sauvegardes effectuées par AWS Backup sont considérées comme des sauvegardes initiées par l'utilisateur et sont prises en compte dans le quota de sauvegarde initié par l'utilisateur pour Amazon. FSx Vous pouvez consulter et restaurer les sauvegardes effectuées AWS Backup dans la FSx console, la CLI et l'API Amazon. Toutefois, vous ne pouvez pas supprimer les sauvegardes effectuées AWS Backup dans la FSx console, la CLI ou l'API Amazon. Pour plus d'informations sur la façon AWS Backup de sauvegarder vos systèmes de FSx fichiers Amazon, consultez Working with Amazon FSx File Systems dans le manuel du AWS Backup développeur.

Copie de sauvegardes

Vous pouvez utiliser Amazon FSx pour copier manuellement les sauvegardes d'un même AWS compte vers un autre Région AWS (copies interrégionales) ou au sein du même compte Région AWS (copies internes à la région). Vous ne pouvez effectuer des copies entre régions qu'au sein d' AWS

une même partition. Vous pouvez créer des copies de sauvegarde initiées par l'utilisateur à l'aide de la FSx console Amazon ou de l'API. AWS CLI Lorsque vous créez une copie de sauvegarde initiée par l'utilisateur, elle est de type`USER_INITIATED`.

Vous pouvez également l'utiliser AWS Backup pour copier des sauvegardes d'un Régions AWS AWS compte à l'autre. AWS Backup est un service de gestion des sauvegardes entièrement géré qui fournit une interface centrale pour les plans de sauvegarde basés sur des règles. Grâce à sa gestion entre comptes, vous pouvez automatiquement utiliser des politiques de sauvegarde pour appliquer des plans de sauvegarde à tous les comptes de votre organisation.

Les copies de sauvegarde interrégionales sont particulièrement utiles pour la reprise après sinistre entre régions. Vous effectuez des sauvegardes et vous les copiez dans une autre AWS région afin qu'en cas de sinistre dans la région principale Région AWS, vous puissiez effectuer une restauration à partir d'une sauvegarde et rétablir rapidement la disponibilité dans l'autre AWS région. Vous pouvez également utiliser des copies de sauvegarde pour cloner votre ensemble de données de fichiers sur un autre Région AWS ou au sein d'un même jeu de données Région AWS. Vous effectuez des copies de sauvegarde au sein du même AWS compte (entre régions ou régions) à l'aide de la FSx console Amazon ou de l' AWS CLI API Amazon FSx for Lustre. Vous pouvez également l'utiliser AWS Backuppour effectuer des copies de sauvegarde, à la demande ou selon des règles.

Les copies de sauvegarde entre comptes sont utiles pour répondre à vos exigences de conformité réglementaire en matière de copie de sauvegardes sur un compte isolé. Ils fournissent également une couche supplémentaire de protection des données pour empêcher la suppression accidentelle ou malveillante des sauvegardes, la perte d'informations d'identification ou la compromission des AWS KMS clés. Les sauvegardes entre comptes prennent en charge le fan-in (copie des sauvegardes de plusieurs comptes principaux vers un compte de copie de sauvegarde isolé) et le fan-out (copie des sauvegardes d'un compte principal vers plusieurs comptes de copie de sauvegarde isolés).

Vous pouvez créer des copies de sauvegarde entre comptes en les utilisant AWS Backup avec le AWS Organizations support. Les limites des comptes pour les copies entre comptes sont définies par des AWS Organizations politiques. Pour plus d'informations sur l'utilisation AWS Backup pour créer des copies de sauvegarde entre comptes, consultez la section Création de copies de sauvegarde Comptes AWS dans le Guide du AWS Backup développeur.

Limites relatives à la copie de sauvegarde

Les restrictions suivantes s'appliquent lorsque vous copiez des sauvegardes :

- Les sauvegardes de systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering ne prennent pas en charge les copies de sauvegarde.
- Les copies de sauvegarde interrégionales ne sont prises en charge qu'entre deux régions commerciales Régions AWS, entre les régions Chine (Pékin) et Chine (Ningxia), et entre les régions AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest), mais pas entre ces ensembles de régions.
- Les copies de sauvegarde entre régions ne sont pas prises en charge dans les régions optionnelles.
- Vous pouvez créer des copies de sauvegarde régionales dans n'importe quel Région AWS endroit.
- Le statut de la sauvegarde source doit être défini sur « `AVAILABLE` Pour que vous puissiez la copier ».
- Vous ne pouvez pas supprimer une sauvegarde source si elle est copiée. Un court délai peut s'écouler entre le moment où la sauvegarde de destination devient disponible et le moment où vous êtes autorisé à supprimer la sauvegarde source. Vous devez garder ce délai à l'esprit si vous essayez à nouveau de supprimer une sauvegarde source.
- Vous pouvez avoir jusqu'à cinq demandes de copie de sauvegarde en cours vers une seule destination Région AWS par compte.

Autorisations pour les copies de sauvegarde interrégionales

Vous utilisez une déclaration de politique IAM pour accorder l'autorisation d'effectuer une opération de copie de sauvegarde. Pour communiquer avec la AWS région source afin de demander une copie de sauvegarde interrégionale, le demandeur (rôle IAM ou utilisateur IAM) doit avoir accès à la sauvegarde source et à la région source. AWS

Vous utilisez cette politique pour accorder des autorisations à l'`CopyBackup`action relative à l'opération de copie de sauvegarde. Vous spécifiez l'action dans le `Action` champ de la stratégie et vous spécifiez la valeur de la ressource dans le `Resource` champ de la stratégie, comme dans l'exemple suivant.

JSON

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

```
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111122223333:backup/*"
        }
    ]
}
```

Pour plus d'informations sur les politiques IAM, consultez la section Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

Copies complètes et incrémentielles

Lorsque vous copiez une sauvegarde vers une sauvegarde Région AWS différente de la sauvegarde source, la première copie est une copie de sauvegarde complète. Après la première copie de sauvegarde, toutes les copies de sauvegarde suivantes vers la même région de destination au sein du même AWS compte sont incrémentielles, à condition que vous n'ayez pas supprimé toutes les sauvegardes précédemment copiées dans cette région et que vous utilisiez la même clé. AWS KMS Si les deux conditions ne sont pas remplies, l'opération de copie aboutit à une copie de sauvegarde complète (et non incrémentielle).

Copier des sauvegardes au sein d'un même Compte AWS

Vous pouvez copier des sauvegardes de systèmes FSx de fichiers Lustre à l' AWS Management Console aide de la CLI et de l'API, comme décrit dans les procédures suivantes.

Pour copier une sauvegarde au sein du même compte (entre régions ou dans une région) à l'aide de la console

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Sauvegardes.
3. Dans le tableau Sauvegardes, choisissez la sauvegarde que vous souhaitez copier, puis choisissez Copier la sauvegarde.
4. Dans la section Settings (Paramètres), procédez comme suit :

    - Dans la liste Région de destination, choisissez une AWS région de destination dans laquelle copier la sauvegarde. La destination peut se trouver dans une autre AWS région (copie interrégionale) ou dans la même AWS région (copie régionale).

- (Facultatif) Sélectionnez Copier les balises pour copier les balises de la sauvegarde source vers la sauvegarde de destination. Si vous sélectionnez Copier les balises et que vous ajoutez également des balises à l'étape 6, toutes les balises sont fusionnées.

5. Dans le champ Chiffrement, choisissez la clé de AWS KMS chiffrement pour chiffrer la sauvegarde copiée.
6. Pour les balises (facultatif), entrez une clé et une valeur pour ajouter des balises à votre sauvegarde copiée. Si vous ajoutez des balises ici et que vous avez également sélectionné Copier les balises à l'étape 4, toutes les balises sont fusionnées.
7. Choisissez Copier la sauvegarde.

   Votre sauvegarde est copiée à l'intérieur de la même Compte AWS page vers la sauvegarde sélectionnée Région AWS.

Pour copier une sauvegarde dans le même compte (entre régions ou dans une région) à l'aide de la CLI

- Utilisez la commande `copy-backup` CLI ou l'opération CopyBackupAPI pour copier une sauvegarde dans le même AWS compte, que ce soit dans une AWS région ou au sein d'une AWS région.

  La commande suivante copie une sauvegarde dont l'ID est « `backup-0abc123456789cba7` from the `us-east-1` Region ».

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  La réponse indique la description de la sauvegarde copiée.

  Vous pouvez consulter vos sauvegardes sur la FSx console Amazon ou par programmation à l'aide de la commande `describe-backups` CLI ou de l'opération DescribeBackupsAPI.

Restauration des sauvegardes

Vous pouvez utiliser une sauvegarde disponible pour créer un nouveau système de fichiers, en restaurant efficacement un point-in-time instantané d'un autre système de fichiers. Vous pouvez restaurer une sauvegarde à l'aide de la AWS CLI console ou de l'un des AWS SDKs. La restauration

d'une sauvegarde sur un nouveau système de fichiers prend le même temps que la création d'un nouveau système de fichiers. Les données restaurées à partir de la sauvegarde sont chargées latéralement dans le système de fichiers, période pendant laquelle vous constaterez une latence légèrement plus élevée.

> **Note**
>
> Vous ne pouvez restaurer votre sauvegarde que sur un système de fichiers ayant le même type de déploiement, la même classe de stockage, la même capacité de débit, la même capacité de stockage, le même type de compression de données et le même type de compression de données Région AWS que l'original. Vous pouvez augmenter la capacité de stockage de votre système de fichiers restauré une fois qu'il sera disponible.

Pour restaurer un système de fichiers à partir d'une sauvegarde à l'aide de la console

1. Ouvrez la console Amazon FSx for Lustre à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord de la console, choisissez Sauvegardes dans la barre de navigation de gauche.
3. Choisissez la sauvegarde que vous souhaitez restaurer dans le tableau des sauvegardes, puis choisissez Restaurer la sauvegarde.

   L'assistant de création du système de fichiers s'ouvre avec la plupart des paramètres prédéfinis en fonction de la configuration du système de fichiers à partir duquel la sauvegarde a été créée. Vous pouvez éventuellement modifier la configuration du Virtual Private Cloud (VPC) ou choisir une version plus récente de Lustre. Notez que les autres paramètres de configuration, tels que le type de déploiement et le débit par unité de stockage, ne peuvent pas être modifiés pendant la restauration.
4. Complétez l'assistant comme vous le faites lorsque vous créez un nouveau système de fichiers.
5. Choisissez Review and create.
6. Passez en revue les paramètres que vous avez choisis FSx pour votre système de fichiers Amazon for Lustre, puis choisissez Create file system.

Vous avez effectué une restauration à partir d'une sauvegarde et un nouveau système de fichiers est en cours de création. Lorsque son statut passe à`AVAILABLE`, vous pouvez utiliser le système de fichiers normalement.

Suppression de sauvegardes

La suppression d'une sauvegarde est une action permanente irrécupérable. Toutes les données d'une sauvegarde supprimée sont également supprimées. Ne supprimez pas une sauvegarde si vous n'êtes pas certain de ne pas en avoir besoin à nouveau à l'avenir. Vous ne pouvez pas supprimer les sauvegardes effectuées AWS Backup dans la FSx console, la CLI ou l'API Amazon.

Pour supprimer une sauvegarde

1. Ouvrez la console Amazon FSx for Lustre à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord de la console, choisissez Sauvegardes dans la barre de navigation de gauche.
3. Choisissez la sauvegarde que vous souhaitez supprimer dans le tableau des sauvegardes, puis choisissez Supprimer la sauvegarde.
4. Dans la boîte de dialogue Supprimer les sauvegardes qui s'ouvre, vérifiez que l'ID de la sauvegarde identifie la sauvegarde que vous souhaitez supprimer.
5. Vérifiez que la case est cochée pour la sauvegarde que vous souhaitez supprimer.
6. Choisissez Supprimer les sauvegardes.

Votre sauvegarde et toutes les données incluses sont désormais définitivement et irrémédiablement supprimées.

Surveillance des systèmes de fichiers Amazon FSx pour Lustre

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de votre système de fichiers FSx for Lustre et de vos autres AWS solutions. La collecte de données de surveillance provenant de toutes les parties de votre AWS solution vous permet de corriger plus facilement une défaillance multipoint si elle se produit. Vous pouvez surveiller votre système de fichiers FSx for Lustre, signaler un problème et prendre des mesures automatiquement le cas échéant à l'aide des outils suivants :

- Amazon CloudWatch — Surveille vos AWS ressources et les applications que vous exécutez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés et définir des alarmes qui vous avertissent lorsqu'une métrique spécifiée atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre la capacité de stockage ou d'autres indicateurs pour vos instances Amazon FSx for Lustre et lancer automatiquement de nouvelles instances en cas de besoin.
- Journalisation Lustre — Surveille les événements de journalisation activés pour votre système de fichiers. Lustre Logging écrit ces événements dans Amazon CloudWatch Logs.
- AWS CloudTrail— Capture les appels d'API et les événements associés effectués par vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l’adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu.

Les sections suivantes fournissent des informations sur la façon d'utiliser les outils avec vos systèmes de fichiers FSx for Lustre.

Rubriques

- Surveillance avec Amazon CloudWatch
- Journalisation avec Amazon CloudWatch Logs
- Journalisation FSx des appels d'API Lustre avec AWS CloudTrail

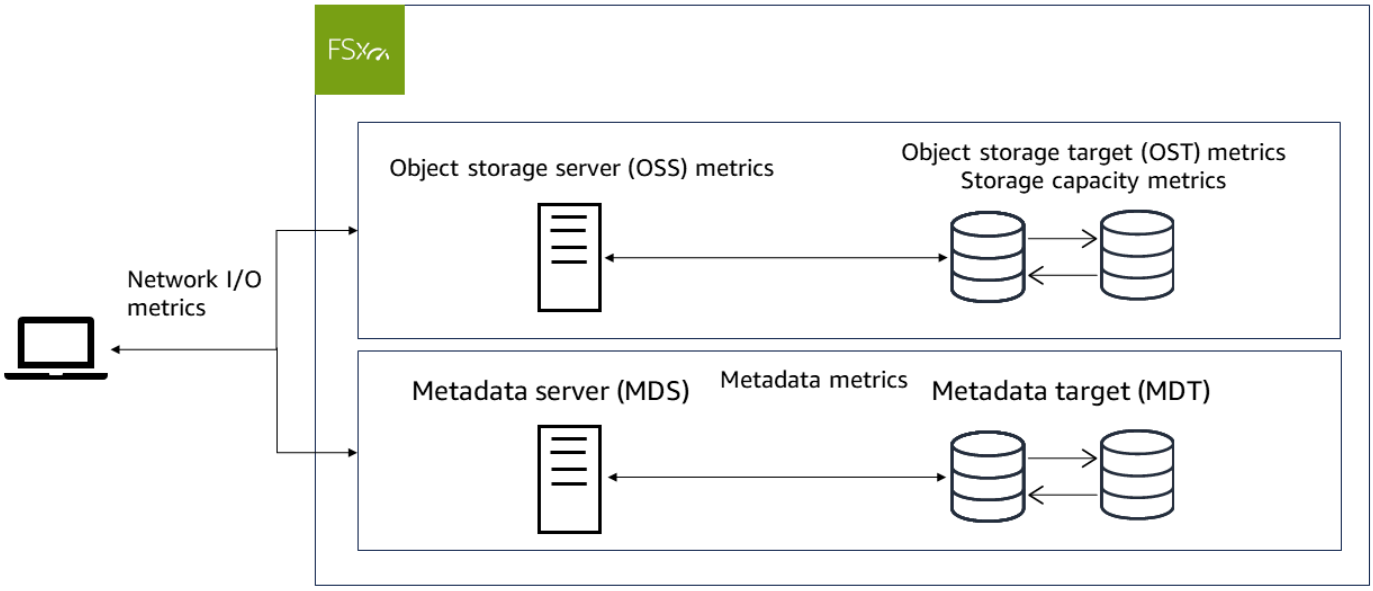
Surveillance avec Amazon CloudWatch

Vous pouvez surveiller Amazon FSx for Lustre en utilisant CloudWatch, qui collecte et traite les données brutes d'Amazon FSx pour Lustre en indicateurs lisibles en temps quasi réel. Ces statistiques sont conservées pendant une période de 15 mois, afin que vous puissiez accéder aux informations historiques et avoir une meilleure idée des performances de votre application ou service. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon.

CloudWatch les indicateurs FSx pour Lustre sont organisés en six catégories :

- I/O Métriques du réseau : mesurez l'activité entre les clients et votre système de fichiers.
- Statistiques du serveur de stockage d'objets : mesurez le débit réseau du serveur de stockage d'objets (OSS) et l'utilisation du débit du disque.
- Mesures relatives aux cibles de stockage d'objets : mesurez le débit du disque cible de stockage d'objets (OST) et le taux d'utilisation des IOPS du disque.
- Métriques de métadonnées : mesurez l'utilisation du processeur du serveur de métadonnées (MDS), l'utilisation des IOPS des cibles de métadonnées (MDT) et les opérations de métadonnées des clients.
- Mesures de capacité de stockage : mesurez l'utilisation de la capacité de stockage.
- Métriques du référentiel de données S3 : mesurez l'âge du plus vieux message en attente d'importation ou d'exportation, et renommez les messages traités par le système de fichiers.

Le schéma suivant illustre un système de fichiers FSx pour Lustre, ses composants et ses catégories métriques.



FSx for Lustre envoie des données métriques à CloudWatch des intervalles d'une minute.

> **Note**
>
> Les métriques ne peuvent pas être publiées pendant les fenêtres de maintenance du système de fichiers de votre système de fichiers Amazon FSx for Lustre.

Rubriques

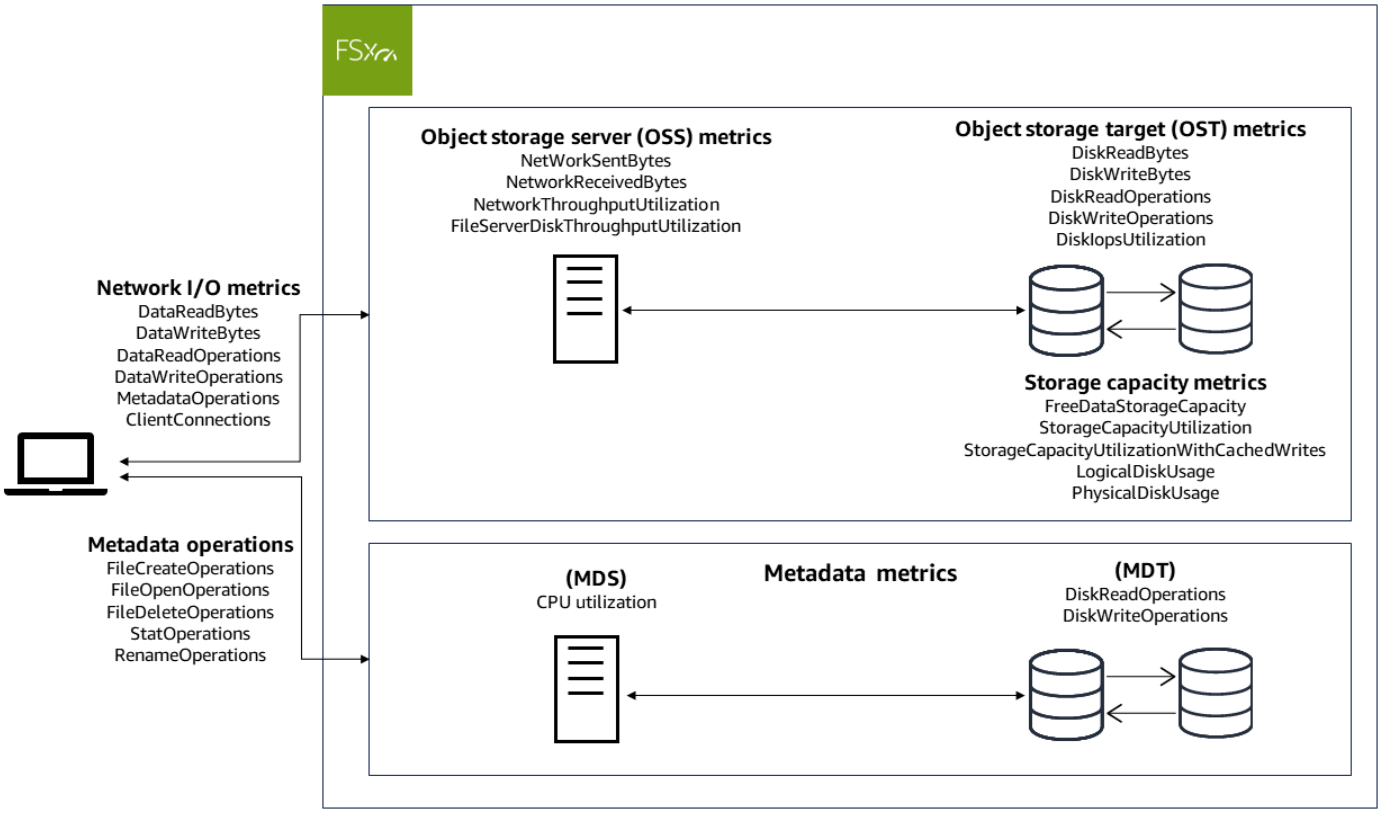
- Comment utiliser les CloudWatch métriques Amazon FSx for Lustre
- Accès aux CloudWatch métriques
- Métriques et dimensions d'Amazon FSx for Lustre
- Avertissements et recommandations en matière de performances
- Création d' CloudWatch alarmes pour surveiller les métriques

Comment utiliser les CloudWatch métriques Amazon FSx for Lustre

Chaque système de fichiers Amazon FSx for Lustre comporte deux composants architecturaux principaux :

- Un ou plusieurs serveurs de stockage d'objets (OSSs) qui fournissent des données aux clients qui accèdent au système de fichiers. Chaque système OSS est attaché à un ou plusieurs volumes de stockage, appelés cibles de stockage d'objets (OSTs), qui hébergent les données de votre système de fichiers.
- Un ou plusieurs serveurs de métadonnées (MDSs) qui fournissent des métadonnées aux clients qui accèdent au système de fichiers. Chaque MDS est attaché à un volume de stockage, appelé cible de métadonnées (MDT), qui stocke des métadonnées telles que les noms de fichiers, les répertoires, les autorisations d'accès et les mises en page des fichiers.

FSx for Lustre fournit des indicateurs permettant de suivre les performances et l'utilisation des ressources des serveurs de stockage et de métadonnées de votre système de fichiers, ainsi que des volumes de stockage associés. CloudWatch Le schéma suivant illustre un système de fichiers Amazon FSx for Lustre avec ses composants architecturaux, ainsi que les CloudWatch indicateurs de performance et de ressources disponibles pour la surveillance.



Vous pouvez utiliser le panneau Surveillance et performance du tableau de bord de votre système de fichiers dans la console Amazon FSx for Lustre pour consulter les indicateurs décrits dans les tableaux suivants. Pour de plus amples informations, veuillez consulter Accès aux CloudWatch métriques.

Activité du système de fichiers (dans l'onglet Résumé)

Comment puis-je...	Diagramme	Métriques pertinentes
... déterminer la capacité de stockage disponible sur mon système de fichiers ?	Capacité de stockage disponible (octets)	`FreeDataStorageCapacity`
... déterminer le débit client total de mon système de fichiers ?	Débit client total (octets/s)	SOMME (`DataReadBytes +DataWriteBytes )`/ PÉRIODE (en secondes)
... déterminer le nombre total d'IOPS des clients de mon système de fichiers ?	Nombre total d'IOPS par seconde du client (opérations/s)	`SUM(DataReadOperations + DataWriteOperations + MetadataOperations )/PERIOD (in seconds)`
... déterminer le nombre de connexions établies entre les clients et mon serveur de fichiers ?	Connexions client (nombre)	`ClientConnections`
... déterminer l'utilisation des performances des métadonnées de mon système de fichiers ?	Utilisation des métadonnées par IOPS (pourcentage)	`MAX(MDT Disk IOPS)`

Onglet de rangement

Comment puis-je...	Diagramme	Métriques pertinentes
... déterminez la quantité de stockage disponible ?	Capacité de stockage disponible (octets)	`FreeDataStorageCapacity`
... déterminer le pourcentage de stockage utilisé pour mon système de fichiers, à l'exclusion de l'espace réservé aux écritures mises en cache sur les clients ?	Utilisation totale de la capacité de stockage (pourcentage)	`StorageCapacityUtilization`
... déterminer le pourcentage de stockage utilisé pour mon système de fichiers, y compris l'espace réservé aux écritures mises en cache sur les clients ?	Utilisation totale de la capacité de stockage (pourcentage)	`StorageCapacityUtilizationWithCachedWrites`
... déterminer le pourcentage de stockage utilisé par mon système de fichiers, à l' OSTs exclusion de l'espace réservé aux écritures mises en cache sur les clients ?	Utilisation totale de la capacité de stockage par OST (pourcentage)	`StorageCapacityUtilization`
... déterminer le pourcentage de stockage utilisé pour mon système de fichiers OSTs, y compris	Utilisation totale de la capacité	`StorageCapacityUtilizationWithCachedWrites`

Comment puis-je...	Diagramme	Métriques pertinentes
l'espace réservé aux écritures mises en cache sur les clients ?	de stockage par OST avec subventions du client (pourcentage)	
... déterminer le taux de compression des données de mon système de fichiers ?	Économies de compression	100* (`LogicalDiskUsage -PhysicalDiskUSage )/LogicalDiskUsage`

Performances du stockage d'objets (dans l'onglet Performances)

Comment puis-je...	Diagramme	Métriques pertinentes
... déterminer le débit réseau entre les clients et le OSSs pourcentage de la limite allouée ?	Débit du réseau (pourcentage)	`NetworkThroughputUtilization`
... déterminer le débit du disque entre le système OSS et son OSTs pourcentage de la limite allouée ?	Débit du disque (pourcentage)	`FileServerDiskThroughputUtilization`
... déterminer les IOPS pour les opérations auxquelles l'accès est OSTs accordé en pourcentage de la limite allouée ?	Nombre d'E/S par seconde sur le disque (pourcentage)	`DiskIopsUtilization`

Performances des métadonnées (dans l'onglet Performances)

Comment puis-je...	Diagramme	Métriques pertinentes
... déterminer le pourcentage d'utilisation du processeur du serveur de métadonnées ?	Utilisation du processeur (pourcentage)	`CPUUtilization`
... déterminer l'utilisation des IOPS par métadonnées en pourcentage de la limite allouée ?	Utilisation des métadonnées par IOPS	`MAX(MDT Disk IOPS)`

Accès aux CloudWatch métriques

Vous pouvez accéder aux métriques FSx d'Amazon for CloudWatch Lustre de différentes manières :

- La console Amazon FSx pour Lustre.
- La CloudWatch console.
- L'interface de ligne de CloudWatch commande (CLI).
- L' CloudWatch API.

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

Utilisation de la console Amazon FSx for Lustre

Pour consulter les statistiques à l'aide de la console Amazon FSx for Lustre

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Systèmes de fichiers, puis choisissez le système de fichiers contenant les mesures que vous souhaitez consulter.
3. Sur la page Résumé, choisissez Surveillance et performances pour voir les indicateurs de votre système de fichiers.

Le panneau Surveillance et performance comporte quatre onglets.

- Choisissez Résumé (onglet par défaut) pour afficher les avertissements, les CloudWatch alarmes et les graphiques actifs relatifs à l'activité du système de fichiers.
- Choisissez Stockage pour afficher la capacité de stockage, les indicateurs d'utilisation et les avertissements actifs.
- Choisissez Performances pour consulter les indicateurs de performance du serveur de fichiers et du stockage, ainsi que les avertissements actifs.
- Choisissez les CloudWatch alarmes pour afficher les graphiques de toutes les alarmes configurées pour votre système de fichiers.

Utilisation de la CloudWatch console

Pour afficher les métriques à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de noms FSx.
4. (Facultatif) Pour afficher une métrique, entrez son nom dans le champ de recherche.
5. (Facultatif) Pour explorer les indicateurs, sélectionnez la catégorie qui correspond le mieux à votre question.

À l'aide du AWS CLI

Pour accéder aux métriques depuis AWS CLI

- Utilisez la commande `list-metrics` avec l'espace de noms `--namespace "AWS/FSx"`. Pour plus d'informations, consultez la référence de la commande AWS CLI.

Utilisation de l' CloudWatch API

Pour accéder aux métriques depuis l' CloudWatch API

- Appelez `GetMetricStatistics`. Pour plus d'informations, consultez Amazon CloudWatch API Reference.

Métriques et dimensions d'Amazon FSx for Lustre

Amazon FSx for Lustre publie les métriques décrites dans les tableaux suivants dans l'espace de `AWS/FSx` noms d'Amazon CloudWatch FSx pour tous les systèmes de fichiers Lustre.

Rubriques

- FSx pour les I/O métriques du réseau Lustre
- FSx pour les métriques du serveur de stockage d'objets Lustre
- FSx pour les métriques cibles de stockage d'objets Lustre
- FSx pour les métriques de métadonnées Lustre
- FSx pour les mesures de capacité de stockage Lustre
- FSx pour les métriques du référentiel Lustre S3
- FSx pour Lustre dimensions

FSx pour les I/O métriques du réseau Lustre

L'espace de `AWS/FSx` noms inclut les I/O métriques réseau suivantes. Toutes ces mesures ont une seule dimension,`FileSystemId`.

Métrique	Description
`DataReadBytes`	Le nombre d'octets entre les lectures effectuées par les clients et le système de fichiers. La `Sum` statistique représente le nombre total d'octets associés aux opérations de lecture pendant la période spécifiée. La `Minimum` statistiq ue représente le nombre minimum d'octets associés aux opération s de lecture sur un seul OST. La `Maximum` statistique représente le nombre maximum d'octets associés aux opérations de lecture sur l'OST. La `Average` statistique est le nombre moyen d'octets associés aux opérations de lecture par OST. La `SampleCount` statistique est le nombre de. OSTs Pour calculer le débit Moyen (octets par seconde) pour une période, divisez la statistique `Sum` par le nombre de secondes constituant la période.

Métrique	Description
	Unités : • Octets pour`Sum`,`Minimum`,`Maximum`,`Average`. • Nombre de `SampleCount` . Statistiques valides : `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`
`DataWriteBytes`	Le nombre d'octets provenant des écritures effectuées par les clients dans le système de fichiers. La statistique `Sum` correspond au nombre total d’octets associés aux opérations d’écriture. La `Minimum` statistique représente le nombre minimum d'octets associés aux opérations d'écriture sur un seul OST. La `Maximum` statistique représente le nombre maximum d'octets associés aux opérations d'écriture sur l'OST. La `Average` statistique est le nombre moyen d'octets associés aux opérations d'écriture par OST. La `SampleCount` statistique est le nombre de. OSTs 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`Sum`,`Minimum`,`Maximum`,`Average`. • Nombre de `SampleCount` . Statistiques valides : `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrique	Description
`DataReadOperations`	Le nombre d'opérations de lecture. La `Sum` statistique représente le nombre total d'opérations de lecture. La `Minimum` statistique représente le nombre minimum d'opérations de lecture sur un seul OST. La `Maximum` statistique représente le nombre maximum d'opérations de lecture sur l'OST. La `Average` statistiq ue représente le nombre moyen d'opérations de lecture par OST. La `SampleCount` statistique est le nombre de. OSTs Pour calculer le nombre moyen d'opérations de lecture (opérations par seconde) pendant une période, divisez la `Sum` statistique par le nombre de secondes de la période. Unités : • Comptez pour `Sum``Minimum`,`Maximum`,`Average`,`SampleCount` .  Statistiques valides : `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt`

Métrique	Description
`DataWrite Operations`	Le nombre d'opérations d'écriture. La `Sum` statistique représente le nombre total d'opérations d'écritur e. La `Minimum` statistique représente le nombre minimum d'opérati ons d'écriture sur un seul OST. La `Maximum` statistique représente le nombre maximum d'opérations d'écriture sur l'OST. La `Average` statistique représente le nombre moyen d'opérations d'écriture par OST. La `SampleCount` statistique est le nombre de. OSTs Pour calculer le nombre moyen d'opérations d'écriture (opérations par seconde) pendant une période, divisez la `Sum` statistique par le nombre de secondes de la période. Unités : • Comptez pour `Sum``Minimum`,`Maximum`,`Average`,`SampleCount` .  Statistiques valides : `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt`

Métrique	Description
`Metadata0 perations`	Le nombre d'opérations de métadonnées. La `Sum` statistique représente le nombre d'opérations de métadonnées. La `Minimum` statistique représente le nombre minimum d'opérations de métadonnées par MDT. La `Maximum` statistique représente le nombre maximum d'opérations de métadonnées par MDT. La `Average` statistiq ue représente le nombre moyen d'opérations de métadonnées par MDT. La `SampleCount` statistique est le nombre de. MDTs Pour calculer le nombre moyen d'opérations de métadonnées (opératio ns par seconde) pour une période, divisez la `Sum` statistique par le nombre de secondes de la période. Unités : • Comptez pour `SumMinimum`,`Maximum`,`Average`,`SampleCount` . Statistiques valides : `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt`
`ClientCon nections`	Nombre de connexions actives entre les clients et le système de fichiers. Unité : nombre

FSx pour les métriques du serveur de stockage d'objets Lustre

L'espace de `AWS/FSx` noms inclut les métriques du serveur de stockage d'objets (OSS) suivantes. Toutes ces mesures prennent deux dimensions, `FileSystemId` et`FileServer`.

- `FileSystemId`— L'ID de AWS ressource de votre système de fichiers.
- `FileServer`— Le nom du serveur de stockage d'objets (OSS) de votre système de Lustre fichiers. Chaque système OSS est approvisionné avec une ou plusieurs cibles de stockage d'objets (OSTs). Les logiciels libres utilisent la convention de dénomination OSS< HostIndex >, qui *`HostIndex`* représente une valeur hexadécimale à 4 chiffres (par exemple,`0SS0001`). L'ID d'un OSS est l'ID du premier OST qui lui est attaché. Par exemple, le premier OSS attaché à `0ST0000` et`0ST0001`, utilisera`0SS0000`, et le second OSS attaché à`0ST0002`, `0ST0003` utilisera`0SS0002`.

Métrique	Description
`NetworkThroughputUtilization`	Utilisation du débit réseau en pourcentage du débit réseau disponible pour votre système de fichiers. Cette métrique est équivalente à la somme `NetworkSentBytes` et `NetworkReceivedBytes` en pourcentage de la capacité de débit réseau d'un système d'exploitation pour votre système de fichiers. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSSs. La `Average` statistique représente l'utilisation moyenne du débit réseau pour le système OSS donné sur la période spécifiée. La `Minimum` statistique représente l'utilisation du débit réseau la plus faible pour le système OSS donné sur une minute, pendant la période spécifiée. La `Maximum` statistique représente le taux d'utilisation du débit réseau le plus élevé pour le système OSS donné sur une minute, pendant la période spécifiée. Unité : pourcentage Statistiques valides : `Average`, `Minimum`, `Maximum`
`NetworkSentBytes`	Le nombre d'octets envoyés par le système de fichiers. L'ensemble du trafic est pris en compte dans cette métrique, y compris les mouvements de données vers et depuis des référentiels de données liés. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSSs. La `Sum` statistique est le nombre total d'octets envoyés sur le réseau par le système OSS donné au cours de la période spécifiée.

Métrique	Description
	La `Average` statistique est le nombre moyen d'octets envoyés sur le réseau par le système OSS donné au cours de la période spécifiée. La `Minimum` statistique est le plus petit nombre d'octets envoyés sur le réseau par le système OSS donné au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'octets envoyés sur le réseau par le système OSS donné au cours de la période spécifiée. Pour calculer le débit envoyé (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes pendant la période spécifiée. Unité : octets Statistiques valides : `SumAverage`,`Minimum`, `Maximum`

Métrique	Description
`NetworkReceivedBytes`	Nombre d'octets reçus par le système de fichiers. L'ensemble du trafic est pris en compte dans cette métrique, y compris les mouvements de données vers et depuis des référentiels de données liés. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSSs. La `Sum` statistique est le nombre total d'octets reçus sur le réseau par le système OSS donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'octets reçus sur le réseau par le système OSS donné au cours de la période spécifiée. La `Minimum` statistique est le plus petit nombre d'octets reçus sur le réseau par le système OSS donné au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'octets reçus sur le réseau par le système OSS donné au cours de la période spécifiée. Pour calculer le débit (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes pendant la période spécifiée. Unité : octets Statistiques valides : `SumAverage`,`Minimum`, `Maximum`

Métrique	Description
`FileServerDiskThroughputUtilization`	Débit du disque entre votre système OSS et le système associé OSTs, sous forme de pourcentage de la limite provisionnée déterminée par la capacité de débit. Cette métrique est équivalente à la somme `DiskReadBytes` et `DiskWriteBytes` en pourcentage de la capacité de débit du disque OSS pour votre système de fichiers. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSSs. La `Average` statistique représente l'utilisation moyenne du débit du disque OSS pour le système OSS donné au cours de la période spécifiée. La `Minimum` statistique représente l'utilisation la plus faible du débit du disque OSS pour le système OSS donné au cours de la période spécifiée. La `Maximum` statistique représente le taux d'utilisation du débit de disque OSS le plus élevé pour le système OSS donné au cours de la période spécifiée. Unité : pourcentage Statistiques valides : `Average`, `Minimum`, `Maximum`

FSx pour les métriques cibles de stockage d'objets Lustre

L'espace de `AWS/FSx` noms inclut les métriques OST (Object Storage Target) suivantes. Toutes ces mesures prennent deux dimensions, `FileSystemId` et`StorageTargetId`.

> **Note**
>
> `DiskReadOperations`et `DiskWriteOperations` les métriques ne sont pas disponibles sur les systèmes de fichiers Scratch, et `DiskIopsUtilization` les métriques ne sont pas disponibles sur les systèmes de fichiers Scratch et Persistent HDD.

Métrique	Description
`DiskReadBytes`	Le nombre d'octets (E/S de disque) de n'importe quel disque est lu à partir de cet OST. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSTs. La `Sum` statistique est le nombre total d'octets lus en une minute à partir de l'OST donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'octets lus chaque minute à partir de l'OST donné au cours de la période spécifiée. La `Minimum` statistique est le plus petit nombre d'octets lus chaque minute à partir de l'OST donné au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'octets lus chaque minute à partir de l'OST donné au cours de la période spécifiée. Pour calculer le débit du disque de lecture (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes de la période. Unité : octets Statistiques valides : `Sum`,`Average`,`Minimum`, et, `Maximum`
`DiskWriteBytes`	Le nombre d'octets (E/S de disque) de n'importe quel disque écrit à partir de cet OST. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSTs. La `Sum` statistique est le nombre total d'octets écrits chaque minute à partir de l'OST donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'octets écrits chaque minute à partir de l'OST donné au cours de la période spécifiée. La `Minimum` statistique est le plus petit nombre d'octets écrits chaque minute à partir de l'OST donné au cours de la période spécifiée.

Métrique	Description
	La `Maximum` statistique représente le plus grand nombre d'octets écrits chaque minute à partir de l'OST donné au cours de la période spécifiée. Pour calculer le débit du disque de lecture (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes de la période Unité : octets Statistiques valides : `SumAverage`,`Minimum`, et, `Maximum`
`DiskRead0 perations`	Nombre d'opérations de lecture (E/S sur disque) sur cet OST. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSTs. La `Sum` statistique est le nombre total d'opérations de lecture effectuées par l'OST donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'opérations de lecture effectuées chaque minute par l'OST donné au cours de la période spécifiée. La `Minimum` statistique représente le plus petit nombre d'opérations de lecture effectuées chaque minute par l'OST donné au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'opérations de lecture effectuées chaque minute par l'OST donné au cours de la période spécifiée. Pour calculer le nombre moyen d'IOPS sur le disque au cours de la période, utilisez la `Average` statistique et divisez le résultat par 60 (secondes). Unités : nombre Statistiques valides : `SumAverage`,`Minimum`, et `Maximum`

Métrique	Description
`DiskWrite Operations`	Nombre d'opérations d'écriture (E/S sur disque) sur cet OST. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSTs. La `Sum` statistique est le nombre total d'opérations d'écriture effectuées par l'OST donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'opérations d'écritur e effectuées chaque minute par l'OST donné au cours de la période spécifiée. La `Minimum` statistique représente le plus petit nombre d'opérations d'écriture effectuées chaque minute par l'OST donné au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'opérations d'écriture effectuées chaque minute par l'OST donné au cours de la période spécifiée. Pour calculer le nombre moyen d'IOPS sur le disque au cours de la période, utilisez la `Average` statistique et divisez le résultat par 60 (secondes). Unités : nombre Statistiques valides : `Sum``Average`,`Minimum`, et `Maximum`

Métrique	Description
`DiskIopsUtilization`	L'utilisation d'un OST par seconde sur le disque, en pourcentage de la limite d'IOPS du disque OST. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSTs. La `Average` statistique représente l'utilisation moyenne des IOPS du disque pour l'OST donné au cours de la période spécifiée. La `Minimum` statistique représente le taux d'utilisation IOPS le plus faible du disque pour l'OST donné au cours de la période spécifiée. La `Maximum` statistique représente le taux d'utilisation IOPS le plus élevé du disque pour l'OST donné au cours de la période spécifiée. Unité : pourcentage Statistiques valides : `Average`, `Minimum`, et `Maximum`

FSx pour les métriques de métadonnées Lustre

L'`AWS/FSx`espace de noms inclut les métriques de métadonnées suivantes. La `CPUUtilization` métrique prend les `FileServer` dimensions `FileSystemId` et, tandis que les autres mesures prennent les `StorageTargetId` dimensions `FileSystemId` et.

- `FileSystemId`— L'ID de AWS ressource de votre système de fichiers.
- `StorageTargetId`— Nom de la cible de métadonnées (MDT). MDTs utilisez la convention de dénomination MDT< MDTIndex > (par exemple,`MDT0001`).
- `FileServer`— Le nom du serveur de métadonnées (MDS) de votre système de Lustre fichiers. Chaque MDS est approvisionné avec une cible de métadonnées (MDT). MDS utilise la convention de dénomination MDS< HostIndex >, qui `HostIndex` représente une valeur hexadécimale à 4 chiffres dérivée à l'aide de l'index MDT sur le serveur. Par exemple, le premier MDS approvisionné avec `MDT0000` utiliseraMDS0000, et le second MDS approvisionné avec utilisera. `MDT0001` `MDS0001` Votre système de fichiers contient plusieurs serveurs de métadonnées si une configuration de métadonnées est spécifiée pour votre système de fichiers.

Métrique	Description
`CPUUtilization`	Pourcentage d'utilisation des ressources du processeur MDS de votre système de fichiers. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers MDSs. La `Average` statistique est l'utilisation moyenne du processeur du MDS sur une période spécifiée. La `Minimum` statistique représente le taux d'utilisation du processeur le plus faible pour le MDS donné au cours de la période spécifiée. La `Maximum` statistique représente le taux d'utilisation du processeur le plus élevé pour le MDS donné au cours de la période spécifiée. Unité : pourcentage Statistiques valides :`Average`, `Minimum` et `Maximum`
`FileCreateOperations`	Nombre total d'opérations de création de fichiers. Unité : nombre
`FileOpenOperations`	Nombre total d'opérations d'ouverture de fichiers. Unité : nombre
`FileDeleteOperations`	Nombre total d'opérations de suppression de fichiers.

Métrique	Description
	Unité : nombre
`StatOperations`	Nombre total d'opérations statistiques. Unité : nombre
`RenameOperations`	Nombre total de renommages de répertoires, qu'il s'agisse de renommages de répertoires sur place ou de renommages entre répertoires. Unité : nombre

FSx pour les mesures de capacité de stockage Lustre

L'`AWS/FSx`espace de noms inclut les mesures de capacité de stockage suivantes. Toutes ces mesures prennent deux dimensions, `StorageTargetId` sauf `FileSystemId` `LogicalDiskUsage` et celles `PhysicalDiskUsage` qui prennent la `FileSystemId` dimension.

Métrique	Description
`FreeDataStorageCapacity`	La quantité de capacité de stockage disponible dans cet OST. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSTs. La `Sum` statistique est le nombre total d'octets disponibles dans l'OST donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'octets disponibles dans l'OST donné au cours de la période spécifiée. La `Minimum` statistique est le plus petit nombre d'octets disponibles dans l'OST donné au cours de la période spécifiée.

Métrique	Description
	La `Maximum` statistique représente le plus grand nombre d'octets disponibles dans l'OST donné au cours de la période spécifiée. Unité : octets Statistiques valides : `SumAverage`,`Minimum`, et `Maximum`
`StorageCapacityUtilization`	L'utilisation de la capacité de stockage pour un système de fichiers OST donné. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSTs. La `Average` statistique représente le taux moyen d'utilisa tion de la capacité de stockage pour un OST donné sur une période spécifiée. La `Minimum` statistique représente le niveau minimum d'utilisation de la capacité de stockage pour un OST donné sur une période spécifiée. La `Maximum` statistique représente le niveau maximal d'utilisation de la capacité de stockage pour un OST donné sur une période spécifiée. Unité : pourcentage Statistiques valides : `Average`, `Minimum`, `Maximum`

Métrique	Description
`StorageCapacityUtilizationWithCachedWrites`	Utilisation de la capacité de stockage pour un système de fichiers OST donné, y compris l'espace réservé aux écritures mises en cache sur le client. Une métrique est émise chaque minute pour chacun de vos systèmes de fichiers OSTs. La `Average` statistique représente le taux moyen d'utilisation de la capacité de stockage pour un OST donné sur une période spécifiée. La `Minimum` statistique représente le niveau minimum d'utilisation de la capacité de stockage pour un OST donné sur une période spécifiée. La `Maximum` statistique représente le niveau maximal d'utilisation de la capacité de stockage pour un OST donné sur une période spécifiée. Unité : pourcentage Statistiques valides : `Average`, `Minimum`, `Maximum`

Métrique	Description
`LogicalDiskUsage`	La quantité de données logiques stockées (non compressées). La `Sum` statistique représente le nombre total d'octets logiques stockés dans le système de fichiers. La `Minimum` statistique est le plus petit nombre d'octets logiques stockés dans un OST dans le système de fichiers. La `Maximum` statistique représente le plus grand nombre d'octets logiques stockés dans un OST du système de fichiers. La `Average` statistique est le nombre moyen d'octets logiques stockés par OST. La `SampleCount` statistique est le nombre de. OSTs Unités : • Octets pour `Sum``Minimum`,`Maximum`. • Nombre de `SampleCount` .  Statistiques valides : `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrique	Description
PhysicalDiskUsage	La quantité de stockage physiquement occupée par les données du système de fichiers (compressées). La Sum statistique représente le nombre total d'octets occupés OSTs dans le système de fichiers. La Minimum statistique est le nombre total d'octets occupés dans l'OST le plus vide. La Maximum statistique est le nombre total d'octets occupés dans l'OST le plus complet. La Average statistique est le nombre moyen d'octets occupés par OST. La SampleCount statistique est le nombre de. OSTs Unités : • Octets pour SumMinimum,Maximum. • Nombre de SampleCount . Statistiques valides : Sum, Minimum, Maximum, Average, SampleCount

FSx pour les métriques du référentiel Lustre S3

FSx for Lustre publie les métriques suivantes AutoImport (importation automatique) et AutoExport (exportation automatique) dans l'espace de FSx noms de. CloudWatch Ces mesures utilisent des dimensions pour permettre des mesures plus précises de vos données. Toutes AutoImport les AutoExport métriques ont les Publisher dimensions « FileSystemId et ».

Métrique	Description
AgeOfOldestQueuedMessage Dimension : AutoExport	Âge, en secondes, du message le plus ancien en attente d'exportation. La Average statistique indique l'âge moyen du plus vieux message en attente d'exporta tion. La Maximum statistique correspond

Métrique	Description
	au nombre maximal de secondes pendant lesquelles un message est resté dans la file d'exportation. La `Minimum` statistique correspond au nombre minimal de secondes pendant lesquelles un message est resté dans la file d'exportation. La valeur zéro indique qu'aucun message n'attend d'être exporté. Unités : secondes Statistiques valides : `Average`, `Minimum`, `Maximum`

Métrique	Description
`RepositoryRenameOperations` Dimension : `AutoExport`	Nombre de renommages traités par le système de fichiers en réponse à un changement de nom de répertoire plus important. La `Sum` statistique représente le nombre total d'opérations de renommage résultant d'un changement de nom de répertoire. La `Average` statistique représente le nombre moyen d'opérations de renommage pour le système de fichiers. La `Maximum` statistique représente le nombre maximal d'opérations de renommage associées à un changemen t de nom de répertoire dans le système de fichiers. La `Minimum` statistique représent e le nombre minimum de renommages associés à un changement de nom de répertoire dans le système de fichiers. Unités : nombre Statistiques valides : `Sum``Average`,`Minimum`,`Maximum`,

Métrique	Description
`AgeOfOldestQueuedMessage` Dimension : `AutoImport`	Âge, en secondes, du message le plus ancien en attente d'importation. La `Average` statistique indique l'âge moyen du plus vieux message en attente d'importation. La `Maximum` statistique correspond au nombre maximal de secondes pendant lesquelles un message est resté dans la file d'importation. La `Minimum` statistique correspond au nombre minimal de secondes pendant lesquelles un message est resté dans la file d'importation. La valeur zéro indique qu'aucun message n'est en attente d'importation. Unités : secondes Statistiques valides : `Average`, `Minimum`, `Maximum`

FSx pour Lustre dimensions

Les métriques Amazon FSx for Lustre utilisent l'espace de `AWS/FSx` noms et utilisent les dimensions suivantes.

- La `FileSystemId` dimension indique l'ID d'un système de fichiers et filtre les métriques que vous demandez à ce système de fichiers individuel. Vous pouvez trouver l'identifiant sur la FSx console Amazon dans le panneau Résumé de la page de détails du système de fichiers, dans le champ ID du système de fichiers. L'ID du système de fichiers prend la forme de*`fs-01234567890123456`*. Vous pouvez également voir l'ID dans la réponse à une commande `describe-file-systems`CLI (l'action d'API équivalente est `DescribeFileSystems`).
- La `StorageTargetId` dimension indique quel OST (cible de stockage d'objets) ou MDT (cible de métadonnées) a publié les métriques de métadonnées. A `StorageTargetId` prend la forme de `OSTxxxx` (par exemple,`OST0001`) ou `MDTxxxx` (par exemple,`MDT0001`).
- La `FileServer` dimension indique ce qui suit

  - Pour les métriques OSS : nom du serveur de stockage d'objets (OSS). Les logiciels libres utilisent la convention de `OSSxxxx` dénomination (par exemple,`OSS0002`).
  - Pour la CPUUtilization métrique : le nom d'un serveur de métadonnées (MDS). Les MDS utilisent la convention de `MDSxxxx` dénomination (par exemple,`MDS0002`).
- La `Publisher` dimension est disponible dans CloudWatch et AWS CLI pour les `AutoImport` métriques `AutoImport` et pour indiquer quel service a publié les métriques.

Pour plus d'informations sur les dimensions, consultez la section Dimensions du guide de CloudWatch l'utilisateur Amazon.

Avertissements et recommandations en matière de performances

FSx for Lustre affiche un avertissement pour CloudWatch les métriques lorsque l'une de ces métriques approche ou dépasse un seuil prédéterminé pour plusieurs points de données consécutifs. Ces avertissements vous fournissent des recommandations pratiques que vous pouvez utiliser pour optimiser les performances de votre système de fichiers.

Les avertissements sont accessibles dans plusieurs zones du tableau de bord de surveillance et de performance de la console Amazon FSx for Lustre. Tous les avertissements et CloudWatch alarmes de FSx performance Amazon actifs ou récents configurés pour le système de fichiers qui sont en état d'alarme apparaissent dans le panneau Surveillance et performances de la section Résumé. L'avertissement apparaît également dans la section du tableau de bord où le graphique métrique est affiché. Ces avertissements disparaissent automatiquement du tableau de bord 24 heures après que les indicateurs sous-jacents soient tombés en dessous du seuil d'avertissement.

Vous pouvez créer des CloudWatch alarmes pour n'importe laquelle des FSx métriques Amazon. Pour de plus amples informations, veuillez consulter Création d' CloudWatch alarmes pour surveiller les métriques.

Utiliser des avertissements relatifs aux performances pour améliorer les performances du système de fichiers

Amazon FSx fournit des recommandations pratiques que vous pouvez utiliser pour optimiser les performances de votre système de fichiers. Vous pouvez prendre les mesures recommandées si vous pensez que le problème persiste ou s'il a un impact sur les performances de votre système de fichiers. En fonction de la métrique qui a déclenché un avertissement, vous pouvez le résoudre en augmentant la capacité de débit, la capacité de stockage ou les IOPS de métadonnées du système de fichiers, comme décrit dans le tableau suivant.

Section du tableau de bord	S'il existe un avertissement pour cette métrique	Faites ceci
Stockage	`Storage capacity utilization`	Augmentez la capacité de stockage de votre système de fichiers. Si l'utilisation de votre capacité de stockage n'est plus élevée que pour un sous-ensemble des cibles de stockage d'objets de votre système de fichiers (OSTs), vous pouvez également rééquilibrer votre charge de travail afin que l'utilisation de votre capacité de stockage soit mieux équilibrée dans l'ensembl e de votre système de fichiers.
	`Storage capacity utilization with cached writes`	Réduisez la taille du cache d'écriture de votre client en configurant le paramètre max_dirty_mb sur vos clients.
Performances de stockage d'objets	`Network throughput`	Augmentez la capacité de débit de votre système de fichiers. Si votre taux d'utilisation du débit est supérieur pour un sous-ensemble des serveurs de stockage d'objets de votre système de fichiers (OSSs), vous pouvez également rééquilibrer votre charge de travail afin que l'utilisation du débit soit mieux équilibrée dans

Section du tableau de bord	S'il existe un avertissement pour cette métrique	Faites ceci
		l'ensemble de votre système de fichiers.
	`Disk throughput`	Augmentez la capacité de débit de votre système de fichiers. Si l'utilisation du débit de votre disque est plus élevée pour un sous-ensemble des serveurs de stockage d'objets de votre système de fichiers (OSSs), vous pouvez également rééquilibrer votre charge de travail afin que l'utilisation du débit de disque soit mieux équilibrée dans l'ensemble de votre système de fichiers.
	`Disk IOPS`	Augmentez la capacité de stockage de votre système de fichiers. Si l'utilisation des IOPS de votre disque est plus élevée pour un sous-ensemble des cibles de stockage d'objets de votre système de fichiers (OSTs), vous pouvez également rééquilibrer votre charge de travail afin que l'utilisation des IOPS sur le disque soit mieux équilibrée dans l'ensemble de votre système de fichiers.

Section du tableau de bord	S'il existe un avertissement pour cette métrique	Faites ceci
Performances des métadonnées	`CPU utilization`	Augmentez la capacité de stockage de votre système de fichiers. Si vous devez adapter les performances des métadonnées indépendamment de la capacité de stockage, vous pouvez migrer vers un nouveau système de fichiers qui prend en charge le provisionnement des performances des métadonnées indépendamment de la capacité de stockage à l'aide du MetadataConfiguration paramètre.
	`Metadata IOPS`	Augmentez les IOPS de métadonnées de votre système de fichiers.

Pour plus d'informations sur les performances du système de fichiers, consultezAmazon FSx pour les performances de Lustre.

Création d' CloudWatch alarmes pour surveiller les métriques

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une seule métrique sur une période que vous spécifiez et exécute une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur une période spécifiée. 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 car elles sont dans un état particulier. L'état doit changer et rester modifié pendant une période spécifiée. Vous pouvez créer une alarme sur la FSx console Amazon ou sur la CloudWatch console.

Les procédures suivantes décrivent comment créer des alarmes pour Amazon FSx for Lustre à l'aide de la console et de l'API. AWS CLI

Pour configurer des alarmes à l'aide de la console Amazon FSx for Lustre

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Systèmes de fichiers, puis choisissez le système de fichiers pour lequel vous souhaitez créer l'alarme.
3. Sur la page Résumé, sélectionnez Surveillance et performances.
4. Choisissez Créer une CloudWatch alarme. Vous êtes ensuite redirigé vers la console CloudWatch.
5. Choisissez Select metrics, puis Next.
6. Dans la section Metrics, choisissez FSX.
7. Choisissez File System Metrics, choisissez la métrique pour laquelle vous souhaitez définir l'alarme, puis sélectionnez Select metric.
8. Dans la section Conditions, choisissez les conditions de l'alarme, puis cliquez sur Suivant.

   > **Note**
   >
   > Les métriques peuvent ne pas être publiées pendant la maintenance du système de fichiers. Pour éviter toute modification inutile et trompeuse des conditions d'alarme et pour configurer vos alarmes de manière à ce qu'elles résistent aux points de données manquants, consultez la section Configuration du traitement des données manquantes par les CloudWatch alarmes dans le guide de CloudWatch l'utilisateur Amazon.

9. Si vous souhaitez vous CloudWatch envoyer un e-mail ou une notification SNS lorsque l'état d'alarme déclenche l'action, choisissez Chaque fois que cet état d'alarme est activé.

   Pour Sélectionner une rubrique SNS, 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. Choisissez Suivant.

> **Warning**
>
> 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.

10. Renseignez les valeurs Name, Description et Whenever de la métrique, puis choisissez Next.
11. Sur la page de prévisualisation et de création, passez en revue l'alarme et choisissez Créer une alarme.

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. Choisissez Créer une alarme pour démarrer l'assistant de création d'alarme.
3. Choisissez FSx Metrics pour localiser une métrique. Pour affiner les résultats, vous pouvez rechercher l'ID de votre système de fichiers. Sélectionnez la métrique pour laquelle vous souhaitez créer une alarme et choisissez Next.
4. Entrez un nom et une description, puis choisissez une valeur Whenever pour la métrique.
5. Si vous souhaitez vous CloudWatch envoyer un e-mail lorsque l'état d'alarme est atteint, choisissez State is ALARM pour Whenever this alarm. Pour Envoyer une notification à, sélectionnez une rubrique SNS existante. Si vous sélectionnez Créer un sujet, vous pouvez configurer les noms et adresses e-mail d'une nouvelle liste d'abonnement par e-mail. La liste est enregistrée et s'affiche dans le champ des alarmes futures.

> **Warning**
>
> 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. Affichez l'aperçu de l'alarme, puis choisissez Créer une alarme ou revenez en arrière pour apporter des modifications.

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 régler une alarme à l'aide du CloudWatch

- Appelez `PutMetricAlarm`. Pour plus d'informations, consultez Amazon CloudWatch API Reference.

Journalisation avec Amazon CloudWatch Logs

FSx for Lustre prend en charge l'enregistrement des événements d'erreur et d'avertissement relatifs aux référentiels de données associés à votre système de fichiers dans Amazon CloudWatch Logs.

> **Note**
>
> La journalisation avec Amazon CloudWatch Logs n'est disponible sur Amazon que FSx pour les systèmes de fichiers Lustre créés après 15 h PST le 30 novembre 2021.

Rubriques

- Aperçu de la journalisation
- Destinations des journaux
- Gestion de la journalisation
- Affichage des journaux

Aperçu de la journalisation

Si vous avez des référentiels de données liés à votre système de fichiers FSx for Lustre, vous pouvez activer l'enregistrement des événements du référentiel de données dans Amazon CloudWatch Logs. Les événements d'erreur et d'avertissement peuvent être enregistrés pour les événements

d'importation, d'exportation et de restauration. Pour plus d'informations sur ces opérations et sur les liens vers des référentiels de données, consultezUtilisation de référentiels de données avec Amazon FSx for Lustre.

Vous pouvez configurer les niveaux de journalisation enregistrés par Amazon FSx , c'est-à-dire déterminer si Amazon FSx enregistrera uniquement les événements d'erreur, uniquement les événements d'avertissement, ou à la fois les événements d'erreur et d'avertissement. Vous pouvez également désactiver la déconnexion des événements à tout moment.

> **Note**
>
> Nous vous recommandons vivement d'activer les journaux pour les systèmes de fichiers associés à un niveau quelconque de fonctionnalités critiques.

Destinations des journaux

Lorsque la journalisation est activée, FSx Lustre doit être configuré avec une destination Amazon CloudWatch Logs. La destination du journal des événements est un groupe de CloudWatch journaux Amazon Logs, et Amazon FSx crée un flux de journal pour votre système de fichiers au sein de ce groupe de journaux. CloudWatch Logs vous permet de stocker, de consulter et de rechercher des journaux d'événements d'audit dans la CloudWatch console Amazon, d'exécuter des requêtes sur les journaux à l'aide CloudWatch de Logs Insights et de déclencher des CloudWatch alarmes ou des fonctions Lambda.

Vous choisissez la destination du journal lorsque vous créez votre système de fichiers FSx for Lustre ou ultérieurement en le mettant à jour. Pour de plus amples informations, veuillez consulter Gestion de la journalisation.

Par défaut, Amazon FSx crée et utilise un groupe de CloudWatch journaux Logs par défaut dans votre compte comme destination du journal des événements. Si vous souhaitez utiliser un groupe de journaux de CloudWatch journaux personnalisé comme destination du journal des événements, voici les exigences relatives au nom et à l'emplacement de la destination du journal des événements :

- Le nom du groupe de CloudWatch journaux Logs doit commencer par le `/aws/fsx/` préfixe.
- Si vous ne disposez pas d'un groupe de CloudWatch journaux Logs existant lorsque vous créez ou mettez à jour un système de fichiers sur la console, Amazon FSx for Lustre peut créer et utiliser un flux de journaux par défaut dans le groupe de CloudWatch `/aws/fsx/lustre`

journaux Logs. Le flux de journal sera créé au format `datarepo_`*`file_system_id`* (par exemple,`datarepo_fs-0123456789abcdef0`).

- Si vous ne souhaitez pas utiliser le groupe de journaux par défaut, l'interface utilisateur de configuration vous permet de créer un groupe de CloudWatch journaux de journaux lorsque vous créez ou mettez à jour votre système de fichiers sur la console.
- Le groupe de CloudWatch journaux Logs de destination doit se trouver sur la même AWS partition Compte AWS que votre système de fichiers Amazon FSx for Lustre. Région AWS

Vous pouvez modifier la destination du journal des événements à tout moment. Dans ce cas, les nouveaux journaux d'événements sont envoyés uniquement à la nouvelle destination.

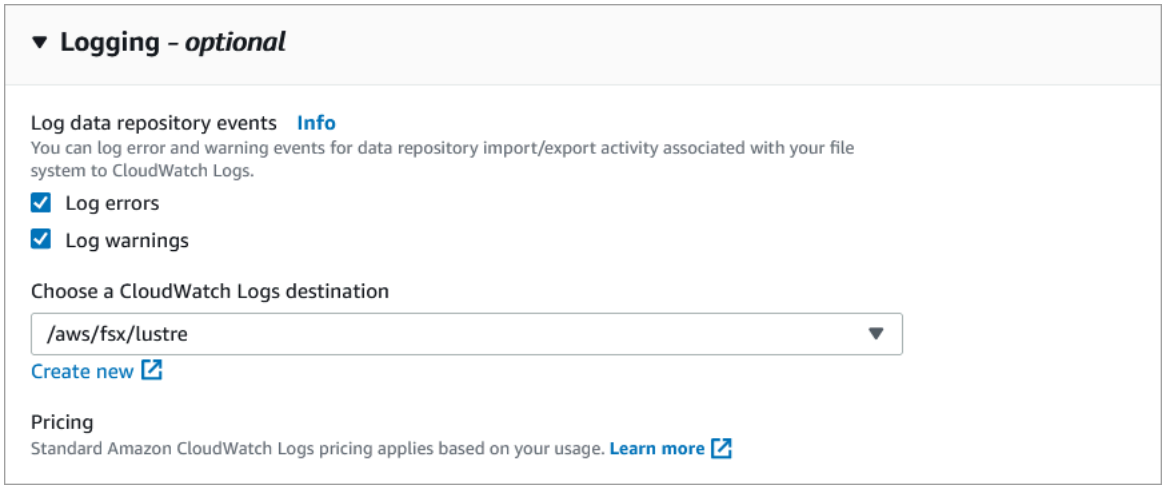
Gestion de la journalisation

Vous pouvez activer la journalisation lorsque vous créez un nouveau système de fichiers FSx pour Lustre ou ultérieurement en le mettant à jour. La journalisation est activée par défaut lorsque vous créez un système de fichiers depuis la FSx console Amazon. Cependant, la journalisation est désactivée par défaut lorsque vous créez un système de fichiers avec l' FSx API Amazon AWS CLI ou Amazon.

Sur les systèmes de fichiers existants sur lesquels la journalisation est activée, vous pouvez modifier les paramètres de journalisation des événements, notamment le niveau de journalisation pour lequel vous souhaitez enregistrer les événements et la destination du journal. Vous pouvez effectuer ces tâches à l'aide de la FSx console Amazon ou de FSx l'API Amazon. AWS CLI

Pour activer la journalisation lors de la création d'un système de fichiers (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau système de fichiers décrite Étape 1 : Créez votre système de fichiers FSx for Lustre dans la section Mise en route.
3. Ouvrez la section Logging - optionnelle. La journalisation est activée par défaut.



4. Passez à la section suivante de l'assistant de création de système de fichiers.

Lorsque le système de fichiers devient disponible, la journalisation est activée.

Pour activer la journalisation lors de la création d'un système de fichiers (CLI)

1. Lorsque vous créez un nouveau système de fichiers, utilisez la `LogConfiguration` propriété avec l'CreateFileSystemopération pour activer la journalisation du nouveau système de fichiers.

```
create-file-system --file-system-type LUSTRE \
    --storage-capacity 1200 --subnet-id subnet-08b31917a72b548a9  \
    --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
        Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
testEventLogging"}"
```

2. Lorsque le système de fichiers devient disponible, la fonctionnalité de journalisation est activée.

Pour modifier la configuration de journalisation (console)

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de Lustre fichiers pour lequel vous souhaitez gérer la journalisation.
3. Choisissez l'onglet Référentiel de données.
4. Dans le panneau de journalisation, choisissez Mettre à jour.
5. Dans la boîte de dialogue Mettre à jour la configuration de la journalisation, modifiez les paramètres souhaités.

a. Choisissez Enregistrer les erreurs pour enregistrer uniquement les événements d'erreur, ou Enregistrer les avertissements pour n'enregistrer que les événements d'avertissement, ou les deux. La journalisation est désactivée si vous n'effectuez aucune sélection.

b. Choisissez une destination de journal CloudWatch Logs existante ou créez-en une nouvelle.

6. Choisissez Enregistrer.

Pour modifier la configuration de journalisation (CLI)

- Utilisez la commande `update-file-system`CLI ou l'opération `UpdateFileSystem`API équivalente.

```
update-file-system --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
        Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
testEventLogging"}"
```

Affichage des journaux

Vous pouvez consulter les journaux une fois qu'Amazon FSx a commencé à les émettre. Vous pouvez consulter les journaux comme suit :

- Vous pouvez consulter les journaux en accédant à la CloudWatch console Amazon et en choisissant le groupe de journaux et le flux de journaux auxquels vos journaux d'événements sont envoyés. Pour plus d'informations, consultez Afficher les données de journal envoyées à CloudWatch Logs dans le guide de l'utilisateur Amazon CloudWatch Logs.
- Vous pouvez utiliser CloudWatch Logs Insights pour rechercher et analyser les données de vos journaux de manière interactive. Pour plus d'informations, consultez Analyser les données des CloudWatch journaux avec Logs Insights dans le guide de l'utilisateur Amazon CloudWatch Logs.
- Vous pouvez également exporter des journaux vers Amazon S3. Pour plus d'informations, consultez Exportation des données de journal vers Amazon S3 dans le guide de l'utilisateur d'Amazon CloudWatch Logs.

Pour en savoir plus sur les causes des défaillances, voirJournaux d'événements du référentiel de données.

Journalisation FSx des appels d'API Lustre avec AWS CloudTrail

Amazon FSx for Lustre 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 FSx for Lustre. CloudTrail capture tous les appels d'API pour Amazon FSx for Lustre sous forme d'événements. Les appels capturés incluent les appels provenant de la console Amazon FSx for Lustre et les appels de code vers les opérations de l'API Amazon FSx for Lustre.

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 FSx for Lustre. 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 qui a été faite à Amazon FSx pour Lustre. Vous pouvez aussi déterminer l'adresse IP à partir de laquelle la demande a été faite, qui a effectué la demande, quand elle a eu lieu et autres informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur Amazon FSx for Lustre dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité d'API a lieu dans Amazon FSx for Lustre, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Amazon FSx for Lustre, créez un parcours. 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 toutes les AWS régions. Le journal enregistre les événements de toutes les AWS régions de la AWS partition et transmet 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 FSx for Lustre sont enregistrés par CloudTrail. Par exemple, les appels aux `TagResource` opérations `CreateFileSystem` et 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 Gestion des identités et des accès AWS (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 en savoir plus, consultez Élément userIdentity CloudTrail dans le Guide de l'utilisateur AWS CloudTrail .

Comprendre les entrées du fichier journal Amazon FSx for Lustre

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 `TagResource` fonctionnement lors de la création d'une balise pour un système de fichiers à partir de la console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
```

```
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`UntagResource`action à effectuer lorsqu'une balise d'un système de fichiers est supprimée de la console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
```

```
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Migrer vers Amazon FSx for Lustre à l'aide de AWS DataSync

Vous pouvez l'utiliser AWS DataSync pour transférer des données entre quatre FSx systèmes de fichiers Lustre. DataSync est un service de transfert de données qui simplifie, automatise et accélère le déplacement et la réplication des données entre des systèmes de stockage autogérés et des services AWS de stockage via Internet ou. Direct Connect DataSync peut transférer les données et les métadonnées de votre système de fichiers, telles que la propriété, les horodatages et les autorisations d'accès.

Comment migrer des fichiers existants vers Lustre FSx à l'aide de AWS DataSync

Vous pouvez utiliser les systèmes de fichiers DataSync with FSx for Lustre pour effectuer des migrations de données ponctuelles, ingérer régulièrement des données pour des charges de travail distribuées et planifier la réplication à des fins de protection et de restauration des données. Pour plus d'informations sur des scénarios de transfert spécifiques, voir Où puis-je transférer mes données AWS DataSync ? dans le guide de AWS DataSync l'utilisateur.

Conditions préalables

Pour migrer les données vers votre configuration FSx for Lustre, vous avez besoin d'un serveur et d'un réseau répondant aux DataSync exigences. Pour en savoir plus, consultez la section Configuration avec AWS DataSync dans le guide de AWS DataSync l'utilisateur.

- Vous avez créé une destination FSx pour le système de fichiers Lustre. Pour de plus amples informations, veuillez consulter Étape 1 : Créez votre système de fichiers FSx for Lustre.
- Les systèmes de fichiers source et de destination sont connectés dans le même cloud privé virtuel (VPC). Le système de fichiers source peut être situé sur site ou dans un autre Amazon VPC Compte AWS, Région AWS ou, mais il doit se trouver dans un réseau connecté à celui du système de fichiers de destination à l'aide d'Amazon VPC Peering, Transit Gateway ou. AWS Direct Connect Site-to-Site VPN Pour plus d’informations, consultez Qu’est-ce que l’appairage de VPC ? dans le Guide d’appairage de VPC Amazon.

> **Note**
>
> DataSync ne peut effectuer un transfert Comptes AWS vers ou FSx depuis Lustre que si l'autre lieu de transfert est Amazon S3.

Étapes de base pour la migration de fichiers à l'aide de DataSync

Le transfert de fichiers d'une source vers une destination DataSync implique les étapes de base suivantes :

1. Téléchargez et déployez un agent dans votre environnement, puis activez-le (inutile en cas de transfert entre deux Services AWS).
2. Créez un emplacement source et un emplacement de destination.
3. Créez une tâche .
4. Exécutez la tâche pour transférer les fichiers depuis la source vers la destination.

Pour plus d’informations, consultez les rubriques suivantes dans le AWS DataSync Guide de l’utilisateur :

- Transfert entre le stockage sur site et AWS
- Configuration des AWS DataSync transferts avec Amazon FSx pour Lustre.
- Déploiement de votre agent Amazon EC2

La sécurité dans Amazon FSx pour Lustre

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le cloud Amazon Web Services. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon FSx for Lustre, voir AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation Amazon FSx for Lustre. Les rubriques suivantes expliquent comment configurer Amazon pour répondre FSx à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser les autres services Amazon qui vous aident à surveiller et à sécuriser votre Amazon FSx for Lustre ressources.

Vous trouverez ci-dessous une description des considérations de sécurité relatives à l'utilisation de Amazon FSx.

Rubriques

- Protection des données dans Amazon FSx for Lustre
- Gestion des identités et des accès pour Amazon FSx for Lustre
- Contrôle d'accès au système de fichiers avec Amazon VPC
- Réseau Amazon VPC ACLs
- Validation de conformité pour Amazon FSx for Lustre
- Amazon FSx pour Lustre et points de terminaison VPC d'interface ()AWS PrivateLink

Protection des données dans Amazon FSx for Lustre

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon FSx for Lustre. 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 Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Amazon FSx ou autre Services AWS à

l'aide de la console AWS CLI, de l'API ou AWS SDKs. 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 FSx for Lustre
- Confidentialité du trafic inter-réseau

Chiffrement des données dans Amazon FSx for Lustre

Amazon FSx for Lustre prend en charge deux formes de chiffrement pour les systèmes de fichiers : le chiffrement des données au repos et le chiffrement des données en transit. Le chiffrement des données au repos est automatiquement activé lors de la création d'un système de FSx fichiers Amazon. Le chiffrement des données en transit est automatiquement activé lorsque vous accédez à un système de FSx fichiers Amazon à partir d' EC2instances Amazon compatibles avec cette fonctionnalité.

Quand utiliser le chiffrement ?

Si votre entreprise est soumise à des politiques d'entreprise ou réglementaires qui exigent le chiffrement des données et des métadonnées au repos, nous vous recommandons de créer un système de fichiers chiffré et de monter votre système de fichiers en cryptant les données en transit.

Pour plus d'informations sur la création d'un système de fichiers chiffré au repos à l'aide de la console, voir Créer votre Amazon FSx for Lustre système de fichiers.

Rubriques

- Chiffrement de données au repos
- chiffrement des données en transit

Chiffrement de données au repos

Le chiffrement des données au repos est automatiquement activé lorsque vous créez un Amazon FSx for Lustre système de fichiers via le AWS Management Console AWS CLI, ou par

programmation via l' FSx API Amazon ou l'un des. AWS SDKs Votre organisation peut exiger le chiffrement de toutes les données qui répondent à une classification spécifique ou qui sont associées à une application, une charge de travail ou un environnement spécifique. Si vous créez un système de fichiers persistant, vous pouvez spécifier la AWS KMS clé avec laquelle chiffrer les données. Si vous créez un système de fichiers scratch, les données sont cryptées à l'aide de clés gérées par Amazon FSx. Pour plus d'informations sur la création d'un système de fichiers chiffré au repos à l'aide de la console, voir Créer votre Amazon FSx for Lustre système de fichiers.

> **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.

Pour plus d'informations sur FSx les utilisations de Lustre AWS KMS, voirComment ? Amazon FSx for Lustre utilise AWS KMS.

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 manière transparente par Amazon FSx for Lustre, vous n'avez donc pas à modifier vos applications.

Amazon FSx for Lustre utilise l'algorithme de chiffrement AES-256 standard pour chiffrer les données du système de fichiers au repos. Pour de plus amples informations, consultez Principes de base du chiffrement dans le Guide du développeur AWS Key Management Service .

Comment ? Amazon FSx for Lustre utilise AWS KMS

Amazon FSx for Lustre chiffre les données automatiquement avant leur écriture dans le système de fichiers et les déchiffre automatiquement au fur et à mesure de leur lecture. Les données sont cryptées à l'aide d'un chiffrement par blocs XTS-AES-256. Tous les systèmes de fichiers Scratch FSx for Lustre sont chiffrés au repos à l'aide de clés gérées par AWS KMS. Amazon FSx for Lustre s'intègre à AWS KMS la gestion des clés. Les clés utilisées pour chiffrer les systèmes de fichiers temporaires au repos sont uniques par système de fichiers et détruites une fois le système de fichiers

supprimé. Pour les systèmes de fichiers persistants, vous choisissez la clé KMS utilisée pour chiffrer et déchiffrer les données. Vous spécifiez la clé à utiliser lorsque vous créez un système de fichiers persistant. Vous pouvez activer, désactiver ou révoquer les autorisations sur cette clé KMS. Cette clé KMS peut être de l'un des deux types suivants :

- Clé gérée par AWS pour Amazon FSx — Il s'agit de la clé KMS par défaut. La création et le stockage d'une clé KMS ne vous sont pas facturés, mais des frais d'utilisation s'appliquent. Pour en savoir plus, consultez Pricing AWS Key Management Service (Tarification).
- 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.

Si vous utilisez une clé gérée par le client comme clé KMS pour le chiffrement et le déchiffrement des données de fichiers, vous pouvez activer la rotation des clés. 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.

> **Important**
>
> Amazon FSx accepte uniquement les clés KMS de chiffrement symétriques. Vous ne pouvez pas utiliser de clés KMS asymétriques avec Amazon FSx.

Politiques FSx clés d'Amazon pour AWS KMS

Les politiques de clé constituent le principal moyen de contrôler l'accès aux clés KMS. Pour plus d'informations sur les politiques clés, consultez la section Utilisation des politiques clés AWS KMS dans le Guide du AWS Key Management Service développeur.La liste suivante décrit toutes les autorisations AWS KMS associées prises en charge par Amazon FSx 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 KMS, sans exposer le texte clair des données côté client. Les données sont d'abord déchiffrées, puis chiffrées à nouveau. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : GenerateDataKeyWithoutPlaintext — (Obligatoire) Renvoie une clé de chiffrement des données chiffrée sous une clé KMS. Cette autorisation est incluse dans la politique clé par défaut sous kms : GenerateDataKey *.
- kms : CreateGrant — (Obligatoire) Ajoute une autorisation à une clé pour spécifier qui peut utiliser la clé et dans quelles conditions. Les octrois sont des mécanismes d'autorisation alternatifs aux stratégies de clé. Pour plus d'informations sur les subventions, consultez la section Utilisation des subventions dans le Guide du AWS Key Management Service développeur. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : DescribeKey — (Obligatoire) Fournit des informations détaillées sur la clé KMS 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 remplit la liste pour sélectionner la clé 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.

chiffrement des données en transit

Scratch 2 et les systèmes de fichiers persistants peuvent chiffrer automatiquement les données en transit lorsque le système de fichiers est accessible à partir d' EC2 instances Amazon qui prennent en charge le chiffrement en transit, ainsi que pour toutes les communications entre les hôtes au sein du système de fichiers. Pour savoir quelles EC2 instances prennent en charge le chiffrement en transit, consultez la section Chiffrement en transit dans le guide de EC2 l'utilisateur Amazon.

Pour obtenir la liste des Régions AWS produits dans lesquels Amazon FSx for Lustre est disponible, consultezDisponibilité du type de déploiement.

Confidentialité du trafic inter-réseau

Cette rubrique décrit comment Amazon FSx sécurise les connexions entre le service et d'autres sites.

Trafic entre Amazon FSx et les clients sur site

Vous disposez de deux options de connectivité entre votre réseau privé et AWS :

- Une AWS Site-to-Site VPN connexion. Pour plus d'informations, voir Qu'est-ce que c'est AWS Site-to-Site VPN ?
- Une AWS Direct Connect connexion. Pour plus d'informations, voir Qu'est-ce que c'est AWS Direct Connect ?

Vous pouvez accéder à FSx Lustre via le réseau pour accéder aux opérations d'API AWS publiées pour effectuer des tâches administratives et Lustre ports pour interagir avec le système de fichiers.

Chiffrer le trafic des API

Pour accéder aux opérations d'API AWS publiées, les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2 ou version ultérieure. Nous exigeons TLS 1.2 et recommandons TLS 1.3. Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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 le AWS Security Token Service (STS) pour générer des informations de sécurité temporaires afin de signer les demandes.

Chiffrement du trafic de données

Le chiffrement des données en transit est activé à partir des EC2 instances prises en charge qui accèdent aux systèmes de fichiers depuis le AWS Cloud. Pour plus d'informations, consultezchiffrement des données en transit. FSx for Lustre n'offre pas de chiffrement natif lors du transit entre les clients sur site et les systèmes de fichiers.

Gestion des identités et des accès pour Amazon FSx for Lustre

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon FSx . IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités

- Gestion de l’accès à l’aide de politiques
- Comment Amazon FSx for Lustre fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour Amazon for Lustre FSx
- AWS politiques gérées pour Amazon FSx for Lustre
- Résolution des problèmes d'identité et d'accès à Amazon FSx for Lustre
- Utiliser des tags avec Amazon FSx
- Utilisation de rôles liés à un service pour Amazon FSx

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes d'identité et d'accès à Amazon FSx for Lustre)
- Administrateur du service : déterminez l’accès des utilisateurs et soumettez les demandes d’autorisation (voir Comment Amazon FSx for Lustre fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l’accès (voir Exemples de politiques basées sur l'identité pour Amazon for Lustre FSx)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d’informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l’utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d’informations, consultez Signature AWS Version 4 pour les demandes d’API dans le Guide de l’utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, 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 qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et 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. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies 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. Vous devez spécifier un principal dans une politique basée sur les ressources.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon FSx for Lustre fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon FSx, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Amazon. FSx

Fonctionnalités IAM que vous pouvez utiliser avec Amazon FSx pour Lustre

Fonctionnalité IAM	FSx Assistance Amazon
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d’identification temporaires	Oui
Transmission des sessions d’accès (FAS)	Oui
Rôles du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Amazon FSx et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Amazon FSx

Prend en charge les politiques basées sur l’identité : oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Définition d’autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. 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 l'identité pour Amazon FSx

Pour consulter des exemples de politiques FSx basées sur l'identité d'Amazon, consultez. Exemples de politiques basées sur l'identité pour Amazon for Lustre FSx

Politiques basées sur les ressources au sein d'Amazon FSx

Prend en charge les politiques basées sur les ressources : non

Actions politiques pour Amazon FSx

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des FSx actions Amazon, consultez la section Actions définies par Amazon FSx pour Lustre dans le Service Authorization Reference.

Les actions politiques sur Amazon FSx utilisent le préfixe suivant avant l'action :

```
fsx
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Pour consulter des exemples de politiques FSx basées sur l'identité d'Amazon, consultez. Exemples de politiques basées sur l'identité pour Amazon for Lustre FSx

Ressources relatives aux politiques pour Amazon FSx

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de FSx ressources Amazon et leurs caractéristiques ARNs, consultez la section Ressources définies par Amazon FSx pour Lustre dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon FSx pour Lustre.

Pour consulter des exemples de politiques FSx basées sur l'identité d'Amazon, consultez. Exemples de politiques basées sur l'identité pour Amazon for Lustre FSx

Clés relatives aux conditions de politique pour Amazon FSx

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de FSx condition Amazon, consultez la section Clés de condition pour Amazon FSx pour Lustre dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon FSx pour Lustre.

Pour consulter des exemples de politiques FSx basées sur l'identité d'Amazon, consultez. Exemples de politiques basées sur l'identité pour Amazon for Lustre FSx

Listes de contrôle d'accès (ACLs) sur Amazon FSx

Supports ACLs : Non

Contrôle d'accès basé sur les attributs (ABAC) avec Amazon FSx

Prise en charge d’ABAC (balises dans les politiques) : Oui

Le contrôle d’accès par attributs (ABAC) est une stratégie d’autorisation qui définit les autorisations en fonction des attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l’accès basé sur des étiquettes, vous devez fournir les informations d’étiquette dans l’élément de condition d’une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d’informations sur ABAC, consultez Définition d’autorisations avec l’autorisation ABAC dans le Guide de l’utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l’ABAC, consultez Utilisation du contrôle d’accès par attributs (ABAC) dans le Guide de l’utilisateur IAM.

Pour plus d'informations sur le balisage des FSx ressources Amazon, consultezMarquez vos ressources Amazon FSx for Lustre.

Pour visualiser un exemple de politique basée sur l’identité permettant de limiter l’accès à une ressource en fonction des balises de cette ressource, consultez Utilisation de balises pour contrôler l'accès à vos FSx ressources Amazon.

Utilisation d'informations d'identification temporaires avec Amazon FSx

Prend en charge les informations d’identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d’informations, consultez Informations d’identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l’utilisateur IAM.

Transférer les sessions d'accès pour Amazon FSx

Prend en charge les sessions d’accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d’accès.

Rôles de service pour Amazon FSx

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu’un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d’IAM. Pour plus d’informations, consultez Création d’un rôle pour la délégation d’autorisations à un Service AWS dans le Guide de l’utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les FSx fonctionnalités d'Amazon. Modifiez les rôles de service uniquement lorsque Amazon FSx fournit des conseils à cet effet.

Rôles liés à un service pour Amazon FSx

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création et la gestion des rôles FSx liés aux services Amazon, consultez. Utilisation de rôles liés à un service pour Amazon FSx

Exemples de politiques basées sur l'identité pour Amazon for Lustre FSx

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier FSx des ressources Amazon. 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.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Amazon FSx, y compris le format ARNs de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon FSx for Lustre dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la FSx console Amazon
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer FSx des ressources Amazon dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à

vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la FSx console Amazon

Pour accéder à la console Amazon FSx for Lustre, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux FSx ressources Amazon présentes dans votre Compte AWS. Si vous

créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la FSx console Amazon, associez également la politique `AmazonFSxConsoleReadOnlyAccess` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Vous pouvez consulter les politiques relatives `AmazonFSxConsoleReadOnlyAccess` aux services FSx gérés d'Amazon et les autres dansAWS politiques gérées pour Amazon FSx for Lustre.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour Amazon FSx for Lustre

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d’utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d’informations, consultez Politiques gérées par AWS dans le Guide de l’utilisateur IAM.

Amazon FSx ServiceRolePolicy

Permet FSx à Amazon de gérer les AWS ressources en votre nom. Pour en savoir plus, consultez Utilisation de rôles liés à un service pour Amazon FSx.

AWS politique gérée : Amazon FSx DeleteServiceLinkedRoleAccess

Vous ne pouvez pas joindre de `AmazonFSxDeleteServiceLinkedRoleAccess` à vos entités IAM. Cette politique est liée à un service et utilisée uniquement avec le rôle lié au service pour ce service. Vous ne pouvez pas joindre, détacher, modifier ou supprimer cette politique. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon FSx.

Cette politique accorde des autorisations administratives qui permettent FSx à Amazon de supprimer son rôle lié au service pour l'accès à Amazon S3, utilisé uniquement par Amazon FSx pour Lustre.

Détails de l'autorisation

Cette politique inclut des autorisations permettant `iam` FSx à Amazon de consulter, de supprimer et de consulter le statut de suppression des rôles liés au FSx service pour l'accès à Amazon S3.

Pour consulter les autorisations associées à cette politique, consultez Amazon FSx DeleteServiceLinkedRoleAccess dans le AWS Managed Policy Reference Guide.

AWS politique gérée : Amazon FSx FullAccess

Vous pouvez associer Amazon FSx FullAccess à vos entités IAM. Amazon associe FSx également cette politique à un rôle de service qui permet FSx à Amazon d'effectuer des actions en votre nom.

Fournit un accès complet à Amazon FSx et aux AWS services associés.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux un accès complet pour effectuer toutes les FSx actions Amazon, à l'exception `BypassSnaplockEnterpriseRetention` de.
- `ds`— Permet aux directeurs d'accéder aux informations relatives aux Directory Service annuaires.
- `ec2`
  - Permet aux principaux de créer des balises dans les conditions spécifiées.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
- `iam`— Permet aux principes de créer un rôle lié à un FSx service Amazon au nom de l'utilisateur. Cela est nécessaire pour qu'Amazon FSx puisse gérer les AWS ressources au nom de l'utilisateur.

- `firehose`— Permet aux directeurs d'écrire des enregistrements sur un Amazon Data Firehose. Cela est nécessaire FSx pour que les utilisateurs puissent surveiller l'accès au système de fichiers Windows File Server en envoyant des journaux d'accès d'audit à Firehose.
- `logs`— Permet aux principaux de créer des groupes de journaux, des flux de journaux et d'écrire des événements dans des flux de journaux. Cela est nécessaire FSx pour que les utilisateurs puissent surveiller l'accès au système de fichiers Windows File Server en envoyant les journaux d'accès aux audits à CloudWatch Logs.

Pour consulter les autorisations associées à cette politique, consultez Amazon FSx FullAccess dans le AWS Managed Policy Reference Guide.

AWS politique gérée : Amazon FSx ConsoleFullAccess

Vous pouvez associer la politique `AmazonFSxConsoleFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès complet à Amazon FSx et l'accès aux AWS services associés via le AWS Management Console.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux d'effectuer toutes les actions dans la console de FSx gestion Amazon, à l'exception `BypassSnaplockEnterpriseRetention` de.
- `cloudwatch`— Permet aux principaux de consulter les CloudWatch alarmes et les statistiques dans la console FSx de gestion Amazon.
- `ds`— Permet aux principaux de répertorier les informations relatives à un Directory Service répertoire.
- `ec2`
  - Permet aux principaux de créer des balises sur les tables de routage, de répertorier les interfaces réseau, les tables de routage, les groupes de sécurité, les sous-réseaux et le VPC associé à un système de fichiers Amazon. FSx
  - Permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
  - Permet aux principaux de visualiser les interfaces réseau élastiques associées à un système de FSx fichiers Amazon.

- `kms`— Permet aux principaux de répertorier les alias des AWS Key Management Service clés.
- `s3`— Permet aux principaux de répertorier certains ou tous les objets d'un compartiment Amazon S3 (jusqu'à 1 000).
- `iam`— Accorde l'autorisation de créer un rôle lié à un service qui permet FSx à Amazon d'effectuer des actions au nom de l'utilisateur.

Pour consulter les autorisations associées à cette politique, consultez Amazon FSx ConsoleFullAccess dans le AWS Managed Policy Reference Guide.

AWS politique gérée : Amazon FSx ConsoleReadOnlyAccess

Vous pouvez associer la politique `AmazonFSxConsoleReadOnlyAccess` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule à Amazon FSx et aux AWS services associés afin que les utilisateurs puissent consulter les informations relatives à ces services dans le. AWS Management Console

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux de consulter les informations relatives aux systèmes de FSx fichiers Amazon, y compris toutes les balises, dans l'Amazon FSx Management Console.
- `cloudwatch`— Permet aux principaux de consulter les CloudWatch alarmes et les statistiques dans l'Amazon FSx Management Console.
- `ds`— Permet aux principaux de consulter les informations relatives à un Directory Service annuaire dans Amazon FSx Management Console.
- `ec2`
  - Permet aux principaux de visualiser les interfaces réseau, les groupes de sécurité, les sous-réseaux et le VPC associé à un système de FSx fichiers Amazon dans Amazon Management Console. FSx
  - Permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
  - Permet aux principaux de visualiser les interfaces réseau élastiques associées à un système de FSx fichiers Amazon.

- `kms`— Permet aux principaux de consulter les alias des AWS Key Management Service clés dans l'Amazon FSx Management Console.
- `log`— Permet aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante FSx pour un système de fichiers Windows File Server.
- `firehose`— Permet aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante FSx pour un système de fichiers Windows File Server.

Pour consulter les autorisations associées à cette politique, consultez Amazon FSx ConsoleReadOnlyAccess dans le AWS Managed Policy Reference Guide.

AWS politique gérée : Amazon FSx ReadOnlyAccess

Vous pouvez associer la politique `AmazonFSxReadOnlyAccess` à vos identités IAM.

- `fsx`— Permet aux principaux de consulter les informations relatives aux systèmes de FSx fichiers Amazon, y compris toutes les balises, dans l'Amazon FSx Management Console.
- `ec2`— Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.

Pour consulter les autorisations associées à cette politique, consultez Amazon FSx ReadOnlyAccess dans le AWS Managed Policy Reference Guide.

Amazon FSx met à jour AWS ses politiques gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon FSx depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la FSx Historique du document page Amazon.

Modifier	Description	Date
Amazon FSx ServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:AssignIpv6Addresses` qui permet aux principaux d'attribuer des IPv6 adresses aux interfaces réseau des clients dotées d'une `AmazonFSx.FileSystemId` balise.	22 juillet 2025
Amazon FSx ServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:UnassignIpv6Addresses` qui permet aux principaux d'annuler l'attribution d' IPv6 adresses aux interfaces réseau des clients dotées d'une `AmazonFSx.FileSystemId` balise.	22 juillet 2025
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `fsx:CreateAndAttachS3AccessPoint` qui permet aux principaux de créer un point d'accès S3 et de l'associer à un FSx volume.	25 juin 2025
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `fsx:DescribeS3AccessPointAttachments` qui permet aux principaux de répertorier tous les points	25 juin 2025

Modifier	Description	Date
	d'accès S3 Compte AWS dans un Région AWS.	
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `fsx:DetachAndDeleteS3AccessPoint` qui permet aux principaux de supprimer un point d'accès S3.	25 juin 2025
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `fsx:CreateAndAttachS3AccessPoint` qui permet aux principaux de créer un point d'accès S3 et de l'associer à un FSx volume.	25 juin 2025
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `fsx:DescribeS3AccessPointAttachments` qui permet aux principaux de répertorier tous les points d'accès S3 Compte AWS dans un Région AWS.	25 juin 2025
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `fsx:DetachAndDeleteS3AccessPoint` qui permet aux principaux de supprimer un point d'accès S3.	25 juin 2025

Modifier	Description	Date
Amazon FSx ConsoleReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:DescribeNetworkInterfaces` qui permet aux principaux de consulter les interfaces réseau élastiques associées à leur système de fichiers.	25 février 2025
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:DescribeNetworkInterfaces` qui permet aux principaux de consulter les interfaces réseau élastiques associées à leur système de fichiers.	07 février 2025
Amazon FSx ServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024

Modifier	Description	Date
Amazon FSx ReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
Amazon FSx ConsoleReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024

Modifier	Description	Date
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation pour permettre aux utilisateurs d'effectuer une réplication de données entre régions et entre comptes FSx pour les systèmes de fichiers OpenZFS.	20 décembre 2023
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation pour permettre aux utilisateurs d'effectuer une réplication de données entre régions et entre comptes FSx pour les systèmes de fichiers OpenZFS.	20 décembre 2023

Modifier	Description	Date
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation permettant aux utilisateurs d'effectuer une réplication à la demande de volumes FSx pour les systèmes de fichiers OpenZFS.	26 novembre 2023
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation permettant aux utilisateurs d'effectuer une réplication à la demande de volumes FSx pour les systèmes de fichiers OpenZFS.	26 novembre 2023
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs d'afficher, d'activer et de désactiver le support VPC partagé FSx pour les systèmes de fichiers ONTAP Multi-AZ.	14 novembre 2023
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs d'afficher, d'activer et de désactiver le support VPC partagé FSx pour les systèmes de fichiers ONTAP Multi-AZ.	14 novembre 2023

Modifier	Description	Date
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de gérer les configurations réseau FSx pour les systèmes de fichiers OpenZFS Multi-AZ.	9 août 2023
AWS politique gérée : Amazon FSx ServiceRolePolicy — Mise à jour d'une politique existante	Amazon a FSx modifié l'`cloudwatch:PutMetricData` autorisation existante afin qu'Amazon FSx publie CloudWatch les métriques dans l'espace de `AWS/FSx` noms.	24 juillet 2023
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon a FSx mis à jour la politique pour supprimer l'`fsx:*`autorisation et ajouter des `fsx` actions spécifiques.	13 juillet 2023
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon a FSx mis à jour la politique pour supprimer l'`fsx:*`autorisation et ajouter des `fsx` actions spécifiques.	13 juillet 2023
Amazon FSx ConsoleReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs de consulter les indicateurs de performance améliorés et les actions recommandées FSx pour les systèmes de fichiers Windows File Server dans la FSx console Amazon.	21 septembre 2022

Modifier	Description	Date
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs de consulter les indicateurs de performance améliorés et les actions recommandées FSx pour les systèmes de fichiers Windows File Server dans la FSx console Amazon.	21 septembre 2022
Amazon FSx ReadOnlyAccess — Politique de suivi mise en place	Cette politique accorde un accès en lecture seule à toutes les FSx ressources Amazon et à tous les tags qui leur sont associés.	4 février 2022
Amazon FSx DeleteServiceLinkedRoleAccess — Politique de suivi mise en place	Cette politique accorde des autorisations administratives qui permettent FSx à Amazon de supprimer son rôle lié au service pour accéder à Amazon S3.	7 janvier 2022
Amazon FSx ServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de gérer les configurations réseau pour les systèmes de fichiers Amazon FSx for NetApp ONTAP.	2 septembre 2021

Modifier	Description	Date
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des balises sur les tables de routage EC2 pour les appels délimités.	2 septembre 2021
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des systèmes de fichiers multi-AZ Amazon FSx pour NetApp ONTAP.	2 septembre 2021
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des balises sur les tables de routage EC2 pour les appels délimités.	2 septembre 2021
Amazon FSx ServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de décrire et d'écrire dans les flux de CloudWatch journaux Logs. Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers FSx pour les systèmes de fichiers Windows File Server à l'aide CloudWatch des journaux.	8 juin 2021

Modifier	Description	Date
Amazon FSx ServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de décrire et d'écrire dans les flux de diffusion Amazon Data Firehose. Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers FSx pour un système de fichiers Windows File Server à l'aide d'Amazon Data Firehose.	8 juin 2021
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire et de créer des journaux, des groupes de CloudWatch journaux, des flux de journaux et d'écrire des événements dans des flux de journaux. Cela est nécessaire pour que les principaux puissent consulter les journaux d'audit d'accès aux fichiers FSx pour les systèmes de fichiers Windows File Server à l'aide des CloudWatch journaux.	8 juin 2021

Modifier	Description	Date
Amazon FSx FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire et d'écrire des enregistrements sur un Amazon Data Firehose. Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers FSx pour un système de fichiers Windows File Server à l'aide d'Amazon Data Firehose.	8 juin 2021
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent choisir un groupe de CloudWatch journaux Logs existant lors de la configuration de l'audit d'accès aux fichiers FSx pour un système de fichiers Windows File Server.	8 juin 2021

Modifier	Description	Date
Amazon FSx ConsoleFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent choisir un flux de diffusion Firehose existant lors de la configuration de l'audit d'accès aux fichiers pour FSx un système de fichiers Windows File Server.	8 juin 2021
Amazon FSx ConsoleReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante FSx pour un système de fichiers Windows File Server.	8 juin 2021

Modifier	Description	Date
Amazon FSx ConsoleReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante FSx pour un système de fichiers Windows File Server.	8 juin 2021
Amazon FSx a commencé à suivre les modifications	Amazon FSx a commencé à suivre les modifications apportées AWS à ses politiques gérées.	8 juin 2021

Résolution des problèmes d'identité et d'accès à Amazon FSx for Lustre

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon FSx et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action sur Amazon FSx
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes FSx ressources Amazon

Je ne suis pas autorisé à effectuer une action sur Amazon FSx

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 `fsx:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx: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 `fsx:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon FSx.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez 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 sur Amazon FSx. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes FSx ressources Amazon

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Amazon FSx prend en charge ces fonctionnalités, consultezComment Amazon FSx for Lustre fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Utiliser des tags avec Amazon FSx

Vous pouvez utiliser des balises pour contrôler l'accès aux FSx ressources Amazon et pour implémenter le contrôle d'accès basé sur les attributs (ABAC). Pour appliquer des balises aux FSx ressources Amazon lors de la création, les utilisateurs doivent disposer de certaines autorisations Gestion des identités et des accès AWS (IAM).

Accorder l'autorisation de baliser les ressources lors de la création

Avec certaines actions de l'API Amazon FSx for Lustre qui créent des ressources, vous pouvez spécifier des balises lors de la création de la ressource. Vous pouvez utiliser ces balises de

ressources pour implémenter le contrôle d'accès basé sur les attributs (ABAC). Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

Pour que les utilisateurs puissent étiqueter les ressources lors de leur création, ils doivent être autorisés à utiliser l'action qui crée la ressource, telle que`fsx:CreateFileSystem`. Si des balises sont spécifiées dans l'action de création de ressources, IAM octroie une autorisation supplémentaire à l'`fsx:TagResource`action afin de vérifier si les utilisateurs sont autorisés à créer des balises. Par conséquent, les utilisateurs doivent également avoir des autorisations explicites d'utiliser l'action `fsx:TagResource`.

L'exemple de politique suivant permet aux utilisateurs de créer des systèmes de fichiers et de leur appliquer des balises lors de leur création dans un système spécifique Compte AWS.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*"
      ]
    }
  ]
}
```

De même, la politique suivante permet aux utilisateurs de créer des sauvegardes sur un système de fichiers spécifique et d'appliquer des balises à la sauvegarde lors de la création de la sauvegarde.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

L'`fsx:TagResource`action est évaluée uniquement si des balises sont appliquées lors de l'action de création de ressources. Par conséquent, un utilisateur autorisé à créer une ressource (en supposant qu'il n'existe aucune condition de balisage) n'a pas besoin d'autorisation pour utiliser l'`fsx:TagResource`action si aucune balise n'est spécifiée dans la demande. Toutefois, si l'utilisateur essaie de créer une ressource avec des balises, la demande échoue s'il n'a pas les autorisations d'utiliser l'action `fsx:TagResource`.

Pour plus d'informations sur le balisage des FSx ressources Amazon, consultezMarquez vos ressources Amazon FSx for Lustre. Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès aux ressources Amazon FSx for Lustre, consultezUtilisation de balises pour contrôler l'accès à vos FSx ressources Amazon.

Utilisation de balises pour contrôler l'accès à vos FSx ressources Amazon

Pour contrôler l'accès aux FSx ressources et aux actions Amazon, vous pouvez utiliser des politiques IAM basées sur des balises. Vous pouvez fournir le contrôle de deux manières :

- Vous pouvez contrôler l'accès aux FSx ressources Amazon en fonction des balises associées à ces ressources.
- Vous pouvez contrôler les balises qui peuvent être transmises dans une condition de demande IAM.

Pour plus d'informations sur l'utilisation des balises pour contrôler l'accès aux AWS ressources, consultez la section Contrôle de l'accès à l'aide de balises dans le guide de l'utilisateur IAM. Pour plus d'informations sur le balisage des FSx ressources Amazon lors de leur création, consultezAccorder l'autorisation de baliser les ressources lors de la création. Pour plus d'informations sur le balisage des ressources, consultez Marquez vos ressources Amazon FSx for Lustre.

Contrôle de l’accès en fonction des balises sur une ressource

Pour contrôler les actions qu'un utilisateur ou un rôle peut effectuer sur une FSx ressource Amazon, vous pouvez utiliser des balises sur la ressource. Par exemple, vous pouvez autoriser ou refuser des opérations d’API spécifiques sur une ressource de système de fichiers en fonction de la paire clé-valeur de la balise sur la ressource.

Example Exemple de politique — Création d'un système de fichiers activé lorsque vous fournissez une balise spécifique

Cette politique permet à l'utilisateur de créer un système de fichiers uniquement lorsqu'il le balise avec une paire clé-valeur spécifique, dans cet exemple,`key=Department, value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example Exemple de politique — Création de sauvegardes uniquement sur les systèmes de fichiers dotés d'une balise spécifique

Cette politique permet aux utilisateurs de créer des sauvegardes uniquement sur les systèmes de fichiers marqués avec la paire `key=Department, value=Finance` clé-valeur, et la sauvegarde sera créée avec la balise`Deparment=Finance`.

JSON

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

```
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Exemple de politique — Création d'un système de fichiers avec une balise spécifique à partir de sauvegardes dotées d'une balise spécifique

Cette politique permet aux utilisateurs de créer des systèmes de fichiers étiquetés avec `Department=Finance` uniquement à partir de sauvegardes étiquetées avec`Department=Finance`.

JSON

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

```
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Exemple de politique — Supprimer des systèmes de fichiers dotés de balises spécifiques

Cette politique permet à un utilisateur de supprimer uniquement les systèmes de fichiers marqués avec`Department=Finance`. S'ils créent une sauvegarde finale, elle doit être étiquetée avec`Department=Finance`. FSx Pour les systèmes de fichiers Lustre, les utilisateurs doivent avoir le `fsx:CreateBackup` privilège de créer la sauvegarde finale.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
```

```
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Exemple de politique — Création de tâches de référentiel de données sur des systèmes de fichiers avec une balise spécifique

Cette politique permet aux utilisateurs de créer des tâches de référentiel de données étiquetées avec`Department=Finance`, et uniquement sur les systèmes de fichiers étiquetés avec`Department=Finance`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask"
            ],
```

```
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:task/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Utilisation de rôles liés à un service pour Amazon FSx

Amazon FSx utilise des rôles Gestion des identités et des accès AWS liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon. FSx Les rôles liés au service sont prédéfinis par Amazon FSx et incluent toutes les autorisations requises par le service pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration d'Amazon FSx , car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Amazon FSx définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Amazon FSx peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos FSx ressources Amazon, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôles liés à un service. Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées à un service pour Amazon FSx

Amazon FSx utilise deux rôles liés à un service nommés `AWSServiceRoleForAmazonFSx` et `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`* qui exécutent certaines actions sur votre compte. Ces actions incluent par exemple la création d'interfaces réseau élastiques pour vos systèmes de fichiers dans votre VPC et l'accès à votre référentiel de données dans un compartiment Amazon S3. En effet`AWSServiceRoleForFSxS3Access_`*`fs-01234567890`*, ce rôle lié à un service est créé pour chaque système de fichiers Amazon FSx for Lustre que vous créez et qui est lié à un compartiment S3.

AWSServiceRoleForAmazonFSx détails des autorisations

En `AWSServiceRoleForAmazonFSx` effet, la politique d'autorisation des rôles permet FSx à Amazon d'effectuer les actions administratives suivantes au nom de l'utilisateur sur toutes les AWS ressources applicables :

Pour connaître les mises à jour de cette politique, consultez Amazon FSx ServiceRolePolicy.

> **Note**
>
> AWSServiceRoleForAmazonFSx Il est utilisé par tous les types de systèmes de FSx fichiers Amazon ; certaines des autorisations répertoriées ne s'appliquent pas FSx à Lustre.

- `ds`— Permet FSx à Amazon de consulter, d'autoriser et d'annuler les applications de votre Directory Service annuaire.
- `ec2`— Permet FSx à Amazon d'effectuer les opérations suivantes :
  - Affichez, créez et dissociez les interfaces réseau associées à un système de FSx fichiers Amazon.
  - Affichez une ou plusieurs adresses IP élastiques associées à un système de FSx fichiers Amazon.
  - Affichez Amazon VPCs, les groupes de sécurité et les sous-réseaux associés à un système de FSx fichiers Amazon.

  - Attribuez des IPv6 adresses aux interfaces réseau des clients dotées d'une `AmazonFSx.FileSystemId` balise.
  - Annulez l'attribution d' IPv6 adresses aux interfaces réseau des clients dotées d'une `AmazonFSx.FileSystemId` balise.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
  - Créez une autorisation permettant à un utilisateur AWS autorisé d'effectuer certaines opérations sur une interface réseau.
- `cloudwatch`— Permet FSx à Amazon de publier des points de données métriques CloudWatch sous l'espace de FSx noms AWS/.
- `route53`— Permet FSx à Amazon d'associer un Amazon VPC à une zone hébergée privée.
- `logs`— Permet FSx à Amazon de décrire et d'écrire dans les flux de CloudWatch journaux Logs. Cela permet aux utilisateurs d'envoyer les journaux d'audit d'accès aux fichiers FSx pour un système de fichiers Windows File Server vers un flux de CloudWatch journaux.
- `firehose`— Permet FSx à Amazon de décrire et d'écrire dans les flux de diffusion Amazon Data Firehose. Cela permet aux utilisateurs de publier les journaux d'audit d'accès aux fichiers FSx pour un système de fichiers Windows File Server sur un flux de diffusion Amazon Data Firehose.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
```

```
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
```

```
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
```

```
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Toute mise à jour de cette politique est décrite dansAmazon FSx met à jour AWS ses politiques gérées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations du rôle lié à un service dans le Guide de l'utilisateur IAM.

AWSServiceRoleForFSxDétails des autorisations S3 Access

En `AWSServiceRoleForFSxS3Access_`*`file-system-id`* effet, la politique d'autorisation des rôles permet FSx à Amazon d'effectuer les actions suivantes sur un compartiment Amazon S3 hébergeant le référentiel de données d'un système de fichiers Amazon FSx for Lustre.

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutObject`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Amazon FSx

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un système de fichiers dans le AWS Management Console AWS CLI, le ou l' AWS API, Amazon FSx crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter Un nouveau rôle est apparu dans mon compte IAM.

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 un système de fichiers, Amazon FSx crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour Amazon FSx

Amazon FSx ne vous autorise pas à modifier ces rôles liés aux services. Après avoir 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 Modification d’un rôle lié à un service dans le Guide de l’utilisateur IAM.

Supprimer un rôle lié à un service pour Amazon FSx

Si vous n’avez plus besoin d’utiliser une fonctionnalité 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. Toutefois, vous devez supprimer tous vos systèmes de fichiers et toutes vos sauvegardes avant de pouvoir supprimer manuellement le rôle lié à un service.

> **Note**
>
> Si le FSx service Amazon utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer manuellement le rôle lié au service à l’aide d’IAM

Utilisez la console IAM, l'interface de ligne de commande IAM ou l'API IAM pour supprimer le rôle lié à un service AWSServiceRoleForAmazonFSx. Pour en savoir plus, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles FSx liés aux services Amazon

Amazon FSx prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et Points de terminaison AWS.

Contrôle d'accès au système de fichiers avec Amazon VPC

Un système de FSx fichiers Amazon est accessible via une interface réseau élastique qui réside dans le cloud privé virtuel (VPC) basé sur le service Amazon VPC que vous associez à votre système de fichiers. Vous accédez à votre système de FSx fichiers Amazon via son nom DNS, qui correspond à l'interface réseau du système de fichiers. Seules les ressources du VPC associé, ou d'un VPC pair, peuvent accéder à l'interface réseau de votre système de fichiers. Pour de plus amples informations, veuillez consulter Qu'est-ce qu'Amazon VPC ? dans le Guide de l'utilisateur Amazon VPC.

> **Warning**
>
> Vous ne devez ni modifier ni supprimer l'interface Amazon FSx Elastic network. La modification ou la suppression de l'interface réseau peut entraîner une perte permanente de connexion entre votre VPC et votre système de fichiers.

Groupes de sécurité Amazon VPC

Pour mieux contrôler le trafic réseau passant par l'interface réseau de votre système de fichiers au sein de votre VPC, vous utilisez des groupes de sécurité pour limiter l'accès à vos systèmes de fichiers. Un groupe de sécurité agit comme un pare-feu virtuel pour contrôler le trafic des ressources associées. Dans ce cas, la ressource associée est l'interface réseau de votre système de fichiers. Vous utilisez également des groupes de sécurité VPC pour contrôler le trafic réseau de votre Lustre clients.

Groupes de sécurité compatibles avec EFA

Si vous souhaitez créer un groupe de sécurité compatible EFA FSx pour Lustre, vous devez d'abord créer un groupe de sécurité compatible EFA et le spécifier comme groupe de sécurité pour le

système de fichiers. Un EFA nécessite un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance du groupe de sécurité lui-même et du groupe de sécurité des clients si les clients résident dans un autre groupe de sécurité. Pour plus d'informations, consultez Étape 1 : Préparation d'un groupe de sécurité compatible EFA dans le guide de l'utilisateur Amazon EC2 .

Contrôle de l'accès à l'aide de règles entrantes et sortantes

Pour utiliser un groupe de sécurité afin de contrôler l'accès à votre système de FSx fichiers Amazon et Lustre clients, vous ajoutez les règles entrantes pour contrôler le trafic entrant et les règles sortantes pour contrôler le trafic sortant de votre système de fichiers et Lustre clients. Assurez-vous de disposer des bonnes règles de trafic réseau dans votre groupe de sécurité pour mapper le partage de FSx fichiers de votre système de fichiers Amazon à un dossier de votre instance de calcul prise en charge.

Pour plus d'informations sur les règles des groupes de sécurité, consultez la section Règles des groupes de sécurité dans le guide de EC2 l'utilisateur Amazon.

Pour créer un groupe de sécurité pour votre système de FSx fichiers Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
3. Sélectionnez Créer un groupe de sécurité.
4. Attribuez un nom et une description au groupe de sécurité.
5. Pour le VPC, choisissez le VPC associé à votre système de FSx fichiers Amazon pour créer le groupe de sécurité au sein de ce VPC.
6. Choisissez Create (Créer) pour créer le groupe de sécurité.

Ensuite, vous ajoutez des règles entrantes au groupe de sécurité que vous venez de créer pour activer Lustre trafic entre vos serveurs de fichiers FSx for Lustre.

Pour ajouter des règles de trafic entrant à votre groupe de sécurité

1. Sélectionnez le groupe de sécurité que vous venez de créer s'il n'est pas déjà sélectionné. Pour Actions, choisissez Modifier les règles entrantes.
2. Ajoutez les règles de trafic entrant suivantes.

Type	Protocole	Plage de ports	Source	Description
Règle TCP personnalisée	TCP	988	Choisissez Personnalisé et entrez l'ID du groupe de sécurité que vous venez de créer	Autorise Lustre trafic entre FSx les serveurs de fichiers Lustre
Règle TCP personnalisée	TCP	988	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité associés à votre Lustre clients	Autorise Lustre trafic entre les serveurs de fichiers FSx pour Lustre et Lustre clients
Règle TCP personnalisée	TCP	1018-1023	Choisissez Personnalisé et entrez l'ID du groupe de sécurité que vous venez de créer	Autorise Lustre trafic entre FSx les serveurs de fichiers Lustre
Règle TCP personnalisée	TCP	1018-1023	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité associés à votre Lustre clients	Autorise Lustre trafic entre les serveurs de fichiers FSx pour Lustre et Lustre clients

3. Choisissez Enregistrer pour enregistrer et appliquer les nouvelles règles de trafic entrant.

Par défaut, les règles du groupe de sécurité autorisent tout le trafic sortant (Tout, 0.0.0.0/0). Si votre groupe de sécurité n'autorise pas tout le trafic sortant, ajoutez les règles sortantes suivantes à votre groupe de sécurité. Ces règles autorisent le trafic entre FSx les serveurs de fichiers Lustre et Lustre clients, et entre Lustre serveurs de fichiers.

Pour ajouter des règles de trafic sortant à votre groupe de sécurité

1. Choisissez le même groupe de sécurité auquel vous venez d'ajouter les règles entrantes. Pour Actions, choisissez Modifier les règles sortantes.
2. Ajoutez les règles sortantes suivantes.

Type	Protocole	Plage de ports	Source	Description
Règle TCP personnalisée	TCP	988	Choisissez Personnalisé et entrez l'ID du groupe de sécurité que vous venez de créer	Autorisation Lustre trafic entre FSx les serveurs de fichiers Lustre
Règle TCP personnalisée	TCP	988	Choisissez Personnalisé et entrez le groupe IDs de sécurité du groupe de sécurité associé à votre Lustre clients	Autorisation Lustre trafic entre les serveurs de fichiers FSx pour Lustre et Lustre clients
Règle TCP personnalisée	TCP	1018-1023	Choisissez Personnalisé et entrez l'ID du groupe de sécurité que vous venez de créer	Autorise Lustre trafic entre FSx les serveurs de fichiers Lustre

Type	Protocole	Plage de ports	Source	Description
Règle TCP personnalisée	TCP	1018-1023	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité associés à votre Lustre clients	Autorise Lustre trafic entre les serveurs de fichiers FSx pour Lustre et Lustre clients

3. Choisissez Enregistrer pour enregistrer et appliquer les nouvelles règles de trafic sortant.

Pour associer un groupe de sécurité à votre système de FSx fichiers Amazon

1. Ouvrez la FSx console Amazon à l'adresse https://console.aws.amazon.com/fsx/.
2. Sur le tableau de bord de la console, choisissez votre système de fichiers pour en afficher les détails.
3. Dans l'onglet Réseau et sécurité, cliquez sur le lien de la EC2 console Amazon sous Interface (s) réseau (s) pour afficher toutes les interfaces réseau de votre système de fichiers.
4. Pour chaque interface réseau, choisissez Actions, puis Modifier les groupes de sécurité.
5. Dans la boîte de dialogue Modifier les groupes de sécurité, choisissez les groupes de sécurité que vous souhaitez associer à l'interface réseau.
6. Choisissez Save (Enregistrer).

Lustre règles du groupe de sécurité VPC client

Vous utilisez des groupes de sécurité VPC pour contrôler l'accès à votre Lustre clients en ajoutant des règles entrantes pour contrôler le trafic entrant et des règles sortantes pour contrôler le trafic sortant de votre Lustre clients. Assurez-vous de disposer des bonnes règles de trafic réseau dans votre groupe de sécurité afin de garantir que Lustre le trafic peut circuler entre votre Lustre clients et vos systèmes de FSx fichiers Amazon.

Ajoutez les règles de trafic entrant suivantes aux groupes de sécurité appliqués à votre Lustre clients.

Type	Protocole	Plage de ports	Source	Description
Règle TCP personnalisée	TCP	988	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité appliqués à votre Lustre clients	Autorise Lustre trafic entre Lustre clients
Règle TCP personnalisée	TCP	988	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité associés à vos systèmes de fichiers FSx pour Lustre	Autorise Lustre trafic entre les serveurs de fichiers FSx pour Lustre et Lustre clients
Règle TCP personnalisée	TCP	1018-1023	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité appliqués à votre Lustre clients	Autorise Lustre trafic entre Lustre clients
Règle TCP personnalisée	TCP	1018-1023	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité associés à vos systèmes	Autorise Lustre trafic entre les serveurs de fichiers FSx pour Lustre et Lustre clients

Type	Protocole	Plage de ports	Source	Description
			de fichiers FSx pour Lustre	

Ajoutez les règles sortantes suivantes aux groupes de sécurité appliqués à votre Lustre clients.

Type	Protocole	Plage de ports	Source	Description
Règle TCP personnalisée	TCP	988	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité appliqués à votre Lustre clients	Autorise Lustre trafic entre Lustre clients
Règle TCP personnalisée	TCP	988	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité associés à vos systèmes de fichiers FSx pour Lustre	Autorisation Lustre trafic entre les serveurs de fichiers FSx pour Lustre et Lustre clients
Règle TCP personnalisée	TCP	1018-1023	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité appliqués à votre Lustre clients	Autorise Lustre trafic entre Lustre clients

Type	Protocole	Plage de ports	Source	Description
Règle TCP personnalisée	TCP	1018-1023	Choisissez Personnalisé et entrez le groupe IDs de sécurité des groupes de sécurité associés à vos systèmes de fichiers FSx pour Lustre	Autorise Lustre trafic entre les serveurs de fichiers FSx pour Lustre et Lustre clients

Réseau Amazon VPC ACLs

Une autre option pour sécuriser l'accès au système de fichiers au sein de votre VPC consiste à établir des listes de contrôle d'accès réseau (réseau ACLs). Le réseau est distinct ACLs des groupes de sécurité, mais possède des fonctionnalités similaires pour ajouter une couche de sécurité supplémentaire aux ressources de votre VPC. Pour plus d'informations sur la mise en œuvre du contrôle d'accès via le réseau ACLs, consultez la section Contrôler le trafic vers les sous-réseaux à l'aide du réseau ACLs dans le guide de l'utilisateur Amazon VPC.

Validation de conformité pour Amazon FSx for Lustre

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. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

Amazon FSx pour Lustre et points de terminaison VPC d'interface ()AWS PrivateLink

Vous pouvez améliorer le niveau de sécurité de votre VPC en configurant Amazon FSx pour qu'il utilise un point de terminaison VPC d'interface. Les points de terminaison VPC d'interface sont alimentés par AWS PrivateLinkune technologie qui vous permet d'accéder à Amazon en privé FSx APIs sans passerelle Internet, appareil NAT, connexion VPN ou connexion. Direct Connect Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec Amazon. FSx APIs Le trafic entre votre VPC et Amazon FSx ne quitte pas le AWS réseau.

Chaque point de terminaison VPC d'interface est représenté par une ou plusieurs interfaces réseau élastiques dans vos sous-réseaux. Une interface réseau fournit une adresse IP privée qui sert de point d'entrée pour le trafic vers l' FSx API Amazon.

Considérations relatives aux points de terminaison FSx VPC de l'interface Amazon

Avant de configurer un point de terminaison VPC d'interface pour Amazon FSx, assurez-vous de consulter les propriétés et les limites du point de terminaison d'interface VPC dans le guide de l'utilisateur Amazon VPC.

Vous pouvez appeler n'importe quelle opération d' FSx API Amazon depuis votre VPC. Par exemple, vous pouvez créer un système de fichiers FSx pour Lustre en appelant l' CreateFileSystem API depuis votre VPC. Pour obtenir la liste complète d'Amazon FSx APIs, consultez la section Actions du manuel Amazon FSx API Reference.

Considérations relatives au peering VPC

Vous pouvez en connecter d'autres VPCs au VPC à l'aide de points de terminaison VPC d'interface à l'aide de l'appairage VPC. Le peering VPC est une connexion réseau entre deux. VPCs Vous pouvez établir une connexion d'appairage VPC entre les vôtres ou avec un VPC dans un autre. VPCs Compte AWS Ils VPCs peuvent également être en deux versions différentes Régions AWS.

Le trafic entre pairs VPCs reste sur le AWS réseau et ne traverse pas l'Internet public. Une fois peered, VPCs les ressources telles que les instances Amazon Elastic Compute Cloud (Amazon EC2) présentes dans les deux instances VPCs peuvent accéder à l' FSx API Amazon via les points de terminaison VPC de l'interface créés dans l'un des. VPCs

Création d'un point de terminaison VPC d'interface pour Amazon API FSx

Vous pouvez créer un point de terminaison VPC pour l' FSx API Amazon à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez la section Création d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Pour une liste complète des points de FSx terminaison Amazon, consultez la section Points de FSx terminaison et quotas Amazon dans le. Référence générale d'Amazon Web Services

Pour créer un point de terminaison VPC d'interface pour Amazon FSx, utilisez l'une des méthodes suivantes :

- **`com.amazonaws.region.fsx`**— Crée un point de terminaison pour les opérations FSx d'API Amazon.
- **`com.amazonaws.region.fsx-fips`**— Crée un point de terminaison pour l' FSx API Amazon conforme à la norme fédérale de traitement de l'information (FIPS) 140-2.

Pour utiliser l'option DNS privé, vous devez définir les `enableDnsSupport` attributs `enableDnsHostnames` et de votre VPC. Pour plus d'informations, consultez la section Affichage et mise à jour du support DNS pour votre VPC dans le guide de l'utilisateur Amazon VPC.

Sauf Régions AWS en Chine, si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à Amazon FSx avec le point de terminaison VPC en utilisant son nom DNS par défaut pour le Région AWS, par exemple. `fsx.us-east-1.amazonaws.com` Pour la Chine (Pékin) et la Chine (Ningxia) Régions AWS, vous pouvez effectuer des demandes d'API avec le point de terminaison VPC `fsx-api.cn-north-1.amazonaws.com.cn` en utilisant `fsx-api.cn-northwest-1.amazonaws.com.cn` et, respectivement.

Pour plus d'informations, consultez la section Accès à un service via un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour Amazon FSx

Pour mieux contrôler l'accès à l' FSx API Amazon, vous pouvez éventuellement associer une politique Gestion des identités et des accès AWS (IAM) à votre point de terminaison VPC. La stratégie spécifie les éléments suivants :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.

- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d’informations, consultez Contrôle de l’accès aux services avec points de terminaison d’un VPC dans le Guide de l’utilisateur Amazon VPC.

Quotas de service pour Amazon FSx pour Lustre

Vous trouverez ci-dessous des informations sur les quotas lorsque vous travaillez avec Amazon FSx pour Lustre.

Rubriques

- Les quotas que vous pouvez augmenter
- Quotas de ressources pour chaque système de fichiers
- Considérations supplémentaires

Les quotas que vous pouvez augmenter

Vous trouverez ci-dessous les quotas d'Amazon FSx for Lustre par AWS compte et par AWS région, que vous pouvez augmenter.

Ressource	Par défaut	Description
LustreSystèmes de fichiers persistants 1	100	Le nombre maximum de systèmes de fichiers Amazon FSx for Lustre Persistent 1 que vous pouvez créer dans ce compte.
Lustre2 systèmes de fichiers persistants	100	Le nombre maximum de systèmes de fichiers Amazon FSx for Lustre Persistent 2 que vous pouvez créer dans ce compte.
LustreCapacité de stockage persistante sur disque dur (par système de fichiers)	102 000	Capacité maximale de stockage sur disque dur (en GiB) que vous pouvez configurer pour un système de fichiers persistant Amazon FSx for Lustre.

Ressource	Par défaut	Description
LustreCapacité de stockage de 1 fichier persistante	100800	Capacité de stockage maximale (en GiB) que vous pouvez configurer pour tous les systèmes de fichiers Amazon FSx for Lustre Persistent 1 dans ce compte.
LustreCapacité de stockage de 2 fichiers persistante	100800	Capacité de stockage maximale (en GiB) que vous pouvez configurer pour tous les systèmes de fichiers Amazon FSx for Lustre Persistent 2 dans ce compte.
LustreSystèmes de fichiers Scratch	100	Le nombre maximum de systèmes de fichiers scratch Amazon FSx for Lustre que vous pouvez créer dans ce compte.
LustreCapacité de stockage des rayures	100800	Capacité de stockage maximale (en GiB) que vous pouvez configurer pour tous les systèmes de fichiers scratch Amazon FSx for Lustre dans ce compte.
LustreCapacité de débit persistante à hiérarchisation intelligente	100 000	La quantité totale de capacité de débit (in MBps) autorisée pour tous les systèmes de fichiers Amazon FSx for Lustre Intelligent-Tiering de ce compte.

Ressource	Par défaut	Description
LustreCapacité de stockage du cache de lecture SSD à hiérarchisation intelligente persistante	100800	La capacité maximale de stockage du cache de lecture SSD provisionnée (en GiB) que vous pouvez configure r pour tous les systèmes de fichiers FSx Amazon for Lustre Intelligent-Tiering de ce compte.
Lustresauvegardes	500	Le nombre maximum de sauvegardes initiées par l'utilisateur que vous pouvez avoir pour tous les systèmes de fichiers Amazon FSx for Lustre dans ce compte.

Pour demander une augmentation de quota

1. Ouvrez la console Service Quotas.
2. Dans le panneau de navigation, choisissez Services AWS .
3. Sélectionnez Lustre.
4. Choisissez un quota.
5. Choisissez Demander une augmentation de quota, puis suivez les instructions pour demander une augmentation de quota.
6. Pour consulter l'état de la demande de quota, sélectionnez Historique des demandes de quotas dans le volet de navigation de la console.

Pour plus d’informations, consultez Demande d’augmentation de quota dans le Guide de l’utilisateur Service Quotas.

Quotas de ressources pour chaque système de fichiers

Vous trouverez ci-dessous les limites des ressources Amazon FSx for Lustre pour chaque système de fichiers d'une AWS région.

Ressource	Limite par système de fichiers
Nombre maximum de tags	50
Durée de conservation maximale pour les sauvegardes automatisées	90 jours
Nombre maximum de demandes de copie de sauvegarde en cours vers une seule région de destination par compte.	5
Nombre de mises à jour de fichiers depuis un compartiment S3 lié par système de fichiers	10 millions par mois
Capacité de stockage minimale, systèmes de fichiers SSD	1,2 TiB
Capacité de stockage minimale, systèmes de fichiers HDD	6 Tio
Débit minimal par unité de stockage, SSD	50 MBps
Débit maximal par unité de stockage, SSD	1000 MBps
Débit minimal par unité de stockage, disque dur	12 MBps
Débit maximal par unité de stockage, disque dur	40 MBps

Considérations supplémentaires

En outre, notez les éléments suivants :

- Vous pouvez utiliser chaque clé AWS Key Management Service (AWS KMS) sur un maximum de 125 systèmes de fichiers Amazon FSx for Lustre.

- Pour obtenir la liste des AWS régions dans lesquelles vous pouvez créer des systèmes de fichiers, consultez Amazon FSx Endpoints and Quotas dans le Références générales AWS.

Résolution des problèmes liés FSx à Amazon pour Lustre

Cette section couvre différents scénarios et solutions de dépannage pour les systèmes de fichiers Amazon FSx for Lustre.

Si vous rencontrez des problèmes non répertoriés ci-dessous, essayez de poser une question sur le forum Amazon FSx for Lustre.

Rubriques

- La création d'un système de fichiers FSx pour Lustre échoue
- Résolution des problèmes de montage du système de fichiers
- Vous ne pouvez pas accéder à votre système de fichiers
- Impossible de valider l'accès à un compartiment S3 lors de la création d'un DRA
- Le changement de nom des répertoires prend beaucoup de temps
- Résolution des problèmes liés à un compartiment S3 lié mal configuré
- Résolution des problèmes de stockage
- Résolution FSx des problèmes liés au pilote Lustre CSI

La création d'un système de fichiers FSx pour Lustre échoue

L'échec d'une demande de création de système de fichiers peut avoir plusieurs causes, comme décrit dans les rubriques suivantes.

Impossible de créer un système de fichiers compatible EFA en raison d'un groupe de sécurité mal configuré

La création d'un système de fichiers compatible FSx pour Lustre EFA échoue avec le message d'erreur suivant :

```
Insufficient security group permissions to create an EFA-enabled file system.
Update security group to allow all internal inbound and outbound traffic.
```

Action à exécuter

Assurez-vous que le groupe de sécurité VPC que vous utilisez pour l'opération de création est configuré comme décrit dans. Groupes de sécurité compatibles avec EFA Un EFA nécessite un

groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance du groupe de sécurité lui-même et du groupe de sécurité des clients si les clients résident dans un autre groupe de sécurité.

Impossible de créer un système de fichiers en raison d'un groupe de sécurité mal configuré

La création d'un système de fichiers FSx pour Lustre échoue avec le message d'erreur suivant :

```
The file system cannot be created because the default security group in the subnet
 provided
or the provided security groups do not permit Lustre LNET network traffic on port 988
```

Action à exécuter

Assurez-vous que le groupe de sécurité VPC que vous utilisez pour l'opération de création est configuré comme décrit dans. Contrôle d'accès au système de fichiers avec Amazon VPC Vous devez configurer le groupe de sécurité pour autoriser le trafic entrant sur les ports 988 et 1018-1023 à partir du groupe de sécurité lui-même ou du CIDR du sous-réseau complet, qui est nécessaire pour permettre aux hôtes du système de fichiers de communiquer entre eux.

Impossible de créer un système de fichiers en raison d'erreurs liées à une capacité insuffisante

Vous pouvez recevoir une erreur de capacité insuffisante lorsque vous tentez de créer un nouveau système de fichiers, de mettre à jour la capacité de stockage ou de modifier la capacité de débit.

Cause

Cette erreur se produit lorsque FSx for Lustre ne dispose pas actuellement d'une capacité matérielle suffisante dans la zone de disponibilité demandée pour répondre à votre demande.

Solution

Pour résoudre ce problème, essayez ce qui suit :

- Patientez quelques minutes et réessayez votre demande, car la disponibilité des capacités change fréquemment.
- Essayez votre demande dans une autre zone de disponibilité.

- Essayez l'opération avec une taille de stockage inférieure ou un niveau de débit inférieur

Impossible de créer un système de fichiers lié à un compartiment S3

Si la création d'un nouveau système de fichiers lié à un compartiment S3 échoue, un message d'erreur similaire au suivant s'affiche.

```
User: arn:aws:iam::012345678901:user/username is not authorized to perform:
 iam:PutRolePolicy on resource: resource ARN
```

Cette erreur peut se produire si vous essayez de créer un système de fichiers lié à un compartiment Amazon S3 sans les autorisations IAM nécessaires. Les autorisations IAM requises prennent en charge le rôle lié au service Amazon FSx for Lustre qui est utilisé pour accéder au compartiment Amazon S3 spécifié en votre nom.

Action à exécuter

Assurez-vous que votre entité IAM (utilisateur, groupe ou rôle) dispose des autorisations appropriées pour créer des systèmes de fichiers. Cela inclut l'ajout de la politique d'autorisation qui prend en charge le rôle lié au service Amazon FSx for Lustre. Pour de plus amples informations, veuillez consulter Ajouter des autorisations pour utiliser les référentiels de données dans Amazon S3.

Pour plus d'informations sur les rôles liés à un service, consultez Utilisation de rôles liés à un service pour Amazon FSx.

Résolution des problèmes de montage du système de fichiers

L'échec d'une commande de montage d'un système de fichiers peut avoir plusieurs causes, comme décrit dans les rubriques suivantes.

Le montage du système de fichiers échoue immédiatement

La commande de montage du système de fichiers échoue immédiatement. Le code suivant en présente un exemple.

```
mount.lustre: mount fs-0123456789abcdef0.fsx.us-east-1.aws@tcp:/fsx at /lustre
failed: No such file or directory
```

```
Is the MGS specification correct?
Is the filesystem name correct?
```

Cette erreur peut se produire si vous n'utilisez pas la bonne `mountname` valeur lors du montage d'un système de fichiers persistant ou Scratch 2 à l'aide de la mount commande. Vous pouvez obtenir la `mountname` valeur à partir de la réponse de la describe-file-systems AWS CLI commande ou de l'opération DescribeFileSystemsd'API.

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 lustre file_system_dns_name@tcp:/mountname /mnt/fsx

[2+ minute wait here]
Connection timed out
```

Cette erreur peut se produire parce que les groupes de sécurité de l'instance Amazon EC2 ou du système de fichiers ne sont pas correctement configurés.

Action à exécuter

Assurez-vous que vos groupes de sécurité pour le système de fichiers respectent les règles entrantes spécifiées dansGroupes de sécurité Amazon VPC.

Le montage automatique échoue et l’instance ne répond pas

Dans certains cas, le montage automatique d'un système de fichiers peut échouer et votre instance Amazon EC2 peut cesser de répondre.

Ce problème peut se produire si l'`_netdev`option n'a pas été déclarée. Si elle `_netdev` est manquante, votre instance Amazon 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 Support.

Le montage du système de fichiers échoue lors du démarrage du système

Le montage du système de fichiers échoue lors du démarrage du système. Le montage est automatisé à l'aide de`/etc/fstab`. Lorsque le système de fichiers n'est pas monté, l'erreur suivante apparaît dans le journal système correspondant à la période de démarrage de l'instance.

```
LNetError: 3135:0:(lib-socket.c:583:lnet_sock_listen()) Can't create socket: port 988
 already in use
LNetError: 122-1: Can't start acceptor on port 988: port already in use
```

Cette erreur peut se produire lorsque le port 988 n'est pas disponible. Lorsque l'instance est configurée pour monter des systèmes de fichiers NFS, il est possible que les montages NFS lient son port client au port 988

Action à exécuter

Vous pouvez contourner ce problème en ajustant les options du client NFS `noresvport` et de `noauto` montage dans la mesure du possible.

Le montage du système de fichiers à l'aide du nom DNS échoue

Des noms de service de noms de domaine (DNS) mal configurés peuvent provoquer des échecs de montage du système de fichiers, comme le montrent les scénarios suivants.

Scénario 1 : le montage d'un système de fichiers utilisant un nom de service de noms de domaine (DNS) échoue. Le code suivant en présente un exemple.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: Can't parse NID
'file_system_dns_name@tcp:/mountname'
```

Action à exécuter

Vérifiez la configuration de votre cloud privé virtuel (VPC). Si vous utilisez un VPC personnalisé, assurez-vous que les paramètres DNS sont activés. Pour plus d'informations, consultez Utilisation de DNS avec votre VPC dans le Amazon VPC Guide de l'utilisateur.

Pour spécifier un nom DNS dans la `mount` commande, procédez comme suit :

- Assurez-vous que l'instance Amazon EC2 se trouve dans le même VPC que votre système de fichiers Amazon FSx for Lustre.
- Connectez votre instance Amazon EC2 au sein d'un VPC configuré pour utiliser le serveur DNS fourni par Amazon. Pour en savoir plus, consultez Jeux d'options DHCP dans le Guide de l'utilisateur Amazon VPC.
- Assurez-vous que les noms d'hôte DNS sont activés sur le VPC Amazon de l'instance Amazon EC2 connectée. Pour plus d'informations, consultez la section Mise à jour du support DNS pour votre VPC dans le guide de l'utilisateur Amazon VPC.

Scénario 2 : le montage d'un système de fichiers utilisant un nom de service de noms de domaine (DNS) échoue. Le code suivant en présente un exemple.

```
mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: mount file_system_dns_name@tcp:/mountname at /mnt/fsx failed: Input/
output error Is the MGS running?
```

Action à exécuter

Assurez-vous que les règles de trafic sortant correctes sont appliquées aux groupes de sécurité VPC du client. Cette recommandation est particulièrement vraie si vous n'utilisez pas le groupe de sécurité par défaut ou si vous l'avez modifié. Pour de plus amples informations, veuillez consulter Groupes de sécurité Amazon VPC.

Vous ne pouvez pas accéder à votre système de fichiers

L'impossibilité d'accéder à votre système de fichiers peut avoir plusieurs causes, chacune ayant sa propre résolution, comme suit.

L'adresse IP élastique attachée à l'interface Elastic Network du système de fichiers a été supprimée

Amazon FSx ne prend pas en charge l'accès aux systèmes de fichiers depuis l'Internet public. Amazon détache FSx automatiquement toute adresse IP élastique, qui est une adresse IP publique accessible depuis Internet, attachée à l'interface Elastic Network d'un système de fichiers.

L'interface Elastic Network du système de fichiers a été modifiée ou supprimée

Vous ne devez ni modifier ni supprimer l'interface Elastic Network du système de fichiers. La modification ou la suppression de l'interface réseau peut entraîner une perte permanente de connexion entre votre VPC et votre système de fichiers. Créez un nouveau système de fichiers et ne modifiez ni ne supprimez l'interface FSx Elastic Network. Pour de plus amples informations, veuillez consulter Contrôle d'accès au système de fichiers avec Amazon VPC.

Impossible de valider l'accès à un compartiment S3 lors de la création d'un DRA

La création d'une association de référentiel de données (DRA) à partir de la FSx console Amazon ou à l'aide de la commande `create-data-repository-association` CLI (CreateDataRepositoryAssociationc'est l'action d'API équivalente) échoue avec le message d'erreur suivant.

```
Amazon FSx is unable to validate access to the S3 bucket. Ensure the IAM role or user
you are using has s3:Get*, s3:List* and s3:PutObject permissions to the S3 bucket
 prefix.
```

> **Note**
>
> Vous pouvez également obtenir l'erreur ci-dessus lors de la création d'un système de fichiers Scratch 1, Scratch 2 ou Persistent 1 lié à un référentiel de données (compartiment ou préfixe S3) à l'aide de la FSx console Amazon ou de la commande `create-file-system` CLI (CreateFileSystemaction d'API équivalente).

Action à exécuter

Si le système de fichiers FSx for Lustre se trouve dans le même compte que le compartiment S3, cette erreur signifie que le rôle IAM que vous avez utilisé pour la demande de création ne dispose pas des autorisations nécessaires pour accéder au compartiment S3. Assurez-vous que le rôle IAM dispose des autorisations répertoriées dans le message d'erreur. Ces autorisations prennent en charge le rôle lié au service Amazon FSx for Lustre qui est utilisé pour accéder au compartiment Amazon S3 spécifié en votre nom.

Si le système de fichiers FSx for Lustre se trouve dans un compte différent de celui du compartiment S3 (cas multi-comptes), en plus de vérifier que le rôle IAM que vous avez utilisé dispose des autorisations requises, la politique du compartiment S3 doit être configurée pour autoriser l'accès depuis le compte dans lequel le package FSx for Lustre a été créé.

Pour plus d'informations sur les autorisations de compartiment entre comptes S3, consultez l'exemple 2 : le propriétaire du compartiment accorde des autorisations de compartiment entre comptes dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Le changement de nom des répertoires prend beaucoup de temps

Question

J'ai renommé un répertoire sur un système de fichiers lié à un compartiment Amazon S3 et j'ai activé l'exportation automatique. Pourquoi les fichiers de ce répertoire mettent-ils longtemps à être renommés dans le compartiment S3 ?

Réponse

Lorsque vous renommez un répertoire dans le système de fichiers, FSx for Lustre crée de nouveaux objets S3 pour tous les fichiers et répertoires du répertoire renommé. Le temps nécessaire pour propager le renommage du répertoire en S3 est directement corrélé à la quantité de fichiers et de répertoires qui sont les descendants du répertoire renommé.

Résolution des problèmes liés à un compartiment S3 lié mal configuré

Dans certains cas, le compartiment S3 lié d'un système de fichiers FSx for Lustre peut présenter un état du cycle de vie du référentiel de données mal configuré.

Cause possible

Cette erreur peut se produire si Amazon FSx ne dispose pas des autorisations Gestion des identités et des accès AWS (IAM) nécessaires pour accéder au référentiel de données lié. Les autorisations IAM requises prennent en charge le rôle lié au service Amazon FSx for Lustre qui est utilisé pour accéder au compartiment Amazon S3 spécifié en votre nom.

Action à exécuter

1. Assurez-vous que votre entité IAM (utilisateur, groupe ou rôle) dispose des autorisations appropriées pour créer des systèmes de fichiers. Cela inclut l'ajout de la politique d'autorisation qui prend en charge le rôle lié au service Amazon FSx for Lustre. Pour de plus amples informations, veuillez consulter Ajouter des autorisations pour utiliser les référentiels de données dans Amazon S3.
2. À l'aide de l' FSx interface de ligne de commande ou de l'API Amazon, actualisez le système de `AutoImportPolicy` fichiers à l'aide de la commande `update-file-system` CLI (UpdateFileSystemaction d'API équivalente), comme suit.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Pour plus d'informations sur les rôles liés à un service, consultez Utilisation de rôles liés à un service pour Amazon FSx.

Cause possible

Cette erreur peut se produire si le référentiel de données Amazon S3 lié possède une configuration de notification d'événements existante dont les types d'événements se chevauchent avec la configuration de notification d' FSx événements Amazon (`s3:ObjectCreated:*`,`s3:ObjectRemoved:*`).

Cela peut également se produire si la configuration des notifications d' FSx événements Amazon sur le compartiment S3 lié a été supprimée ou modifiée.

Action à exécuter

1. Supprimez toute notification d'événement existante sur le compartiment S3 lié qui utilise l'un ou l'autre des types d'événements utilisés par la configuration des FSx événements, `s3:ObjectCreated:*` et`s3:ObjectRemoved:*`.
2. Assurez-vous qu'il existe une configuration de notification d'événement S3 dans votre compartiment S3 lié avec le nom`FSx`, les types d'`s3:ObjectCreated:*`événements et envoyez-la à la rubrique SNS avec`ARN:`*`topic_arn_returned_in_API_response`*. `s3:ObjectRemoved:*`
3. Réappliquez la configuration des notifications d' FSx événements sur le compartiment S3 à l'aide de la FSx CLI ou de l'API Amazon, afin d'actualiser celle du système de `AutoImportPolicy`

fichiers. Pour ce faire, utilisez la commande `update-file-system` CLI (UpdateFileSystemc'est l'action d'API équivalente), comme suit.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Résolution des problèmes de stockage

Dans certains cas, il se peut que vous rencontriez des problèmes de stockage avec votre système de fichiers. Vous pouvez résoudre ces problèmes à l'aide de `lfs` commandes telles que la `lfs migrate` commande.

Erreur d'écriture due à l'absence d'espace sur la cible de stockage

Vous pouvez vérifier l'utilisation du stockage de votre système de fichiers à l'aide de la `lfs df -h` commande, comme décrit dansDisposition du stockage du système de fichiers. Le `filesystem_summary` champ indique l'utilisation totale du stockage du système de fichiers.

Si l'utilisation du disque du système de fichiers est de 100 %, envisagez d'augmenter la capacité de stockage de votre système de fichiers. Pour de plus amples informations, veuillez consulter Gestion de la capacité de stockage.

Si l'utilisation du stockage du système de fichiers n'est pas de 100 % et que des erreurs d'écriture persistent, le fichier dans lequel vous écrivez est peut-être réparti par bandes sur un OST plein.

Action à exécuter

- Si plusieurs d'entre eux OSTs sont pleins, augmentez la capacité de stockage de votre système de fichiers. Vérifiez que le stockage n'est pas déséquilibré OSTs en suivant les instructions de la Stockage déséquilibré sur OSTs section.
- Si vous n' OSTs êtes pas plein, ajustez la taille de la mémoire tampon des pages sales du client en appliquant le réglage suivant à toutes vos instances clientes :

```
sudo lctl set_param osc.*.max_dirty_mb=64
```

Stockage déséquilibré sur OSTs

Amazon FSx for Lustre distribue les nouvelles bandes de fichiers de manière uniforme OSTs. Cependant, il se peut que votre système de fichiers soit toujours déséquilibré en raison de I/O modèles ou de la structure de stockage des fichiers. Par conséquent, certaines cibles de stockage peuvent devenir pleines tandis que d'autres restent relativement vides.

Vous utilisez cette `lfs migrate` commande pour déplacer des fichiers ou des répertoires du plus plein vers le moins plein. OSTs Vous pouvez utiliser la `lfs migrate` commande en mode bloc ou non.

- Le mode bloc est le mode par défaut de la `lfs migrate` commande. Lorsqu'il est exécuté en mode bloc, il acquiert d'`lfs migrate`abord un verrouillage de groupe sur les fichiers et les répertoires avant la migration des données afin d'empêcher toute modification des fichiers, puis relâche le verrou une fois la migration terminée. En empêchant les autres processus de modifier les fichiers, le mode bloc empêche ces processus d'interrompre la migration. L'inconvénient est que le fait d'empêcher une application de modifier un fichier peut entraîner des retards ou des erreurs dans l'application.
- Le mode sans blocage est activé pour la `lfs migrate` commande avec l'`-n`option. Lorsqu'ils sont exécutés `lfs migrate` en mode non bloc, les autres processus peuvent toujours modifier les fichiers en cours de migration. Si un processus modifie un fichier avant d'avoir `lfs migrate` terminé sa migration, il ne `lfs migrate` parviendra pas à migrer ce fichier, laissant le fichier dans sa mise en page par bandes d'origine.

Nous vous recommandons d'utiliser le mode sans blocage, car il est moins susceptible d'interférer avec votre application.

Action à exécuter

1. Lancez une instance client relativement volumineuse (telle que le type d'`c5n.4xlarge`instance Amazon EC2) à monter sur le système de fichiers.
2. Avant d'exécuter le script en mode non bloc ou le script en mode bloc, exécutez d'abord les commandes suivantes sur chaque instance client pour accélérer le processus :

```
sudo lctl set_param 'mdc.*.max_rpcs_in_flight=60'
sudo lctl set_param 'mdc.*.max_mod_rpcs_in_flight=59'
```

3. Démarrez une session d'écran et exécutez le script en mode non bloc ou le script en mode bloc. Assurez-vous de modifier les variables appropriées dans les scripts :

   - Script en mode non bloc :

```
#!/bin/bash

# UNCOMMENT THE FOLLOWING LINES:
#
# TRY_COUNT=0
# MAX_MIGRATE_ATTEMPTS=100
# OSTS="fsname-OST0000_UUID"
# DIR_OR_FILE_MIGRATED="/mnt/subdir/"
# BATCH_SIZE=10
# PARALLEL_JOBS=16 # up to max-procs processes, set to 16 if client is
 c5n.4xlarge with 16 vcpu
# LUSTRE_STRIPING_CONFIG="-E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32" #
 should be consistent with the existing striping setup
#

if [ -z "$TRY_COUNT" -o -z "$MAX_MIGRATE_ATTEMPTS" -o -z "$OSTS" -o -z
 "$DIR_OR_FILE_MIGRATED" -o -z "$BATCH_SIZE" -o -z "$PARALLEL_JOBS" -o -z
 "$LUSTRE_STRIPING_CONFIG" ]; then
    echo "Some variables are not set."
    exit 1
fi

echo "lfs migrate starts"
while true; do
    output=$(sudo lfs find ! -L released --ost $OSTS --print0
 $DIR_OR_FILE_MIGRATED | shuf -z | /bin/xargs -0 -P $PARALLEL_JOBS -n $BATCH_SIZE
 sudo lfs migrate -n $LUSTRE_STRIPING_CONFIG 2>&1)
    if [[ $? -eq 0 ]]; then
        echo "lfs migrate succeeds for $DIR_OR_FILE_MIGRATED at the $TRY_COUNT
 attempt, exiting."
        exit 0
    elif [[ $? -eq 123 ]]; then
        echo "WARN: Target data objects are not located on these OSTs. Skipping
 lfs migrate"
        exit 1
    else
        echo "lfs migrate fails for $DIR_OR_FILE_MIGRATED at the $TRY_COUNT
 attempt, retrying..."
```

```
        if (( ++TRY_COUNT >= MAX_MIGRATE_ATTEMPTS )); then
            echo "WARN: Exceeds max retry attempt. Skipping lfs migrate for
 $DIR_OR_FILE_MIGRATED. Failed with the following error"
            echo $output
            exit 1
        fi
    fi
done
```

- Script en mode bloc :
  - Remplacez les valeurs 0STS par les valeurs de votre OSTs.
  - Entrez une valeur entière de `nproc` pour définir le nombre de processus max-procs à exécuter en parallèle. Par exemple, le type d'`c5n.4xlarge`instance Amazon EC2 est de 16 VCPUs, vous pouvez donc utiliser 16 (ou une valeur inférieure à 16) pour. `nproc`
  - Indiquez le chemin de votre répertoire de montage dans`mnt_dir_path`.

```
# find all OSTs with usage above a certain threshold; for example, greater than
 or equal to 85% full
for OST in $(lfs df -h |egrep '( 8[5-9]| 9[0-9]|100)%'|cut -d' ' -f1); do echo
 ${OST};done|tr '\012' ','

# customer can also just pass OST values directly to OSTS variable
OSTS='dzfevbmv-OST0000_UUID,dzfevbmv-OST0002_UUID,dzfevbmv-OST0004_UUID,dzfevbmv-
OST0005_UUID,dzfevbmv-OST0006_UUID,dzfevbmv-OST0008_UUID'

nproc=<Run up to max-procs processes if client is c5n.4xlarge with 16 vcpu, this
 value can be set to 16>

mnt_dir_path=<mount dir, e.g. '/my_mnt'>

lfs find ${mnt_dir_path} --ost ${OSTS}| xargs -P ${nproc} -n2 lfs migrate -E 100M
 -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32
```

Remarques

- Si vous remarquez un impact sur les performances des lectures du système de fichiers, vous pouvez arrêter les migrations à tout moment en utilisant `ctrl-c` ou `kill -9`, et réduire le nombre de threads (`nproc`valeur) à un nombre inférieur (8, par exemple), puis reprendre la migration des fichiers.

- La `lfs migrate` commande échouera sur un fichier également ouvert par la charge de travail du client. Il génère une erreur et passe au fichier suivant ; il est donc possible que si de nombreux fichiers sont accessibles, le script ne soit pas en mesure de migrer de fichiers, ce qui se reflétera dans le fait que la migration progresse très lentement.
- Vous pouvez surveiller l'utilisation de l'OST à l'aide de l'une des méthodes suivantes :
  - Lors du montage du client, exécutez la commande suivante pour surveiller l'utilisation de l'OST et trouver l'OST dont l'utilisation est supérieure à 85 % :

    ```
    lfs df -h |egrep '( 8[5-9]| 9[1-9]|100)%'
    ```

  - Vérifiez la CloudWatch métrique Amazon`OST FreeDataStorageCapacity`, vérifiez`Minimum`. Si votre script détecte OSTs qu'ils sont pleins à plus de 85 %, utilisez `ctrl-c` ou `kill -9` pour arrêter la migration lorsque la métrique est proche de 15 %.
- Vous pouvez également envisager de modifier la configuration par bandes de votre système de fichiers ou d'un répertoire, afin que les nouveaux fichiers soient répartis sur plusieurs cibles de stockage. Pour plus d'informations, voir dansRegrouper les données dans votre système de fichiers.

Résolution FSx des problèmes liés au pilote Lustre CSI

Amazon FSx for Lustre prend en charge l'accès à partir de conteneurs exécutés sur Amazon EKS à l'aide du pilote open source FSx pour Lustre CSI. Pour obtenir des informations sur le déploiement, consultez la section Utiliser Amazon FSx pour le stockage Lustre dans le guide de l'utilisateur Amazon EKS.

Si vous rencontrez des problèmes avec le pilote CSI FSx pour Lustre pour les conteneurs exécutés sur Amazon EKS, consultez la section Résolution des problèmes liés au pilote CSI (problèmes courants), disponible sur. GitHub

Informations supplémentaires

Cette section fournit une référence des fonctionnalités Amazon FSx prises en charge mais déconseillées.

Rubriques

- Configuration d'un calendrier de sauvegarde personnalisé

Configuration d'un calendrier de sauvegarde personnalisé

Nous vous recommandons AWS Backup de l'utiliser pour configurer un calendrier de sauvegarde personnalisé pour votre système de fichiers. Les informations fournies ici sont fournies à titre de référence si vous devez planifier des sauvegardes plus fréquemment que lorsque vous les utilisez AWS Backup.

Lorsque cette option est activée, Amazon effectue FSx automatiquement une sauvegarde de votre système de fichiers une fois par jour pendant une fenêtre de sauvegarde quotidienne. Amazon FSx applique une période de rétention que vous spécifiez pour ces sauvegardes automatiques. Il prend également en charge les sauvegardes initiées par l'utilisateur, ce qui vous permet d'effectuer des sauvegardes à tout moment.

Vous trouverez ci-dessous les ressources et la configuration nécessaires pour déployer une planification de sauvegarde personnalisée. La planification des sauvegardes personnalisées effectue des sauvegardes initiées par l'utilisateur sur un système de fichiers Amazon FSx for Lustre selon un calendrier personnalisé que vous définissez. Par exemple, une fois toutes les six heures, une fois par semaine, etc. Ce script configure également la suppression des sauvegardes antérieures à la période de rétention spécifiée.

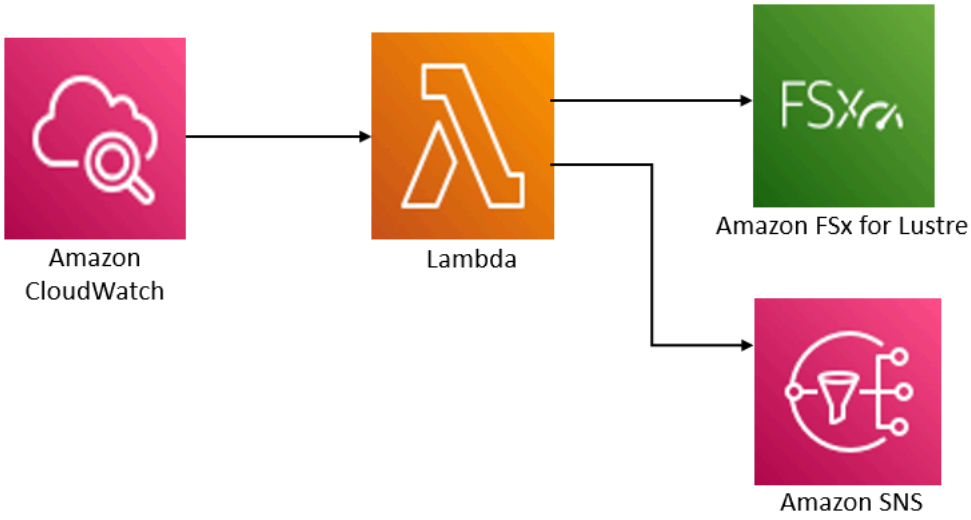
La solution déploie automatiquement tous les composants nécessaires et prend en compte les paramètres suivants :

- Le système de fichiers
- Un modèle de planification CRON pour effectuer des sauvegardes
- Période de conservation des sauvegardes (en jours)
- Les balises de nom de sauvegarde

Pour plus d'informations sur les modèles de planification CRON, consultez la section Expressions de planification pour les règles dans le guide de CloudWatch l'utilisateur Amazon.

Présentation de l’architecture

Le déploiement de cette solution génère les ressources suivantes dans le AWS Cloud.



Cette solution effectue les opérations suivantes :

1. Le CloudFormation modèle déploie un CloudWatch événement, une fonction Lambda, une file d'attente Amazon SNS et un rôle IAM. Le rôle IAM autorise la fonction Lambda à appeler les opérations de l'API FSx Amazon for Lustre.
2. L' CloudWatch événement s'exécute selon un calendrier que vous définissez sous la forme d'un modèle CRON, lors du déploiement initial. Cet événement appelle la fonction Lambda du gestionnaire de sauvegarde de la solution qui appelle l'opération d'API FSx Amazon `CreateBackup` for Lustre pour lancer une sauvegarde.
3. Le gestionnaire de sauvegarde extrait une liste des sauvegardes existantes initiées par l'utilisateur pour le système de fichiers spécifié à l'aide de. `DescribeBackups` Il supprime ensuite les sauvegardes antérieures à la période de rétention, que vous avez spécifiée lors du déploiement initial.
4. Le gestionnaire de sauvegarde envoie un message de notification à la file d'attente Amazon SNS en cas de sauvegarde réussie si vous choisissez l'option d'être averti lors du déploiement initial. Une notification est toujours envoyée en cas de panne.

CloudFormation modèle

Cette solution permet CloudFormation d'automatiser le déploiement de la solution de planification de sauvegarde personnalisée Amazon FSx for Lustre. Pour utiliser cette solution, téléchargez le fsx-scheduled-backupmodèle CloudFormation .template.

Déploiement automatique

La procédure suivante permet de configurer et de déployer cette solution de planification de sauvegarde personnalisée. Le déploiement prend environ cinq minutes. Avant de commencer, vous devez disposer de l'identifiant d'un système de fichiers Amazon FSx for Lustre exécuté dans un Amazon Virtual Private Cloud (Amazon VPC) sur votre AWS compte. Pour plus d'informations sur la création de ces ressources, consultezCommencer à utiliser Amazon FSx pour Lustre.

> **Note**
>
> La mise en œuvre de cette solution entraîne la facturation des AWS services associés. Pour plus d'informations, consultez les pages de détail des tarifs de ces services.

Pour lancer la pile de solutions de sauvegarde personnalisée

1. Téléchargez le fsx-scheduled-backupmodèle CloudFormation .template. Pour plus d'informations sur la création d'une CloudFormation pile, consultez la section Création d'une pile sur la AWS CloudFormation console dans le guide de AWS CloudFormation l'utilisateur.

   > **Note**
   >
   > Par défaut, ce modèle est lancé dans la AWS région USA Est (Virginie du Nord). Amazon FSx for Lustre n'est actuellement disponible que dans des versions spécifiques Régions AWS. Vous devez lancer cette solution dans une AWS région où Amazon FSx for Lustre est disponible. Pour plus d'informations, consultez le Amazon FSx section Régions AWS et points de terminaison dans le Références générales AWS.

2. Pour les paramètres, passez en revue les paramètres du modèle et modifiez-les en fonction des besoins de votre système de fichiers. Cette solution utilise les valeurs par défaut suivantes.

Paramètre	Par défaut	Description
ID du système de fichiers Amazon FSx for Lustre	Aucune valeur par défaut	ID du système de fichiers que vous souhaitez sauvegarder.
Modèle de planification CRON pour les sauvegard es.	0 0/4 * * ? *	Planification de l'exécution de l' CloudWatch événement , du déclenchement d'une nouvelle sauvegarde et de la suppression des anciennes sauvegardes en dehors de la période de conservation.
Conservation des sauvegard es (jours)	7	Nombre de jours pendant lesquels les sauvegardes initiées par l'utilisateur sont conservées. La fonction Lambda supprime les sauvegardes initiées par l'utilisateur datant de plus de ce nombre de jours.
Nom des sauvegardes	sauvegarde planifiée par l'utilisateur	Le nom de ces sauvegardes, qui apparaît dans la colonne Backup Name de la console de gestion Amazon FSx for Lustre.
Notifications de sauvegarde	Oui	Choisissez si vous souhaitez être averti lorsque les sauvegardes sont lancées avec succès. Une notification est toujours envoyée en cas d'erreur.

Paramètre	Par défaut	Description
Adresse e-mail	Aucune valeur par défaut	Adresse e-mail pour s'abonner aux notifications SNS.

3. Choisissez Suivant.
4. Pour Options, choisissez Next.
5. Pour la révision, vérifiez et confirmez les paramètres. Vous devez cocher la case reconnaissant que le modèle crée des ressources IAM.
6. Choisissez Créer pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la CloudFormation console dans la colonne État. Vous devriez voir le statut CREATE_COMPLETE dans environ cinq minutes.

Options supplémentaires

Vous pouvez utiliser la fonction Lambda créée par cette solution pour effectuer des sauvegardes planifiées personnalisées de plusieurs systèmes de fichiers Amazon FSx for Lustre. L'ID du système de fichiers est transmis à la fonction Amazon FSx for Lustre dans le JSON d'entrée pour l' CloudWatch événement. Le JSON par défaut transmis à la fonction Lambda est le suivant, où les valeurs pour `FileSystemId` et `SuccessNotification` sont transmises à partir des paramètres spécifiés lors du lancement de la CloudFormation pile.

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

Pour planifier des sauvegardes pour un système de fichiers Amazon FSx for Lustre supplémentaire, créez une autre règle CloudWatch d'événement. Pour ce faire, utilisez la source d'événements Schedule, avec la fonction Lambda créée par cette solution comme cible. Choisissez Constant (texte JSON) sous Configurer l'entrée. À l'entrée JSON, remplacez simplement l'ID du système de fichiers Amazon FSx par l'ID du système de fichiers Lustre à sauvegarder à la place de`${FileSystemId}`. Vous pouvez également remplacer l'`Yes`un ou `No` l'autre `${SuccessNotification}` dans le JSON ci-dessus.

Les règles d' CloudWatch événements supplémentaires que vous créez manuellement ne font pas partie de la CloudFormation pile de solutions de sauvegarde planifiée personnalisées Amazon FSx for Lustre. Ils ne sont donc pas supprimés si vous supprimez la pile.

Historique du document

- Version de l'API : 01/03/2018
- Dernière mise à jour de la documentation : 30 septembre 2025

Le tableau suivant décrit les modifications importantes apportées au guide de l'utilisateur d'Amazon FSx for Lustre. Pour recevoir des notifications en cas de mise à jour de cette documentation, abonnez-vous au flux RSS.

Modification	Description	Date
Région AWS Support supplémentaire ajouté pour le type de déploiement Persistent 2	Les SSD Persistent 2 FSx pour les systèmes de fichiers Lustre sont désormais disponibles dans la zone locale de l'ouest des États-Unis (Phoenix). Pour plus d'informations, consultez la section Disponibilité des types de déploiement.	30 septembre 2025
Lustresupport client ajouté pour Ubuntu 24 Kernel 6.14.0	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant le noyau Ubuntu 24.04 6.14.0. Pour plus d'informations, consultez la section Installation du Lustre client.	24 septembre 2025
Lustresupport client ajouté pour Amazon Linux 2023 Kernel 6.12	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant le noyau 6.12 d'Amazon Linux 2023. Pour plus d'informations, consultez	9 septembre 2025

	la section Installation du Lustre client.	
Région AWS Support supplémentaire ajouté	FSx pour les systèmes de fichiers Lustre sont désormais disponibles en Asie-Pacifique (Taipei). Pour plus d'informations, consultez la section Disponibilité des types de déploiement.	18 août 2025
Amazon a FSx mis à jour la politique FSx ServiceRolePolicy AWS gérée par Amazon	Amazon FSx a ajouté les `ec2:UnassignIpv6Addresses` autorisations `ec2:AssignIpv6Addresses` et à Amazon FSxServiceRolePolicy. Pour plus d'informations, consultez les FSx mises à jour des politiques AWS gérées par Amazon.	22 juillet 2025
Lustresupport client pour Rocky Linux et Red Hat Enterprise Linux (RHEL) 9.6 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Rocky Linux et Red Hat Enterprise Linux (RHEL) 9.6. Pour plus d'informations, consultez la section Installation du Lustre client.	1er juillet 2025

Amazon a FSx mis à jour la politique FSx FullAccess AWS gérée par Amazon	La politique FSx FullAccess gérée par Amazon a été mise à jour pour ajouter les `fsx:DetachAndDeleteS3AccessPoint` autorisations `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , et.	25 juin 2025
Amazon a FSx mis à jour la politique FSx ConsoleFullAccess AWS gérée par Amazon	La politique FSx ConsoleFullAccess gérée par Amazon a été mise à jour pour ajouter les `fsx:DetachAndDeleteS3AccessPoint` autorisations `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , et.	25 juin 2025
Support ajouté pour la classe de stockage Intelligent-Tiering	Vous pouvez désormais créer FSx pour les systèmes de fichiers Lustre avec la classe de stockage Intelligent-Tiering. La hiérarchisation intelligente fournit un stockage entièrement élastique avec un cache SSD en option pour un accès à faible latence aux données fréquemment consultées. Pour plus d'informations, consultez la section Caractéristiques de performance de la classe de stockage Intelligent-Tiering.	29 mai 2025

Région AWS Support supplémentaire ajouté	FSx pour les systèmes de fichiers Lustre sont désormais disponibles en Asie-Pacifique (Thaïlande) et au Mexique (centre). Pour plus d'informations, consultez la section Disponibilité des types de déploiement.	8 mai 2025
Lustresupport client pour Ubuntu 24 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Ubuntu 24.04. Pour plus d'informations, consultez la section Installation du Lustre client.	19 mars 2025
Amazon a FSx mis à jour la politique FSx ConsoleReadOnlyAccess AWS gérée par Amazon	Amazon a FSx mis à jour la FSx ConsoleReadOnlyAccess politique d'Amazon pour ajouter l'`ec2:DescribeNetworkInterfaces` autorisation. Pour plus d'informations, consultez la FSx ConsoleReadOnlyAccess politique d'Amazon.	25 février 2025
Support ajouté pour la mise à niveau de la version Lustre	Vous pouvez désormais mettre à niveau la version Lustre de votre système de fichiers FSx for Lustre vers une version plus récente. Pour plus d'informations, consultez la section Gestion de la version Lustre.	12 février 2025

Amazon a FSx mis à jour la politique FSx ConsoleFullAccess AWS gérée par Amazon	Amazon a FSx mis à jour la FSx ConsoleFullAccess politique d'Amazon pour ajouter l'`ec2:DescribeNetworkInterfaces` autorisation. Pour plus d'informations, consultez la FSx ConsoleFullAccess politique d'Amazon.	7 février 2025
Région AWS Support supplémentaire ajouté pour le type de déploiement Persistent 2	Les SSD Persistent 2 FSx pour les systèmes de fichiers Lustre sont désormais disponibles en Asie-Pacifique (Malaisie Région AWS). Pour plus d'informations, consultez la section Disponibilité des types de déploiement.	2 janvier 2025
Lustresupport client pour Rocky Linux et Red Hat Enterprise Linux (RHEL) 9.5 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Rocky Linux et Red Hat Enterprise Linux (RHEL) 9.5. Pour plus d'informations, consultez la section Installation du Lustre client.	26 décembre 2024

Support ajouté pour EFA	Vous pouvez désormais créer un système de fichiers FSx pour Lustre Persistent 2 prenant en charge Elastic Fabric Adapter (EFA) afin d'améliorer les performances réseau des instances clientes compatibles EFA. L'activation d'EFA permet également de prendre en charge GPUDirect Storage (GDS) et ENA Express. Pour plus d'informations, consultez la section Utilisation de systèmes de fichiers compatibles avec EFA.	27 novembre 2024
Région AWS Support supplémentaire ajouté pour le type de déploiement Persistent 2	Les SSD Persistent 2 FSx pour les systèmes de fichiers Lustre sont désormais disponibles dans l'ouest des États-Unis (Californie du Nord) Région AWS. Pour plus d'informations, consultez la section Disponibilité des types de déploiement.	27 novembre 2024
Lustresupport client ajouté pour Ubuntu 22 Kernel 6.8.0	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Ubuntu 22.04 Kernel 6.8.0. Pour plus d'informations, consultez la section Installation du Lustre client.	8 novembre 2024

Support ajouté pour des CloudWatch statistiques Amazon supplémentaires et un tableau de bord de surveillance amélioré	FSx for Lustre fournit désormais des indicateurs supplémentaires sur le réseau, les performances et le stockage, ainsi qu'un tableau de bord de surveillance amélioré pour une meilleure visibilité de l'activité du système de fichiers. Pour plus d'informations, consultez la section Surveillance avec Amazon CloudWatch.	25 septembre 2024
Région AWS Support supplémentaire ajouté pour le type de déploiement Persistent 2	Les SSD Persistent 2 FSx pour les systèmes de fichiers Lustre sont désormais disponibles dans la zone locale de l'est des États-Unis (Dallas). Pour plus d'informations, consultez la section Disponibilité des types de déploiement.	20 septembre 2024
Lustresupport client ajouté pour Ubuntu 22 Kernel 6.5.0	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Ubuntu 22.04 Kernel 6.5.0. Pour plus d'informations, consultez la section Installation du Lustre client.	1er août 2024

Lustresupport client pour CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.10 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.10. Pour plus d'informations, consultez la section Installation du Lustre client.	18 juin 2024
Support ajouté pour améliorer les performances des métadonnées	Vous pouvez désormais créer un système de fichiers FSx pour Lustre Persisten t 2 avec une configuration de métadonnées qui permet d'améliorer les performances des métadonnées. Pour plus d'informations, consultez les sections Performances des métadonnées du système de fichiers et Gestion des performances des métadonné es.	6 juin 2024
Région AWS Support supplémentaire ajouté pour le type de déploiement Persisten t 2	Les SSD Persistent 2 FSx pour les systèmes de fichiers Lustre sont désormais disponibles dans la zone locale de l'est des États-Unis (Atlanta). Pour plus d'informa tions, consultez la section Disponibilité des types de déploiement.	29 mai 2024

Lustresupport client pour Rocky Linux et Red Hat Enterprise Linux (RHEL) 9.4 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Rocky Linux et Red Hat Enterprise Linux (RHEL) 9.4. Pour plus d'informations, consultez la section Installation du Lustre client.	16 mai 2024
Région AWS Support supplémentaire ajouté pour le type de déploiement Persistent 2	Les SSD Persistent 2 FSx pour les systèmes de fichiers Lustre sont désormais disponibles dans l'ouest du Canada (Calgary) Région AWS. Pour plus d'informations, consultez la section Disponibilité des types de déploiement.	3 mai 2024
Lustresupport client pour Amazon Linux 2023 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Amazon Linux 2023. Pour plus d'informations, consultez la section Installation du Lustre client.	25 mars 2024
Lustresupport client pour CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.9 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.9. Pour plus d'informations, consultez la section Installation du Lustre client.	9 janvier 2024

Amazon FSx FullAccess a FSx mis à jour les politiques FSx ServiceRolePolicy AWS gérées par Amazon FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon, Amazon et Amazon	Amazon a FSx mis à jour les FSx ServiceRolePolicy politiques d'Amazon FSx FullAccess FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon, Amazon et Amazon pour ajouter l'`ec2:GetSecurityGroupsForVpc` autorisation. Pour plus d'informations, consultez les FSx mises à jour des politiques AWS gérées par Amazon.	9 janvier 2024
Lustresupport client pour Rocky Linux et Red Hat Enterprise Linux (RHEL) 9.0 et 9.3 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Rocky Linux et Red Hat Enterprise Linux (RHEL) 9.0 et 9.3. Pour plus d'informations, consultez la section Installation du Lustre client.	20 décembre 2023
Amazon FSx for Lustre a mis à jour les politiques FSx ConsoleFullAccess AWS gérées par Amazon FSx FullAccess et Amazon	Amazon a FSx mis à jour les FSx ConsoleFullAccess politiques d'Amazon FSx FullAccess et d'Amazon pour ajouter `ManageCrossAccountDataReplication` cette action. Pour plus d'informations, consultez les FSx mises à jour des politiques AWS gérées par Amazon.	20 décembre 2023

Amazon a FSx mis à jour FSx FullAccess les politiques FSx ConsoleFullAccess AWS gérées par Amazon et Amazon	Amazon a FSx mis à jour les FSx ConsoleFullAccess politiques d'Amazon FSx FullAccess et d'Amazon pour ajouter l'`fsx:CopySnapshotAndUpdateVolume` autorisation. Pour plus d'informations, consultez les FSx mises à jour des politiques AWS gérées par Amazon.	26 novembre 2023
Support ajouté pour la mise à l'échelle de la capacité de débit	Vous pouvez désormais modifier la capacité de débit des systèmes de fichiers SSD persistants existants FSx pour Lustre au fur et à mesure de l'évolution de vos exigences en matière de débit. Pour plus d'informations, consultez la section Gestion de la capacité de débit.	16 novembre 2023
Amazon a FSx mis à jour FSx FullAccess les politiques FSx ConsoleFullAccess AWS gérées par Amazon et Amazon	Amazon a FSx mis à jour les FSx ConsoleFullAccess politiques d'Amazon FSx FullAccess et d'Amazon pour ajouter les `fsx:UpdateSharedVPCConfiguration` autorisations `fsx:DescribeSharedVPCConfiguration` et. Pour plus d'informations, consultez les FSx mises à jour des politiques AWS gérées par Amazon.	14 novembre 2023

Support ajouté pour les quotas de projets	Vous pouvez désormais créer des quotas de stockage pour les projets. Un quota de projet s'applique à tous les fichiers ou répertoires associés à un projet. Pour plus d'informations, consultez la section Quotas de stockage.	29 août 2023
Support ajouté pour la Lustre version 2.15	Tous les systèmes de fichiers FSx pour Lustre sont désormais basés sur la Lustre version 2.15 lorsqu'ils sont créés à l'aide de la FSx console Amazon. Pour plus d'informations, consultez Étape 1 : Création de votre système de fichiers Amazon FSx for Lustre.	29 août 2023
Région AWS Support supplémentaire ajouté pour le type de déploiement Persistent 2	Les systèmes de fichiers Persistent 2 FSx pour Lustre sont désormais disponibles en Israël (Tel Aviv Région AWS). Pour plus d'informations, consultez la section Options de déploiement FSx pour les systèmes de fichiers Lustre.	24 août 2023

Support ajouté pour les tâches du référentiel de données de publication	FSx for Lustre fournit désormais des tâches de référentiel de données de publication permettant de publier des fichiers archivés à partir d'un système de fichiers lié à un référentiel de données S3. La libération d'un fichier conserve la liste des fichiers et les métadonnées, mais supprime la copie locale du contenu de ce fichier. Pour plus d'informations, consultez la section Utilisation des tâches du référentiel de données pour libérer des fichiers.	9 août 2023
Amazon a FSx mis à jour la politique FSx ServiceRolePolicy AWS gérée par Amazon	Amazon a FSx mis à jour l'`cloudwatch:PutMetricData` autorisation dans Amazon FSxServiceRolePolicy. Pour plus d'informations, consultez les FSx mises à jour des politiques AWS gérées par Amazon.	24 juillet 2023
Amazon a FSx mis à jour la politique FSx FullAccess AWS gérée par Amazon	Amazon a FSx mis à jour la FSx FullAccess politique d'Amazon afin de supprimer l'`fsx:*`autorisation et d'ajouter des `fsx` actions spécifiques. Pour plus d'informations, consultez la FSx FullAccess politique d'Amazon.	13 juillet 2023

Amazon a FSx mis à jour la politique FSx ConsoleFullAccess AWS gérée par Amazon	Amazon a FSx mis à jour la FSx ConsoleFullAccess politique d'Amazon afin de supprimer l'`fsx:*`autorisation et d'ajouter des `fsx` actions spécifiques. Pour plus d'informations, consultez la FSx ConsoleFullAccess politique d'Amazon.	13 juillet 2023
Lustresupport client pour CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.8 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.8. Pour plus d'informations, consultez la section Installation du Lustre client.	25 mai 2023
Support ajouté AutoImport et AutoExport indicateurs	FSx for Lustre fournit désormais des CloudWatch métriques Amazon qui surveillent les mises à jour automatiques des importations et des exportations pour les systèmes de fichiers liés aux référentiels de données. Pour plus d'informations, consultez la section Surveillance avec Amazon CloudWatch.	31 mars 2023

Ajout du support DRA pour les types de déploiement Persistent 1 et Scratch 2	Vous pouvez désormais créer des associations de référentiels de données pour lier les référentiels de données aux systèmes de fichiers Lustre 2.12 avec les types de déploiement Persistent 1 ou Scratch 2. Pour plus d'informations, consultez la section Utilisation de référentiels de données avec Amazon FSx for Lustre.	29 mars 2023
Lustresupport client pour CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.7 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.7. Pour plus d'informations, consultez la section Installation du Lustre client.	5 décembre 2022
Région AWS Support supplémentaire ajouté pour le type de déploiement Persistent 2	Les SSD Persistent 2 de nouvelle génération FSx pour les systèmes de fichiers Lustre sont désormais disponibles en Europe (Stockholm), en Asie-Pacifique (Hong Kong), en Asie-Pacifique (Mumbai) et en Asie-Pacifique (Séoul) Régions AWS. Pour plus d'informations, consultez la section Options de déploiement FSx pour les systèmes de fichiers Lustre.	10 novembre 2022

Lustresupport client pour CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.6 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS, Rocky Linux et Red Hat Enterprise Linux (RHEL) 8.6. Pour plus d'informations, consultez la section Installation du Lustre client.	8 septembre 2022
Lustresupport client pour Ubuntu 22 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Ubuntu 22.04. Pour plus d'informations, consultez la section Installation du Lustre client.	28 juillet 2022
Lustresupport client pour Rocky Linux ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant Rocky Linux. Pour plus d'informations, consultez la section Installation du Lustre client.	8 juillet 2022
Support ajouté pour les courges Lustre racines	Vous pouvez désormais utiliser la fonctionnalité Lustre root squash pour restreind re l'accès au niveau root aux clients qui tentent d'accéder à votre système de fichiers FSx for Lustre en tant que root. Pour plus d'informations, voir LustreRacine de courge.	25 mai 2022

Région AWS Support supplémentaire ajouté pour le type de déploiement Persistent 2	Les SSD Persistent 2 de nouvelle génération FSx pour les systèmes de fichiers Lustre sont désormais disponibles en Europe (Londres), en Asie-Pacifique (Singapour) et en Asie-Pacifique (Sydney). Régions AWS Pour plus d'informations, consultez la section Options de déploiement FSx pour les systèmes de fichiers Lustre.	19 avril 2022
Support ajouté pour l'utilisation AWS DataSync de la migration de fichiers vers vos systèmes de fichiers Amazon FSx for Lustre.	Vous pouvez désormais l'utiliser AWS DataSync pour migrer des fichiers depuis des systèmes de fichiers existants vers FSx des systèmes de fichiers Lustre. Pour plus d'informations, consultez Comment migrer des fichiers existants vers Lustre à FSx l'aide de Lustre AWS DataSync.	5 avril 2022
Support ajouté pour les points de AWS PrivateLink terminaison VPC d'interface	Vous pouvez désormais utiliser les points de terminaison VPC de l'interface pour accéder à l' FSx API Amazon depuis votre VPC sans envoyer de trafic sur Internet. Pour plus d'informations, consultez Amazon FSx et les points de terminaison VPC d'interface.	5 avril 2022

Support ajouté pour la mise en file d'attente Lustre DRA	Vous pouvez désormais créer une DRA (association de référentiel de données) lorsque vous créez un système de fichiers FSx pour Lustre. La demande sera mise en file d'attente et le DRA sera créé une fois que le système de fichiers sera disponible. Pour plus d'informations, consultez Lier votre système de fichiers à un compartiment S3.	28 février 2022
Lustresupport client pour CentOS et Red Hat Enterprise Linux (RHEL) 8.5 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS et Red Hat Enterprise Linux (RHEL) 8.5. Pour plus d'informations, consultez la section Installation du Lustre client.	20 décembre 2021

Support pour l'exportation des modifications depuis FSx for Lustre vers un référentiel de données lié	Vous pouvez désormais configurer Lustre FSx pour qu'il exporte automatiquement les fichiers nouveaux, modifiés et supprimés de votre système de fichiers vers un référentiel de données Amazon S3 lié. Vous pouvez utiliser les tâches du référentiel de données pour exporter les modifications de données et de métadonnées vers le référentiel de données. Vous pouvez également configurer des liens vers plusieurs référentiels de données. Pour plus d'informations, consultez la section Exportation des modifications apportées au référentiel de données.	30 novembre 2021
Support ajouté pour la Lustre journalisation	Vous pouvez désormais configurer Lustre FSx pour qu'il enregistre les événements d'erreur et d'avertissement relatifs aux référentiels de données associés à votre système de fichiers sur Amazon CloudWatch Logs. Pour plus d'informations, consultez la section Logging with Amazon CloudWatch Logs.	30 novembre 2021

Les systèmes de fichiers SSD persistants prennent en charge un débit plus élevé et une capacité de stockage réduite	Les SSD persistants de nouvelle génération FSx pour les systèmes de fichiers Lustre offrent des options de débit plus élevées et une capacité de stockage minimale inférieur e. Pour plus d'informations, consultez la section Options de déploiement FSx pour les systèmes de fichiers Lustre.	30 novembre 2021
Support ajouté pour la Lustre version 2.12	Vous pouvez désormais choisir Lustre la version 2.12 lorsque vous créez un système de fichiers FSx pour Lustre. Pour plus d'informa tions, consultez Étape 1 : Création de votre système de fichiers Amazon FSx for Lustre.	5 octobre 2021
Lustresupport client pour CentOS et Red Hat Enterprise Linux (RHEL) 8.4 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS et Red Hat Enterprise Linux (RHEL) 8.4. Pour plus d'informations, consultez la section Installat ion du Lustre client.	9 juin 2021

Support ajouté pour la compression des données	Vous pouvez désormais activer la compression des données lorsque vous créez un système de fichiers FSx pour Lustre. Vous pouvez également activer ou désactiver la compression de données sur un système de fichiers existant FSx pour Lustre. Pour plus d'informations, consultez la section Compression Lustre des données.	27 mai 2021
Support ajouté pour la copie de sauvegardes	Vous pouvez désormais utiliser Amazon FSx pour copier des sauvegardes au sein d'un même site Compte AWS vers une autre Région AWS (copies interrégionales) ou dans le même environnement Région AWS (copies internes à la région). Pour plus d'informations, consultez la section Copie de sauvegardes.	12 avril 2021
Lustresupport client pour les ensembles de Lustre fichiers	Le client FSx for Lustre prend désormais en charge l'utilisation de jeux de fichiers pour monter uniquement un sous-ensemble de l'espace de noms du système de fichiers. Pour plus d'informations, consultez la section Montage de jeux de fichiers spécifiques.	18 mars 2021

Support ajouté pour l'accès des clients à l'aide d'adresses IP non privées	Vous pouvez accéder aux systèmes FSx de fichiers Lustre à partir d'un client local à l'aide d'adresses IP non privées. Pour plus d'informations, consultez Montage de systèmes de Amazon FSx fichiers sur site ou depuis un Amazon VPC pair.	17 décembre 2020
Lustresupport client pour CentOS 7.9 basé sur ARM ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS 7.9 basé sur ARM. Pour plus d'informations, consultez la section Installation du Lustre client.	17 décembre 2020
Lustresupport client pour CentOS et Red Hat Enterprise Linux (RHEL) 8.3 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS et Red Hat Enterprise Linux (RHEL) 8.3. Pour plus d'informations, consultez la section Installation du Lustre client.	16 décembre 2020

Support ajouté pour le dimensionnement de la capacité de stockage et de débit	Vous pouvez désormais augmenter la capacité de stockage et de débit des systèmes de fichiers existants FSx pour Lustre au fur et à mesure de l'évolution de vos besoins en matière de stockage et de débit. Pour plus d'informations, consultez la section Gestion du stockage et de la capacité de débit.	24 novembre 2020
Support ajouté pour les quotas de stockage	Vous pouvez désormais créer des quotas de stockage pour les utilisateurs et les groupes. Les quotas de stockage limitent la quantité d'espace disque et le nombre de fichiers qu'un utilisateur ou un groupe peut consommer sur votre système de fichiers FSx for Lustre. Pour plus d'informations, consultez la section Quotas de stockage.	9 novembre 2020
Amazon FSx est désormais intégré à AWS Backup	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder et restaurer vos systèmes de FSx fichiers en plus d'utiliser les FSx sauvegardes natives d'Amazon. Pour plus d'informations, consultez la section Utilisation AWS Backup avec Amazon FSx.	9 novembre 2020

Support ajouté pour les options de stockage sur disque dur	Outre l'option de stockage SSD (Solid State Drive), FSx for Lustre prend désormais en charge l'option de stockage HDD (disque dur). Vous pouvez configurer votre système de fichiers pour utiliser le disque dur pour les charges de travail gourmandes en débit qui impliquent généralement des opérations de fichiers séquentielles volumineuses. Pour plus d'informations, consultez la section Options de stockage multiples.	12 août 2020
Support pour l'importation des modifications du référentiel de données liées dans FSx for Lustre	Vous pouvez désormais configurer votre système de fichiers FSx for Lustre pour importer automatiquement les nouveaux fichiers ajoutés et les fichiers modifiés dans un référentiel de données lié après la création du système de fichiers. Pour plus d'informations, voir Importer automatiquement les mises à jour depuis le référentiel de données.	23 juillet 2020

Lustresupport client pour SUSE Linux SP4 et ajout SP5	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant SP4 SUSE Linux et. SP5 Pour plus d'informations, consultez la section Installation du Lustre client.	20 juillet 2020
Lustresupport client pour CentOS et Red Hat Enterprise Linux (RHEL) 8.2 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant CentOS et Red Hat Enterprise Linux (RHEL) 8.2. Pour plus d'informations, consultez la section Installation du Lustre client.	20 juillet 2020
Support pour les sauvegardes automatiques et manuelles des systèmes de fichiers ajouté	Vous pouvez désormais effectuer des sauvegardes quotidiennes automatiques et des sauvegardes manuelles de systèmes de fichiers non liés à un référentiel de données durable Amazon S3. Pour plus d'informations, consultez la page Utilisation des sauvegardes.	23 Juin 2020

Publication de deux nouveaux types de déploiement de systèmes de fichiers	Les systèmes de fichiers Scratch sont conçus pour le stockage temporaire et le traitement des données à court terme. Les systèmes de fichiers persistants sont conçus pour le stockage et les charges de travail à long terme. Pour plus d'informations, consultez les options FSx de déploiement de Lustre.	12 février 2020
Support pour les métadonnées POSIX ajouté	FSx for Lustre conserve les métadonnées POSIX associées lors de l'importation et de l'exportation de fichiers vers un référentiel de données durable lié sur Amazon S3. Pour plus d'informations, consultez la section Support des métadonnées POSIX pour les référentiels de données.	23 décembre 2019
Nouvelle fonctionnalité de tâches du référentiel de données publiée	Vous pouvez désormais exporter les données modifiées et les métadonnées POSIX associées vers un référentiel de données durable lié sur Amazon S3 à l'aide de tâches de référentiel de données. Pour plus d'informations, consultez la section Tâches du référentiel de données.	23 décembre 2019

Région AWS Support supplémentaire ajouté	FSx for Lustre est désormais disponible dans la région Europe (Londres) Région AWS. FSx Pour connaître les limites spécifiques à la région Lustre, voir Limites.	9 juillet 2019
Région AWS Support supplémentaire ajouté	FSx for Lustre est désormais disponible en Asie-Pacifique (Singapour Région AWS). FSx Pour connaître les limites spécifiques à la région Lustre, voir Limites.	26 juin 2019
Lustresupport client pour Amazon Linux et Amazon Linux 2 ajouté	Le client FSx for Lustre prend désormais en charge les instances Amazon EC2 exécutant et. Amazon Linux Amazon Linux 2 Pour plus d'informations, consultez la section Installation du Lustre client.	11 mars 2019

Ajout du support du chemin d'exportation de données défini par l'utilisateur	Les utilisateurs ont désormais la possibilité de remplacer les objets d'origine dans votre compartiment Amazon S3 ou d'écrire les fichiers nouveaux ou modifiés dans un préfixe que vous spécifiez. Avec cette option, vous disposez d'une flexibilité supplémentaire FSx pour intégrer Lustre dans vos flux de travail de traitement des données. Pour plus d'informations, consultez Exporter des données vers votre compartiment Amazon S3.	6 février 2019
La limite totale de stockage par défaut a été augmentée	Le stockage total par défaut FSx pour tous les systèmes de fichiers Lustre est passé à 100 800 GiB. Pour plus d'informations, consultez Limites .	11 janvier 2019
Amazon FSx for Lustre est désormais disponible pour tous	Amazon FSx for Lustre est un système de fichiers entièrement géré optimisé pour les charges de travail intensives, telles que le calcul haute performance, l'apprentissage automatique et les flux de travail de traitement multimédia.	28 novembre 2018

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.