Guide de l'utilisateur

AWS DataSync

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

AWS DataSync: Guide de l’utilisateur

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

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez 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 que c'est AWS DataSync ? ... 1
Cas d'utilisation ... 2
Avantages ... 3
Ressources supplémentaires ... 3
Comment ça marche ... 4
DataSync architecture de transfert ... 4
Transfert entre le stockage sur site et AWS ... 4
Transfert entre les services AWS de stockage ... 5
Transfert entre les services AWS de stockage et les systèmes de stockage dans d'autres clouds ... 6
Concepts et terminologie ... 7
Agent ... 7
Emplacement ... 8
Tâche ... 8
Exécution des tâches ... 8
Comment DataSync transférer des fichiers, des objets et des répertoires ... 8
Comment DataSync prépare votre transfert de données ... 9
Comment DataSync transfèrent vos données ... 10
Comment DataSync vérifie l'intégrité de vos données ... 10
Comment DataSync fonctionne avec les fichiers ouverts et verrouillés ... 11
Options de transfert récurrentes ... 11
Premiers pas ... 13
Inscrivez-vous pour un Compte AWS ... 13
Création d'un utilisateur doté d'un accès administratif ... 13
Autorisations IAM requises pour utiliser DataSync ... 15
AWS politiques gérées ... 15
Politiques gérées par le client ... 16
Où puis-je l'utiliser DataSync ? ... 16
Comment puis-je l'utiliser DataSync ? ... 16
Combien va DataSync coûter ? ... 16
Composants open source utilisés par DataSync ... 16
Ai-je besoin d'un agent ? ... 16
Situations dans lesquelles vous avez besoin d'un DataSync agent ... 17
Situations dans lesquelles vous n'avez pas besoin d'un DataSync agent ... 17

Utilisation de plusieurs DataSync agents ... 18
Étapes suivantes ... 18
Exigences relatives aux agents ... 19
Exigences relatives à l'hyperviseur ... 19
Exigences relatives aux agents pour les DataSync transferts ... 19
Exigences relatives aux agents pour les Région AWS partitions ... 21
Exigences relatives à la gestion des agents ... 21
Déploiement de votre agent ... 21
Déploiement de votre agent sur VMware ... 21
Déploiement de votre agent sur KVM ... 22
Déploiement de votre agent sur Microsoft Hyper-V ... 23
Déploiement de votre EC2 agent Amazon ... 24
Déploiement de votre agent sur AWS Snowball Edge ... 30
Déploiement de votre agent sur AWS Outposts ... 30
Choisir un point de terminaison de service pour votre agent ... 31
Choisir un point de terminaison de service public ... 31
Choix d'un point de terminaison de service FIPS ... 31
Choix d'un point de terminaison de service VPC ... 32
Activation de votre agent ... 34
Prérequis ... 35
Obtenir une clé d'activation ... 35
Activation de votre agent ... 37
Étapes suivantes ... 40
Vérification des connexions réseau de votre agent ... 41
Accès à la console locale de votre agent ... 41
Vérification de la connexion de votre agent à votre système de stockage ... 42
Vérification de la connexion de votre agent au DataSync service ... 43
Étapes suivantes ... 43
Connecter votre réseau ... 44
1. Connexion réseau entre votre système de stockage et l'agent ... 44
2. Connexion réseau entre votre agent et le DataSync service ... 44
Connexion de votre réseau de stockage à AWS ... 45
Choix d'un point de terminaison de service ... 45
3. Connexion réseau entre le DataSync service et le service AWS de stockage ... 45
Réseauter lorsque vous n'avez pas besoin d'un DataSync agent ... 46
Comment et où DataSync le trafic circule sur le réseau ... 46

Sécurité du réseau pour DataSync ... 46
Exigences réseau ... 46
IPv6 soutien ... 47
Exigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie ... 48
Configuration réseau requise pour les services AWS de stockage ... 53
Exigences réseau pour les points de terminaison publics ou de service FIPS ... 54
Configuration réseau requise pour les points de terminaison de service VPC ... 61
Interfaces réseau pour les transferts de données ... 64
Interfaces réseau pour les transferts avec les agents ... 64
Interfaces réseau pour les transferts sans agents ... 65
Affichage de vos interfaces réseau ... 66
Exemples d'architecture et de routage avec Direct Connect ... 67
Utilisation de Direct Connect avec un point de terminaison de DataSync service VPC ... 67
Utilisation de Direct Connect avec un point de terminaison de service DataSync public ou FIPS ... 71
Étapes suivantes ... 72
Configuration de votre agent pour plusieurs NICs ... 72
Transfert de données ... 73
Où puis-je transférer mes données ? ... 74
Transferts pris en charge dans le même Compte AWS ... 74
Transferts pris en charge entre Comptes AWS ... 76
Transferts pris en charge dans le même Région AWS ... 77
Transferts pris en charge entre Régions AWS ... 78
Déterminer si votre transfert nécessite un DataSync agent ... 78
Transfert vers ou depuis le stockage sur site ... 78
Configuration des transferts avec un serveur de fichiers NFS ... 79
Configuration des transferts avec un serveur de fichiers SMB ... 83
Configuration des transferts avec un cluster HDFS ... 95
Configuration des transferts avec un système de stockage d'objets ... 100
Transfert vers ou depuis le AWS stockage ... 104
Configuration des transferts avec Amazon S3 ... 105
Configuration des transferts avec Amazon EFS ... 138
Configuration des transferts avec FSx pour Windows File Server ... 148
Configuration des transferts avec FSx for Lustre ... 154
Configuration des transferts avec FSx pour OpenZFS ... 156

Configuration des transferts avec FSx for ONTAP ... 160
Transfert vers ou depuis un autre stockage dans le cloud ... 168
Planification des transferts vers ou depuis des systèmes de stockage cloud tiers ... 169
Configuration des transferts avec Google Cloud Storage ... 171
Configuration des transferts avec Microsoft Azure Blob Storage ... 181
Configuration des transferts avec Microsoft Azure Files ... 199
Configuration des transferts avec d'autres solutions de stockage d'objets dans le cloud ... 202
Transfert vers ou depuis un stockage compatible S3 sur Snowball Edge ... 210
Prérequis ... 210
Fournir DataSync un accès au stockage compatible S3 ... 210
Création d'un DataSync agent dans votre environnement de stockage sur site ... 213
Configuration de l'emplacement de la source pour votre transfert ... 214
Configuration de l'emplacement de destination pour votre transfert ... 215
Configuration de vos paramètres de transfert ... 216
Commencer votre transfert ... 216
Limites ... 216
Création d'une tâche de transfert de données ... 217
Création de votre tâche ... 217
Statuts des tâches ... 220
Partitionnement de grands ensembles de données avec plusieurs tâches ... 220
Segmentation des données transférées à l'aide de plusieurs tâches ... 221
Choix d'un mode de tâche pour votre transfert ... 221
Choix des données à transférer ... 227
Vérifier l'intégrité des données ... 268
Définition des limites de bande passante ... 271
Planification de votre tâche ... 273
Marquer vos tâches ... 278
Démarrage d'une tâche de transfert de données ... 282
Démarrage de votre tâche ... 282
Statuts d'exécution des tâches ... 283
Savoir quand votre tâche est en file d'attente ... 285
Annulation de l'exécution de vos tâches ... 285
Surveillance des transferts de données ... 286
Comprendre les compteurs de performance du transfert de données ... 286
Surveillance des transferts de données à l'aide de CloudWatch métriques ... 305
CloudWatch métriques pour DataSync ... 305

Surveillance des transferts de données à l'aide de rapports de tâches 309
Cas d'utilisation 310
Rapports de tâches récapitulatifs uniquement 310
Rapports de tâches standard 310
Exemples de rapports de tâches 314
Limites 317
Création de vos rapports de tâches 317
Afficher vos rapports de tâches 328
Surveillance des transferts de données avec CloudWatch les journaux 329
DataSync Autoriser le téléchargement de journaux dans un groupe de CloudWatch journaux 329
Configuration de la journalisation pour votre DataSync tâche 331
Afficher les journaux des DataSync tâches 334
Se connecter avec CloudTrail 336
Utilisation des DataSync informations contenues dans CloudTrail 336
Comprendre les entrées du fichier DataSync journal 337
Surveillance avec EventBridge 339
DataSync événements de transfert 339
Surveillance à l'aide d'outils manuels 341
Surveillance de votre transfert à l'aide de la DataSync console 341
Surveillez votre transfert à l'aide du AWS CLI 342
Surveillance de votre transfert à l'aide de l'`watch`utilitaire 344
Gestion des ressources 345
Gérer votre DataSync agent 345
Tester la connectivité et les ressources système de votre DataSync agent 345
Remplacement de votre DataSync agent 345
Nettoyage des DataSync ressources 345
Réutilisation de l'infrastructure d'un DataSync agent 345
Gérer votre agent 345
Mises à jour logicielles des agents 346
Statuts des agents 346
Résolution des problèmes liés à votre agent 347
Effectuer la maintenance de votre agent 347
Accès à la console locale de votre agent 347
Configuration des paramètres DHCP, DNS et IP de votre agent 349
Vérification des ressources système de votre agent 353

Synchronisation de l'heure de votre agent VMware 354
Exécution de commandes liées à la maintenance pour votre agent 355
Remplacement de votre agent 357
Création d'un nouvel agent 357
Mettre à jour votre position avec le nouvel agent 358
Étapes suivantes 363
Filtrer DataSync les ressources 364
Paramètres de filtrage 364
Filtrer par localisation 365
Filtrer par tâche 366
Nettoyage des DataSync ressources 367
Supprimer un DataSync agent 367
Réutilisation de l'infrastructure d'un DataSync agent 368
Supprimer un DataSync emplacement 369
Supprimer une DataSync tâche 369
Sécurité 371
Protection des données 372
Chiffrement en transit 372
Chiffrement au repos 375
Confidentialité du trafic inter-réseau 376
Gestion des identités et des accès 377
Gestion des accès 377
AWS politiques gérées 382
Politiques gérées par le client 393
Utilisation des rôles liés aux services 396
Balisage des ressources pendant la création 400
Prévention du problème de l'adjoint confus entre services 402
Validation de conformité 404
Résilience 405
Sécurité de l'infrastructure 406
Sécurisation des identifiants de localisation de stockage 406
Utilisation d'un secret géré par un service chiffré avec une clé par défaut 407
Utilisation d'un secret géré par un service chiffré à l'aide d'une clé personnalisée AWS KMS 408
Utiliser un secret que vous gérez 409
Quotas 413

Limites relatives au système de stockage, aux fichiers et aux objets 413
DataSync quotas 413
Demander une augmentation de quota 419
Résolution des problèmes 420
Résolution des problèmes liés aux agents 420
Comment me connecter à la console locale d'un EC2 agent Amazon ? 420
Que signifie l'erreur « Impossible de récupérer la clé d'activation de l'agent » ? 421
Je ne parviens toujours pas à activer un agent à l'aide d'un point de terminaison de service VPC 421
Que dois-je faire si mon agent est hors ligne ? 421
Je ne sais pas ce qui se passe avec mon agent. Quelqu'un peut-il m'aider ? 422
Résolution des problèmes de localisation 423
Ma tâche a échoué avec un message d'erreur indiquant que les autorisations NFS ont été refusées 423
Ma tâche a échoué en raison d'une erreur de montage NFS 424
Ma tâche a échoué en raison d'une erreur de montage Amazon EFS 425
La propriété des fichiers n'est pas maintenue avec le transfert NFS 425
Ma tâche ne peut pas accéder à un emplacement SMB qui utilise Kerberos 426
Ma tâche a échoué en raison d'une input/output erreur 427
Erreur: `FsS3UnableToConnectToEndpoint` 428
Erreur: `FsS3HeadBucketFailed` 428
Échec de la tâche avec une `Unable to list Azure Blobs on the volume root` erreur 428
Erreur: `FsAzureBlobVolRootListBlobsFailed` 429
Erreur: `SrcLocHitAccess` 429
Erreur: `SyncTaskErrorLocationNotAdded` 429
Erreur: `S3 location creation failed with (InvalidRequestException) when calling the CreateLocationS3 operation` 429
La tâche avec l'emplacement source S3 échoue avec `HeadObject` ou sans `GetObjectTagging` erreur 430
Résolution des problèmes liés aux tâches 430
Erreur : SyncOption valeur non valide. Option : TransferModePreserveDeletedFiles, Valeur : TOUT, SUPPRIMER. 430
L'exécution de la tâche échoue avec une EniNotFounderreur 431
L'exécution de la tâche échoue avec une erreur « Impossible d'allouer de la mémoire » 431
La tâche échoue avec le `Input/Output error` système de fichiers for ONTAP 432

La tâche échoue avec `Connection reset by host` ou `Host is down` pour le système de fichiers ONTAP ... 434
L'exécution de la tâche a un statut de lancement mais rien ne semble se passer ... 434
L'exécution de la tâche semble bloquée dans l'état de préparation ... 435
L'exécution de la tâche s'arrête avant la fin du transfert ... 435
L'exécution de la tâche échoue lors du transfert depuis un bucket Google Cloud Storage ... 435
Il existe des incohérences entre les horodatages de l'exécution des tâches ... 436
L'exécution de la tâche échoue avec une `NoMem` erreur ... 436
L'objet ne parvient pas à être transféré en raison Azure Blob Storage d'une `user metadata key` erreur ... 436
Il y a un `/.aws-datasync` dossier dans l'emplacement de destination ... 437
Impossible de transférer des liens symboliques entre des sites à l'aide du protocole SMB ... 437
Erreurs dans les rapports de tâches ... 438
Résolution des problèmes de vérification des données ... 438
Il existe des incohérences entre le contenu d'un fichier ... 438
Il existe une incompatibilité entre les métadonnées SMB d'un fichier ... 440
Les fichiers à transférer ne se trouvent plus à l'emplacement source ... 441
DataSync Impossible de vérifier les données de destination ... 441
DataSync Impossible de lire les métadonnées des objets ... 442
Les métadonnées définies par le système d'un objet ne correspondent pas ... 443
Comprendre la durée de vérification des données ... 445
Résolution des coûts de stockage S3 avec DataSync ... 445
Didacticiels ... 447
Transfert d'un compte sur site à S3 ... 447
Présentation ... 447
Prérequis : autorisations de compte source requises ... 448
Prérequis : autorisations requises pour le compte de destination ... 450
Étape 1 : Dans votre compte source, créez un DataSync agent ... 451
Étape 2 : dans votre compte source, créez un rôle DataSync IAM pour accéder au compartiment de destination ... 451
Étape 3 : dans votre compte de destination, mettez à jour votre politique de compartiment S3 ... 454
Étape 4 : Dans votre compte de destination, ACLs désactivez-la pour votre compartiment S3 ... 455
Étape 5 : Dans votre compte source, créez un emplacement DataSync source pour votre stockage sur site ... 456

Étape 6 : Dans votre compte source, créez un emplacement de DataSync destination pour votre compartiment S3 ... 456
Étape 7 : Dans votre compte source, créez et lancez votre DataSync tâche ... 457
Ressources connexes ... 457
Transfert entre compartiments S3 entre comptes ... 459
Présentation ... 459
Prérequis : autorisations de compte source requises ... 461
Prérequis : autorisations requises pour le compte de destination ... 463
Étape 1 : dans votre compte source, créez un rôle DataSync IAM pour accéder au compartiment de destination ... 464
Étape 2 : dans votre compte de destination, mettez à jour votre politique de compartiment S3 ... 466
Étape 3 : dans votre compte de destination, ACLs désactivez-la pour votre compartiment S3 ... 467
Étape 4 : Dans votre compte source, créez vos DataSync emplacements ... 468
Étape 5 : Dans votre compte source, créez et lancez votre DataSync tâche ... 470
Résolution des problèmes ... 472
Connexe : transferts entre comptes avec des compartiments S3 utilisant le chiffrement côté serveur ... 470
Réalisation d'une migration de grande envergure ... 473
Qu'est-ce qu'une migration de données volumineuse ? ... 473
Les étapes clés d'une migration de données volumineuses ... 473
Ressources supplémentaires ... 474
Étape 1 : Planification de votre migration ... 474
Exigences relatives à la collecte ... 475
Exécution d'une preuve de concept ... 481
Estimation des délais de migration ... 483
Étape 2 : Implémentation de votre migration ... 485
Accélérer votre migration grâce au partitionnement ... 486
Exécution de vos DataSync tâches ... 487
Surveillance de vos transferts ... 489
DataSync API ... 491
Actions ... 491
CancelTaskExecution ... 494
CreateAgent ... 496
CreateLocationAzureBlob ... 501

CreateLocationEfs 508
CreateLocationFsxLustre 514
CreateLocationFsxOntap 518
CreateLocationFsxOpenZfs 523
CreateLocationFsxWindows 528
CreateLocationHdfs 533
CreateLocationNfs 540
CreateLocationObjectStorage 545
CreateLocationS3 553
CreateLocationSmb 560
CreateTask 568
DeleteAgent 578
DeleteLocation 580
DeleteTask 582
DescribeAgent 584
DescribeLocationAzureBlob 589
DescribeLocationEfs 594
DescribeLocationFsxLustre 600
DescribeLocationFsxOntap 603
DescribeLocationFsxOpenZfs 608
DescribeLocationFsxWindows 612
DescribeLocationHdfs 616
DescribeLocationNfs 621
DescribeLocationObjectStorage 625
DescribeLocationS3 630
DescribeLocationSmb 635
DescribeTask 641
DescribeTaskExecution 651
ListAgents 668
ListLocations 672
ListTagsForResource 676
ListTaskExecutions 680
ListTasks 684
StartTaskExecution 688
TagResource 695
UntagResource 698

UpdateAgent 701
UpdateLocationAzureBlob 703
UpdateLocationEfs 708
UpdateLocationFsxLustre 712
UpdateLocationFsxOntap 715
UpdateLocationFsxOpenZfs 718
UpdateLocationFsxWindows 721
UpdateLocationHdfs 725
UpdateLocationNfs 731
UpdateLocationObjectStorage 735
UpdateLocationS3 741
UpdateLocationSmb 745
UpdateTask 752
UpdateTaskExecution 759
Types de données 761
AgentListEntry 764
AzureBlobSasConfiguration 766
CmkSecretConfig 767
CustomSecretConfig 769
Ec2Config 771
FilterRule 773
FsxProtocol 775
FsxProtocolNfs 776
FsxProtocolSmb 777
FsxUpdateProtocol 779
FsxUpdateProtocolSmb 781
HdfsNameNode 783
LocationFilter 785
LocationListEntry 787
ManagedSecretConfig 789
ManifestConfig 790
NfsMountOptions 792
OnPremConfig 794
Options 795
Platform 804
PrivateLinkConfig 805

QopConfiguration 807
ReportDestination 809
ReportDestinationS3 810
ReportOverride 812
ReportOverrides 813
ReportResult 815
S3Config 816
S3ManifestConfig 817
SmbMountOptions 819
SourceManifestConfig 821
TagListEntry 822
TaskExecutionFilesFailedDetail 823
TaskExecutionFilesListedDetail 825
TaskExecutionListEntry 827
TaskExecutionResultDetail 829
TaskFilter 832
TaskListEntry 834
TaskReportConfig 836
TaskSchedule 838
TaskScheduleDetails 840
Erreurs courantes 841
Paramètres communs 843
Historique de la documentation 846
AWS Glossaire 862
..... dccclxiii

Qu'est-ce que c'est AWS DataSync ?

AWS DataSync est un service de transfert de données en ligne qui simplifie la migration des données et vous aide à transférer rapidement, facilement et en toute sécurité les données de vos fichiers ou objets vers, depuis et entre les services AWS de stockage.

Transferts de stockage sur site

DataSync fonctionne avec les systèmes de stockage sur site suivants :

- Système de fichiers réseau (NFS)
- Bloc de messages du serveur (SMB)
- Systèmes de fichiers distribués Hadoop (HDFS)
- Stockage d'objets

AWS transferts de stockage

DataSync fonctionne avec les services AWS de stockage suivants :

- Amazon S3
- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Autres transferts de stockage dans le cloud

DataSync fonctionne avec les services de stockage suivants dans d'autres clouds :

- Google Cloud Storage
- Microsoft Azure Blob Storage
- Microsoft Azure Files
- Wasabi Cloud Storage

- DigitalOcean Spaces
- Oracle Cloud Infrastructure Object Storage
- Cloudflare R2 Storage
- Backblaze B2 Cloud Storage
- NAVER Cloud Object Storage
- Alibaba Cloud Object Storage Service
- IBM Cloud Object Storage
- Seagate Lyve Cloud

Transferts de stockage Edge

DataSync fonctionne avec les services et appareils de stockage Edge suivants :

- Stockage compatible avec Amazon S3 sur AWS Snowball Edge

Cas d'utilisation

Voici quelques-uns des principaux cas d'utilisation pour DataSync :

- Migrer les données : transférez rapidement les ensembles de données actifs sur le réseau vers les services AWS de stockage. DataSync inclut le chiffrement automatique et la validation de l'intégrité des données pour garantir que vos données arrivent en toute sécurité, intactes et prêtes à être utilisées.
- Archiver les données confidentielles — Déplacez les données confidentielles stockées dans le stockage sur site directement vers des classes de stockage à long terme durables et sécurisées telles que S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Cela peut libérer de la capacité de stockage sur site et arrêter les systèmes existants.
- Répliquer les données : copiez les données dans n'importe quelle classe de stockage Amazon S3, en choisissant la classe de stockage la plus rentable en fonction de vos besoins. Vous pouvez également envoyer des données vers Amazon EFS, FSx pour Windows File Server, FSx pour Lustre ou FSx pour OpenZFS pour un système de fichiers de secours.
- Transférez les données pour un traitement rapide dans le cloud — Transférez des données vers ou depuis des AWS fins de traitement. Cette approche peut accélérer les flux de travail cloud hybrides stratégiques dans de nombreux secteurs. Il s'agit notamment de l'apprentissage automatique dans le secteur des sciences de la vie, de la production vidéo dans les médias et le divertissement,

de l'analyse des mégadonnées dans les services financiers et de la recherche sismique dans l'industrie pétrolière et gazière.

Avantages

En utilisant DataSync, vous pouvez bénéficier des avantages suivants :

- Automatisez le mouvement des données : DataSync facilite le transfert de données sur le réseau entre les systèmes de stockage et les services. DataSync automatise à la fois la gestion des processus de transfert de données et l'infrastructure requise pour des transferts de données performants et sécurisés.
- Transférez les données en toute end-to-end sécurité : DataSync assure la sécurité, notamment le chiffrement et la validation de l'intégrité des données, afin de garantir que vos données arrivent en toute sécurité, intactes et prêtes à être utilisées. DataSync accède à votre AWS espace de stockage par le biais AWS de mécanismes de sécurité intégrés, tels que les AWS Identity and Access Management rôles (IAM). Il prend également en charge les points de terminaison du cloud privé virtuel (VPC), ce qui vous permet de transférer des données sans passer par l'Internet public et d'améliorer encore la sécurité des données copiées en ligne.
- Déplacez les données plus rapidement : DataSync utilise un protocole réseau spécialement conçu et une architecture parallèle multithread pour accélérer vos transferts. Cette approche accélère les migrations, les flux de travail récurrents de traitement des données pour l'analyse et l'apprentissage automatique, ainsi que les processus de protection des données.

Ressources supplémentaires

Nous vous recommandons de lire les documents suivants :

- DataSync ressources — Comprend des blogs, des vidéos et d'autres supports de formation
- AWS Re:post — Consultez la dernière discussion sur le sujet DataSync
- Tarification AWS DataSync

Comment AWS DataSync fonctionne

Découvrez les concepts clés et la terminologie liés aux AWS DataSync transferts, notamment la manière dont les données sont transférées depuis des sites sur site et dans le cloud.

DataSync architecture de transfert

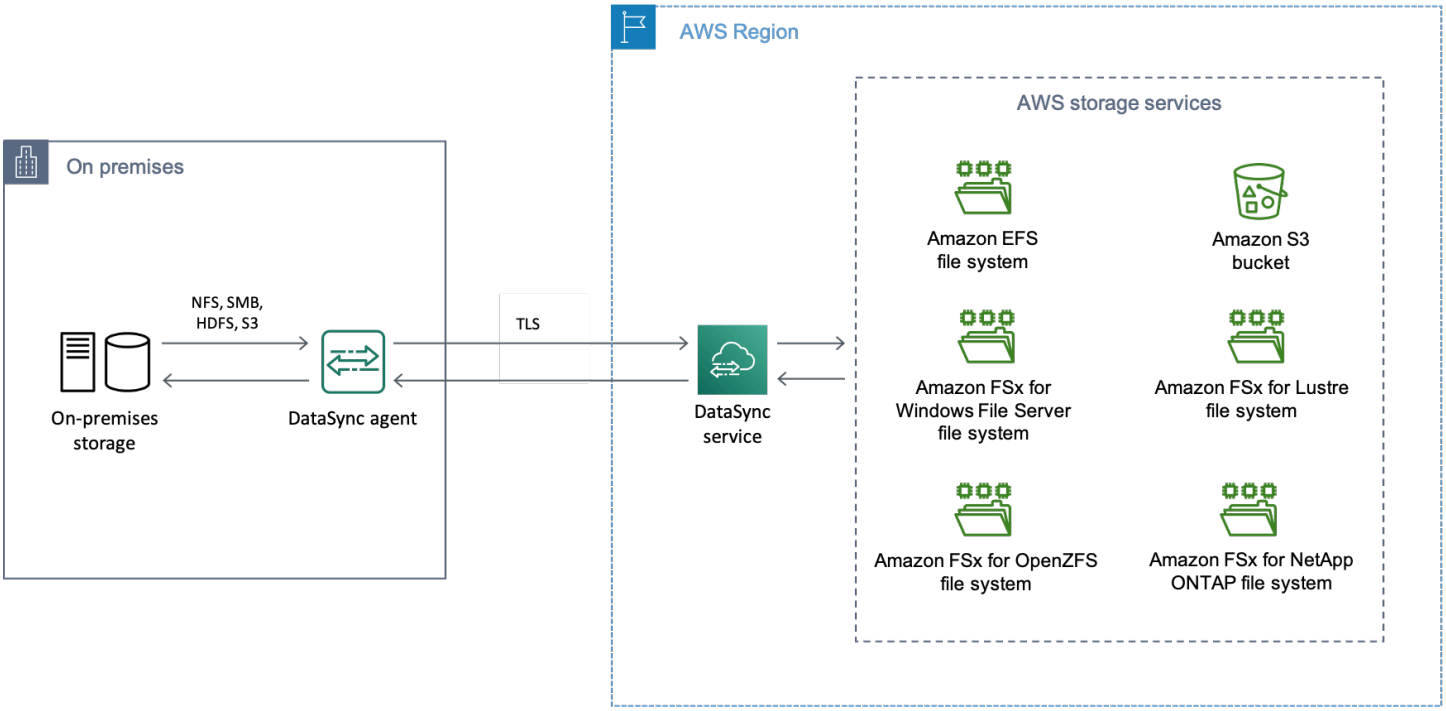
Les diagrammes suivants montrent comment et où DataSync les données de stockage sont généralement transférées. Pour obtenir la liste complète des systèmes et services de stockage DataSync pris en charge, voir Où puis-je transférer mes données AWS DataSync ?

Rubriques

- Transfert entre le stockage sur site et AWS
- Transfert entre les services AWS de stockage
- Transfert entre les services AWS de stockage et les systèmes de stockage dans d'autres clouds

Transfert entre le stockage sur site et AWS

Le schéma suivant présente une présentation générale du DataSync transfert de fichiers entre des systèmes de stockage sur site autogérés et. Services AWS

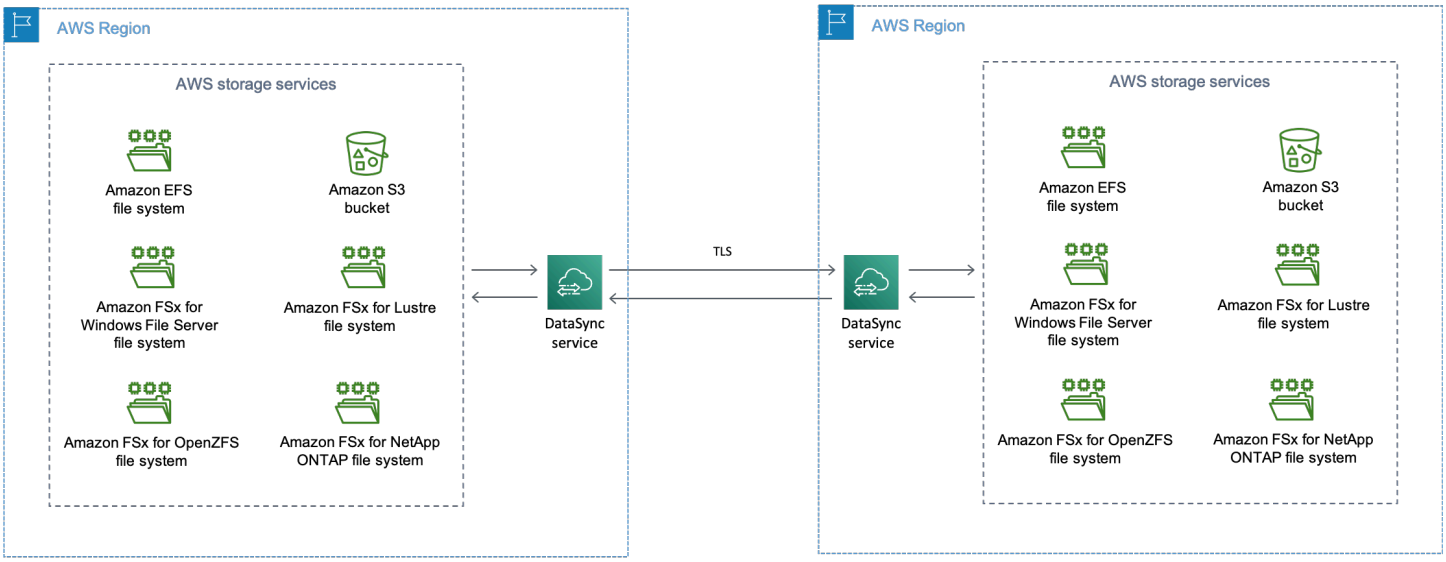


Le schéma illustre un cas d' DataSync utilisation courant :

- DataSync Agent copiant des données depuis un système de stockage sur site.
- Données transférées AWS, cryptées à l'aide du protocole TLS (Transport Layer Security).
- DataSync copie de données vers un service AWS de stockage compatible.

Transfert entre les services AWS de stockage

Le schéma suivant présente une vue d'ensemble détaillée du DataSync transfert de fichiers entre deux Services AWS systèmes Compte AWS.



Le schéma illustre un cas d' DataSync utilisation courant :

- DataSync copie de données depuis un service de AWS stockage pris en charge.
- Données transitant Régions AWS, cryptées à l'aide du protocole TLS.
- DataSync copie de données vers un service AWS de stockage compatible.

Lors du transfert entre services AWS de stockage (qu'ils soient identiques Région AWS ou Régions AWS interconnectés), vos données restent sur le AWS réseau et ne transitent pas par l'Internet public.

> **Important**
>
> Vous payez pour les données transférées entre Régions AWS. Ceci est facturé comme un transfert de données SORTANT de votre région source vers votre région de destination. Pour plus d'informations, consultez la section Tarification des transferts de données.

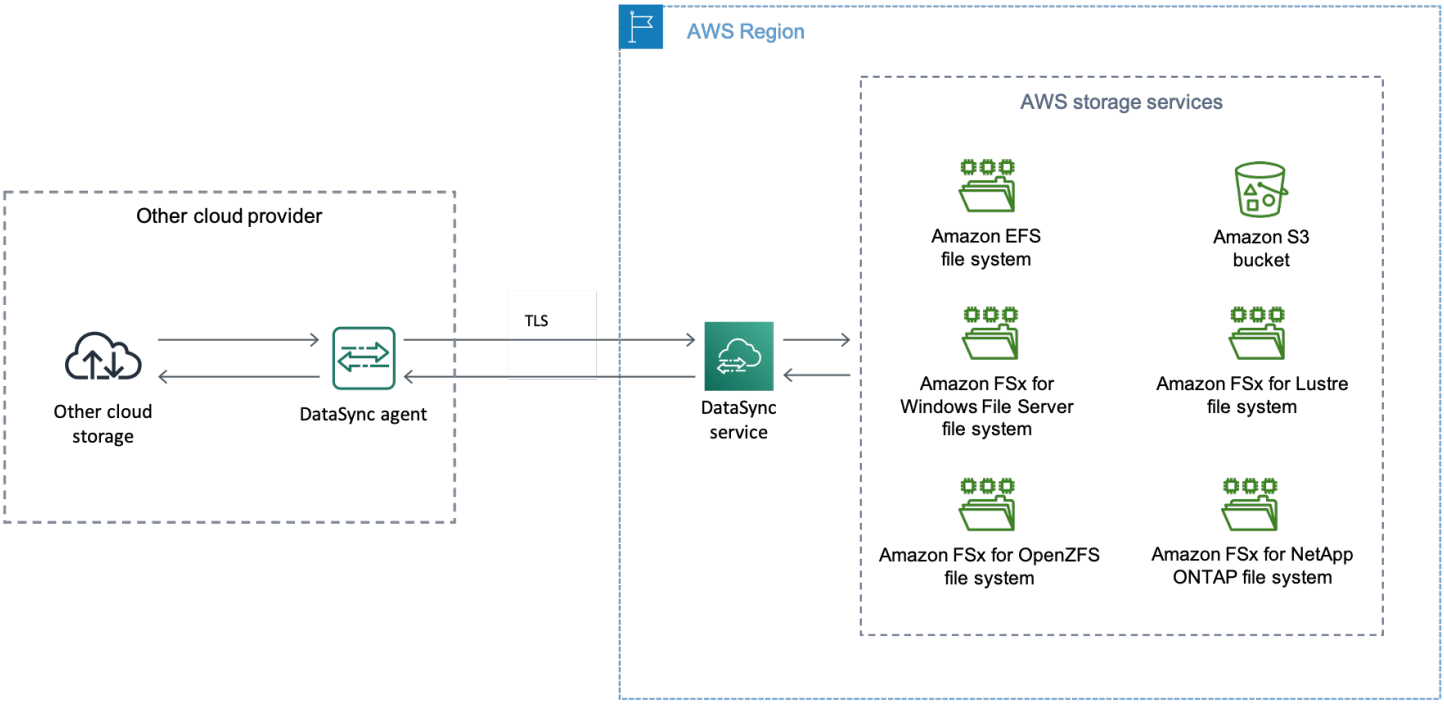
Transfert entre les services AWS de stockage et les systèmes de stockage dans d'autres clouds

Avec DataSync, vous pouvez transférer des données entre d'autres systèmes de stockage cloud et Services AWS. Dans ce contexte, les systèmes de stockage dans le cloud peuvent inclure :

- Systèmes de stockage autogérés, tels qu'un serveur de fichiers NFS dans votre cloud privé virtuel (VPC) intégré. AWS
- Systèmes ou services de stockage hébergés par un autre fournisseur de cloud. Pour de plus amples informations, veuillez consulter Transfert vers ou depuis un autre stockage dans le cloud avec AWS DataSync.

DataSync peut copier des données vers et depuis d'autres clouds avec ou sans l'aide d'un agent. Pour plus d'informations sur les circonstances dans lesquelles utiliser un agent, voir Ai-je besoin d'un AWS DataSync agent ? .

Le schéma suivant présente un aperçu général du DataSync transfert de données entre les services AWS de stockage et un autre fournisseur de cloud.



Concepts et terminologie

Familiarisez-vous avec les fonctionnalités DataSync de transfert.

Rubriques

- Agent
- Emplacement
- Tâche
- Exécution des tâches

Agent

Un agent est une appliance de machine virtuelle (VM) qui permet DataSync de lire et d'écrire dans le stockage lors d'un transfert.

Vous pouvez déployer un agent dans votre environnement de stockage sur VMware ESXi une machine virtuelle basée sur le noyau Linux (KVM) ou des hyperviseurs Microsoft Hyper-V. Pour le stockage dans un cloud privé virtuel (VPC) dans AWS, vous pouvez déployer un agent en tant qu'instance Amazon EC2.

Pour commencer, voir Ai-je besoin d'un AWS DataSync agent ?

Emplacement

Un emplacement décrit l'endroit depuis ou vers lequel vous copiez les données. Chaque DataSync transfert (également appelé tâche) possède un emplacement source et un emplacement de destination. Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.

Tâche

Une tâche décrit un DataSync transfert. Il identifie un emplacement source et un emplacement de destination ainsi que des détails sur la façon de copier des données entre ces emplacements. Vous pouvez également définir la manière dont une tâche gère les métadonnées, les fichiers supprimés et les autorisations.

Exécution des tâches

L'exécution d'une tâche est l'exécution individuelle d'une tâche de DataSync transfert. L'exécution d'une tâche comporte plusieurs phases. Pour de plus amples informations, veuillez consulter Statuts d'exécution des tâches.

Comment DataSync transférer des fichiers, des objets et des répertoires

Lors de l'exécution d'une tâche, DataSync prépare, transfère et vérifie vos données. DataSync Le mode d'exécution de ces actions dépend de la façon dont vous configurez les options de vos DataSync tâches, telles que le mode tâche. Les tâches en mode de base préparent, transfèrent et vérifient vos données de manière séquentielle, tandis que les tâches en mode amélioré les effectuent en parallèle.

Rubriques

- Comment DataSync prépare votre transfert de données
- Comment DataSync transfèrent vos données
- Comment DataSync vérifie l'intégrité de vos données
- Comment DataSync fonctionne avec les fichiers ouverts et verrouillés
- Options de transfert récurrentes

Comment DataSync prépare votre transfert de données

DataSync prépare par défaut votre transfert en examinant vos emplacements source et de destination afin de déterminer ce que vous souhaitez transférer. Cela se fait en scannant le contenu et les métadonnées des deux emplacements afin d'identifier les différences entre les deux.

> **Note**
>
> Si vous configurez votre tâche pour transférer toutes les données, il n'y a aucune préparation. Lorsque vous commencez votre tâche, transférez DataSync immédiatement tout de votre source à votre destination sans comparer les emplacements.

La façon DataSync dont vous préparez votre transfert dépend également de votre mode de tâche :

Préparation améliorée du mode	Préparation du mode de base
DataSync prépare les objets tels qu'ils se trouvent à l'emplacement source. La préparati on se poursuit tout au long de l'exécution de la tâche jusqu'à ce qu'aucun autre objet ne soit répertorié à la source. Contrairement au mode de base, il DataSync permet de préparer un nombre pratiquement illimité d'objets à chaque exécution de tâche.	La préparation peut prendre quelques minutes, quelques heures, voire plus, en fonction du nombre de fichiers, d'objets ou de répertoires présents dans les deux emplacements et des performances de votre stockage. Les articles DataSync inventoriés dans votre source et votre destination sont pris en compte dans vos quotas de tâches. Ces quotas ne sont pas basés sur le nombre d'éléments DataSync transférés lors de chaque exécution de tâche.

DataSync certains fichiers, objets et répertoires peuvent être ignorés lors de la préparation. Cela peut être dû à plusieurs facteurs, tels que la manière dont vous configurez vos tâches et les autorisations du système de stockage. Voici quelques exemples :

- Un fichier existe dans vos emplacements source et de destination. Le fichier de la source n'a pas été modifié depuis l'exécution précédente de la tâche. Comme vous ne transférez que des données modifiées, ce fichier DataSync ne sera pas transféré la prochaine fois que vous exécuterez votre tâche.

- Un objet qui existe dans vos deux emplacements change dans votre source. Lorsque vous exécutez votre tâche, cet objet DataSync est ignoré dans votre destination car votre tâche ne remplace pas les données dans la destination.
- DataSync ignore un objet de votre emplacement source qui utilise une classe de stockage d'archivage et qui n'est pas restauré. Vous devez restaurer un objet archivé DataSync pour pouvoir le lire.
- DataSync ignore un fichier, un objet ou un répertoire dans votre emplacement source car il ne peut pas le lire. Si cela se produit et n'est pas prévu, vérifiez les autorisations d'accès de votre espace de stockage et assurez-vous qu'il DataSync peut lire ce qui a été ignoré.

Comment DataSync transfèrent vos données

DataSync copie vos données (y compris les métadonnées) de la source vers la destination en fonction des options de vos tâches. Par exemple, vous pouvez spécifier les métadonnées à copier, exclure certains fichiers et limiter la consommation de bande DataSync passante, entre autres options.

Le mode de DataSync transfert de vos données dépend également de votre mode de tâche :

Transfert de mode amélioré	Transfert en mode de base
DataSync transfère chaque objet dès qu'il est préparé.	Une DataSync fois toutes vos données préparées, le transfert commence.

DataSynccertains éléments peuvent être ignorés lors du transfert. Si vous configurez votre tâche pour transférer toutes les données, cela peut se produire avec un objet de votre emplacement source qui utilise une classe de stockage d'archivage et qui n'est pas restauré.

Comment DataSync vérifie l'intégrité de vos données

DataSync effectue toujours des contrôles d'intégrité de vos données lors d'un transfert. À la fin d'un transfert, DataSync vous pouvez également effectuer des vérifications supplémentaires uniquement sur les données transférées ou sur l'ensemble de données aux deux emplacements. Pour de plus amples informations, veuillez consulter Configuration du mode de AWS DataSync vérification de l'intégrité des données.

Lors de la vérification de l'intégrité des données, DataSync calcule et compare la somme de contrôle et les métadonnées des fichiers, objets ou répertoires situés dans vos emplacements. Si vous DataSync constatez des différences entre les emplacements, la vérification échoue avec une erreur. Par exemple, vous pouvez voir des erreurs telles que `Checksum failure``Metadata failure`,`Files were added`, ou`Files were removed`.

Le fonctionnement de la vérification dépend de votre mode de tâche et de votre configuration DataSync pour vérifier l'intégrité des données à la fin du transfert.

Vérification du mode améliorée	Vérification du mode de base
DataSync vérifie chaque objet lorsqu'il est transféré vers votre destination. Avec le mode amélioré, DataSync vérifie uniquement les données transférées.	À la fin de votre transfert, DataSync vérifie l'intégrité de vos données. Selon la façon dont vous configurez la vérification des données, cela peut prendre beaucoup de temps pour les grands ensembles de données.

Comment DataSync fonctionne avec les fichiers ouverts et verrouillés

Tenez compte des points suivants lorsque vous essayez de transférer des fichiers ouverts (en cours d'utilisation) ou verrouillés :

- En général, DataSync peut transférer des fichiers ouverts sans aucune limitation.
- Si un fichier est ouvert et est en cours d'écriture pendant un transfert, DataSync vous pouvez détecter ce type d'incohérence lors de la phase de vérification de la tâche de transfert. Pour obtenir la dernière version du fichier, vous devez exécuter à nouveau la tâche.
- Si un fichier est verrouillé et que le serveur DataSync empêche son ouverture, il DataSync ignore le fichier pendant le transfert et enregistre une erreur.
- DataSync Impossible de verrouiller ou de déverrouiller des fichiers.

Options de transfert récurrentes

Outre les transferts ponctuels, DataSync vous pouvez transférer des données de manière récurrente. Voici certaines des options disponibles pour ces situations :

- Planification de l'exécution de votre tâche.
- Transférer uniquement les données modifiées depuis l'exécution de la tâche précédente.
- Suppression de données dans l'emplacement de destination qui ne sont plus présentes dans la source.

Commencer avec AWS DataSync

Avant de commencer AWS DataSync, vous devez vous inscrire à un Compte AWS si vous n'en avez pas. Nous vous recommandons également de savoir où vous DataSync pouvez les utiliser et combien cela peut coûter pour transférer vos données.

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 .

Autorisations IAM requises pour utiliser DataSync

DataSync peut transférer vos données vers un compartiment Amazon S3, un système de fichiers Amazon EFS ou un certain nombre d'autres services de AWS stockage. Pour acheminer vos données là où vous le souhaitez, vous devez disposer des autorisations IAM appropriées associées à votre identité. Par exemple, le rôle IAM que vous utilisez DataSync doit être autorisé à utiliser les opérations Amazon S3 requises pour transférer des données vers un compartiment S3.

Vous pouvez accorder ces autorisations à l'aide des politiques IAM fournies par AWS ou en créant vos propres politiques.

Table des matières

- AWS politiques gérées
- Politiques gérées par le client

AWS politiques gérées

AWS fournit les politiques gérées suivantes pour les cas DataSync d'utilisation courants :

- `AWSDataSyncReadOnlyAccess`— Fournit un accès en lecture seule à. DataSync
- `AWSDataSyncFullAccess`— Fournit un accès complet DataSync et un accès minimal à ses dépendances.

Pour de plus amples informations, veuillez consulter AWS politiques gérées pour AWS DataSync.

Politiques gérées par le client

Vous pouvez créer des politiques IAM personnalisées à utiliser avec DataSync. Pour de plus amples informations, veuillez consulter Politiques gérées par le client IAM pour AWS DataSync.

Où puis-je l'utiliser DataSync ?

Pour obtenir la liste des points Régions AWS de terminaison compatibles, consultez DataSync la section AWS DataSync Points de terminaison et quotas dans le. Références générales AWS

Comment puis-je l'utiliser DataSync ?

Il existe plusieurs manières d'utiliser DataSync :

- DataSync console, qui fait partie du AWS Management Console.
- DataSync API ou AWS CLIpour configurer et gérer par programmation. DataSync
- AWS CloudFormationou Terraform pour approvisionner vos ressources. DataSync
- AWS SDKspour créer des applications qui utilisent DataSync.

Combien va DataSync coûter ?

Sur la page de DataSync tarification, créez une estimation personnalisée en fonction de la quantité de données que vous prévoyez de transférer.

Composants open source utilisés par DataSync

Pour voir les composants open source utilisés par DataSync, téléchargez le lien suivant :

- datasync-open-source-components.zip

Ai-je besoin d'un AWS DataSync agent ?

Pour l'utiliser AWS DataSync, vous aurez peut-être besoin d'un agent. Un agent est une appliance de machine virtuelle (VM) que vous déployez dans votre environnement de stockage pour les transferts de données.

La question de savoir si vous avez besoin d'un agent dépend de plusieurs facteurs, notamment le type de stockage vers ou depuis lequel vous effectuez le transfert, si vous effectuez un transfert de l' Comptes AWS un à l'autre et entre lequel Régions AWS vous effectuez le transfert. Avant de poursuivre votre lecture, vérifiez que le transfert qui vous intéresse est DataSync compatible.

Après avoir déterminé ce qui DataSync convient à votre scénario de transfert, consultez les informations suivantes pour savoir si vous avez besoin d'un agent.

Situations dans lesquelles vous avez besoin d'un DataSync agent

La plupart des situations nécessitant un DataSync agent impliquent un stockage géré par vous ou par un autre fournisseur de cloud.

- Transfert entre les services AWS de stockage et le stockage sur site
- Transfert entre Amazon EFS ou Amazon FSx et le stockage dans d'autres clouds
- Transfert vers ou depuis un stockage périphérique
- Transfert entre certains services AWS de stockage Comptes AWS (lorsqu'aucun des services de stockage n'est Amazon S3)

  Pour de plus amples informations, veuillez consulter Transferts pris en charge entre Comptes AWS.
- Transfert entre une publicité Région AWS et une entreprise AWS GovCloud (US) dont la source et la destination sont Amazon EFS ou Amazon FSx.

Situations dans lesquelles vous n'avez pas besoin d'un DataSync agent

Les situations qui ne nécessitent pas l'intervention d'un agent s'appliquent, que vous effectuiez un transfert dans la même région Région AWS ou dans une autre région.

- Transfert d'un service AWS de stockage à un autre au sein d'un même service Compte AWS
- Transfert entre Amazon S3 et un autre service de AWS stockage Comptes AWS
- Transfert entre Amazon S3 et le stockage d'objets dans d'autres clouds
- Transfert entre une publicité Région AWS et une AWS GovCloud (US) entreprise dont la source ou la destination est Amazon S3

Utilisation de plusieurs DataSync agents

Bien que la plupart des transferts ne nécessitent qu'un seul agent, l'utilisation de plusieurs agents peut accélérer les transferts de grands ensembles de données contenant des millions de fichiers ou d'objets. Dans ces situations, nous recommandons d'exécuter les tâches de transfert en parallèle. Cette approche répartit la charge de travail de transfert entre plusieurs tâches, chaque tâche utilisant son propre agent. Cela permet également de réduire le temps nécessaire DataSync à la préparation et au transfert de vos données. Pour de plus amples informations, veuillez consulter Partitionnement de grands ensembles de données avec plusieurs tâches.

Une autre option, en particulier si vous avez des millions de petits fichiers, consiste à utiliser plusieurs agents dotés d'un même lieu de transfert. Par exemple, vous pouvez connecter jusqu'à quatre agents à votre service de fichiers NFS (Network File System) local. Cette option peut accélérer votre transfert, bien que le temps nécessaire DataSync à sa préparation ne change pas.

Quelle que soit l'approche, sachez que celles-ci peuvent augmenter les opérations d'E/S sur votre stockage et affecter la bande passante de votre réseau. Pour plus d'informations sur l'utilisation de plusieurs agents pour vos DataSync transferts, consultez le blog sur le AWS stockage.

Si vous envisagez d'utiliser plusieurs agents, n'oubliez pas ce qui suit :

- L'utilisation de plusieurs agents sur un même site ne garantit pas une haute disponibilité. Tous les agents associés à un point de vente doivent être en ligne pour que vous puissiez commencer votre tâche de transfert. Si l'un des agents est hors ligne, vous ne pouvez pas exécuter votre tâche.
- Si vous utilisez un point de terminaison de service de cloud privé virtuel (VPC) pour communiquer avec le DataSync service, tous les agents doivent utiliser le même point de terminaison et le même sous-réseau.

Étapes suivantes

- Si vous avez besoin d'un agent, passez en revue les exigences relatives à l'agent afin de comprendre ce qui convient à votre environnement de stockage.
- Si vous n'avez pas besoin d'un agent pour votre transfert, vous pouvez commencer à le configurer.

Exigences pour les AWS DataSync agents

Avant de déployer un AWS DataSync agent dans votre environnement de stockage, assurez-vous de bien comprendre l'hyperviseur de l'agent et les besoins en ressources.

Exigences relatives à l'hyperviseur

Vous pouvez exécuter un DataSync agent sur les hyperviseurs suivants :

- VMware ESXi (version 6.5, 6.7, 7.0 ou 8.0) : VMware ESXi est disponible sur le site Web de Broadcom. Vous avez également besoin d'un client VMware vSphere pour vous connecter à l'hôte.
- Machine virtuelle basée sur le noyau Linux (KVM) : technologie de virtualisation open source gratuite. KVM est inclus dans les versions 2.6.20 et ultérieures de Linux. DataSync est testé et pris en charge pour les distributions CentOS/RHEL 7 et 8, Ubuntu 16.04 LTS et Ubuntu 18.04 LTS. Une autre distribution Linux moderne peut fonctionner, mais le fonctionnement ou les performances ne sont pas garantis. Vous devez activer la virtualisation accélérée par le matériel sur votre hôte KVM pour déployer votre DataSync agent.

  Nous recommandons cette option si vous disposez déjà d'un environnement KVM et que vous connaissez déjà le fonctionnement du KVM.

  L'exécution de KVM sur Amazon EC2 n'est pas prise en charge et ne peut pas être utilisée pour les DataSync agents.
- Microsoft Hyper-V (version 2012 R2, 2016 ou 2019) : pour cette configuration, vous avez besoin d'un gestionnaire Microsoft Hyper-V sur un ordinateur client Microsoft Windows pour vous connecter à l'hôte.

  L' DataSync agent est une machine virtuelle (VM) de génération 1. Pour plus d'informations sur les différences entre la génération 1 et la génération 2 VMs, voir Dois-je créer une machine virtuelle de génération 1 ou 2 dans Hyper-V ?
- Amazon EC2 : DataSync fournit une Amazon Machine Image (AMI) qui contient l' DataSync image. Pour obtenir les types d'instances recommandés, consultez Exigences relatives aux EC2 instances Amazon.

Exigences relatives aux agents pour les DataSync transferts

Pour les DataSync transferts, votre agent doit répondre aux exigences en matière de ressources suivantes.

> **Important**
>
> N'oubliez pas que les exigences des agents pour travailler avec jusqu'à 20 millions de fichiers, d'objets ou de répertoires sont des directives générales. Votre agent peut avoir besoin de ressources supplémentaires en raison d'autres facteurs, tels que le nombre de répertoires dont vous disposez et la taille des métadonnées des objets. Par exemple, l'instance m5.2xlarge d'un EC2 agent Amazon peut toujours ne pas être suffisante pour un transfert de moins de 20 millions de fichiers.

Table des matières

- Exigences relatives aux machines virtuelles
- Exigences relatives aux EC2 instances Amazon

Exigences relatives aux machines virtuelles

Lors du déploiement d'un DataSync agent qui ne se trouve pas sur une EC2 instance Amazon, la machine virtuelle de l'agent a besoin des ressources suivantes :

- Processeurs virtuels : quatre processeurs virtuels assignés à la machine virtuelle.
- Espace disque : 80 Go d'espace disque pour l'installation de l'image de la machine virtuelle et des données système.
- RAM : en fonction de votre scénario de transfert, vous avez besoin de la quantité de mémoire suivante :
  - 32 Go de RAM affectés à la machine virtuelle pour exécuter des tâches avec jusqu'à 20 millions de fichiers, d'objets ou de répertoires.
  - 64 Go de RAM affectés à la machine virtuelle pour exécuter des tâches avec plus de 20 millions de fichiers, d'objets ou de répertoires.

Exigences relatives aux EC2 instances Amazon

Lors du déploiement d'un DataSync agent sur une EC2 instance Amazon, la taille de l'instance doit être d'au moins 2 fois plus grande.

Nous vous recommandons d'utiliser l'une des tailles d'instance suivantes :

- m5.2xlarge : pour les exécutions de tâches impliquant jusqu'à 20 millions de fichiers, d'objets ou de répertoires.
- m5.4xlarge : pour les exécutions de tâches impliquant plus de 20 millions de fichiers, d'objets ou de répertoires.

Exigences relatives aux agents pour les Région AWS partitions

DataSync les images de l'agent sont associées à des Région AWS partitions spécifiques. Par exemple, par défaut, vous ne pouvez pas télécharger un agent dans une publicité Région AWS puis l'activer dans un AWS GovCloud (US) Region.

Exigences relatives à la gestion des agents

Une fois que vous avez activé votre DataSync agent, il le AWS gère pour vous. Pour de plus amples informations, veuillez consulter Gérer votre AWS DataSync agent.

Déploiement de votre AWS DataSync agent

Lors de la création d'un AWS DataSync agent, la première étape consiste à le déployer dans votre environnement de stockage. Vous pouvez déployer un agent sous forme de machine virtuelle (VM) VMware ESXi, de machine virtuelle basée sur le noyau Linux (KVM) et d'hyperviseurs Microsoft Hyper-V. Vous pouvez également déployer un agent en tant qu' EC2 instance Amazon dans un cloud privé virtuel (VPC) intégré. AWS

> **Tip**
>
> Avant de commencer, vérifiez si vous avez besoin d'un DataSync agent.

Déploiement de votre agent sur VMware

Vous pouvez télécharger un agent depuis la DataSync console et le déployer dans votre VMware environnement.

Avant de commencer : assurez-vous que votre environnement de stockage peut prendre en charge un DataSync agent. Pour de plus amples informations, veuillez consulter Exigences relatives aux machines virtuelles.

Pour déployer un agent sur VMware

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Agents, puis Create agent.
3. Pour Hypervisor, choisissez VMWare ESXi, puis choisissez Télécharger l'image.

   L'agent télécharge dans un `.zip` fichier contenant un fichier `.ova` image.
4. Pour minimiser la latence du réseau, déployez l'agent le plus près possible du système de stockage DataSync auquel vous souhaitez accéder (le même réseau local si possible). Pour de plus amples informations, veuillez consulter Exigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie.

   Si nécessaire, consultez la documentation de votre hyperviseur pour savoir comment déployer un `.ova` fichier sur un VMware hôte.
5. Allumez votre hyperviseur, connectez-vous à la machine virtuelle de l'agent et obtenez l'adresse IP de l'agent. Vous avez besoin de cette adresse IP pour activer l'agent.

   Les informations d'identification par défaut de la machine virtuelle de l'agent sont le login **`admin`** et le mot de passe**`password`**. Si nécessaire, modifiez le mot de passe via la console locale de la machine virtuelle.

Étape suivante : Choisir un point de terminaison de service pour votre AWS DataSync agent

Déploiement de votre agent sur KVM

Vous pouvez télécharger un agent depuis la DataSync console et le déployer dans votre environnement KVM.

Avant de commencer : assurez-vous que votre environnement de stockage peut prendre en charge un DataSync agent. Pour de plus amples informations, veuillez consulter Exigences relatives aux machines virtuelles.

Pour déployer un agent sur KVM

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Agents, puis Create agent.
3. Pour Hypervisor, choisissez KVM (Kernel-based Virtual Machine), puis sélectionnez Télécharger l'image.

L'agent télécharge dans un `.zip` fichier contenant un fichier `.qcow2` image.

4. Pour minimiser la latence du réseau, déployez l'agent le plus près possible du système de stockage DataSync auquel vous souhaitez accéder (le même réseau local si possible). Pour de plus amples informations, veuillez consulter Exigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie.
5. Exécutez la commande suivante pour installer votre `.qcow2` image.

```
virt-install \
    --name "datasync" \
    --description "DataSync agent" \
    --os-type=generic \
    --ram=32768 \
    --vcpus=4 \
    --disk path=datasync-yyyymmdd-x86_64.qcow2,bus=virtio,size=80 \
    --network default,model=virtio \
    --graphics none \
    --virt-type kvm \
    --import
```

   Pour plus d'informations sur la gestion de cette machine virtuelle et de votre hôte KVM, consultez la documentation de votre hyperviseur.

6. Mettez votre hyperviseur sous tension, connectez-vous à votre ordinateur virtuel, et obtenez l'adresse IP de l'agent. Vous avez besoin de cette adresse IP pour activer l'agent.

   Les informations d'identification par défaut de la machine virtuelle de l'agent sont le login **`admin`** et le mot de passe**`password`**. Si nécessaire, modifiez le mot de passe via la console locale de la machine virtuelle.

Étape suivante : Choisir un point de terminaison de service pour votre AWS DataSync agent

Déploiement de votre agent sur Microsoft Hyper-V

Vous pouvez télécharger un agent depuis la DataSync console et le déployer dans votre environnement Microsoft Hyper-V.

Avant de commencer : assurez-vous que votre environnement de stockage peut prendre en charge un DataSync agent. Pour de plus amples informations, veuillez consulter Exigences relatives aux machines virtuelles.

Pour déployer un agent sur Hyper-V

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Agents, puis Create agent.
3. Pour Hypervisor, choisissez Microsoft Hyper-V, puis choisissez Télécharger l'image.

   L'agent télécharge dans un `.zip` fichier contenant un fichier `.vhdx` image.
4. Pour minimiser la latence du réseau, déployez l'agent le plus près possible du système de stockage DataSync auquel vous souhaitez accéder (le même réseau local si possible). Pour de plus amples informations, veuillez consulter Exigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie.

   Si nécessaire, consultez la documentation de votre hyperviseur pour savoir comment déployer un `.vhdx` fichier sur un hôte Hyper-V.

   > **Warning**
   >
   > Vous remarquerez peut-être de mauvaises performances réseau si vous activez la file d'attente des machines virtuelles (VMQ) sur un hôte Hyper-V utilisant un adaptateur réseau Broadcom. Pour plus d'informations sur une solution de contournement, consultez la documentation Microsoft.
5. Mettez votre hyperviseur sous tension, connectez-vous à votre ordinateur virtuel, et obtenez l'adresse IP de l'agent. Vous avez besoin de cette adresse IP pour activer l'agent.

   Les informations d'identification par défaut de la machine virtuelle de l'agent sont le login **`admin`** et le mot de passe**`password`**. Si nécessaire, modifiez le mot de passe via la console locale de la machine virtuelle.

Étape suivante : Choisir un point de terminaison de service pour votre AWS DataSync agent

Déploiement de votre EC2 agent Amazon

Vous pouvez déployer un DataSync agent en tant qu' EC2 instance Amazon lors du transfert de données entre :

- Un système de stockage cloud autogéré (par exemple, un serveur de fichiers NFS intégré AWS) et un service AWS de stockage.

- Un fournisseur de stockage dans le cloud (tel que Microsoft Azure Blob Storage ou Google Cloud Storage) et un service AWS de stockage.
- Un compartiment S3 dans une publicité Région AWS et un compartiment S3 dans un AWS GovCloud (US) Region.
- Amazon S3 activé AWS Outposts et un service AWS de stockage.

> **Warning**
>
> Nous vous déconseillons d'utiliser un EC2 agent Amazon avec un stockage sur site en raison de l'augmentation de la latence du réseau. Déployez plutôt l'agent sous forme de machine virtuelle KVM ou Hyper-V dans votre centre de données le plus près possible de votre stockage sur site. VMware

Déploiement de votre EC2 agent

Pour choisir l'AMI d'agent pour votre Région AWS

1. Ouvrez un terminal et copiez la AWS CLI commande suivante pour obtenir le dernier identifiant DataSync Amazon Machine Image (AMI) pour la région dans laquelle vous souhaitez déployer votre EC2 agent Amazon.

```
aws ssm get-parameter --name /aws/service/datasync/ami --region your-region
```

2. Exécutez la commande . Dans la sortie, notez la `"Value"` propriété avec l'ID DataSync AMI.

   Example Exemple de commande et de sortie

```
aws ssm get-parameter --name /aws/service/datasync/ami --region us-east-1


{
    "Parameter": {
        "Name": "/aws/service/datasync/ami",
        "Type": "String",
        "Value": "ami-1234567890abcdef0",
        "Version": 6,
        "LastModifiedDate": 1569946277.996,
        "ARN": "arn:aws:ssm:us-east-1::parameter/aws/service/datasync/ami"
```

```
    }
}
```

Pour déployer votre EC2 agent Amazon

> **Tip**
>
> Pour éviter les frais liés au transfert entre les zones de disponibilité, déployez votre agent de manière à ne pas nécessiter de trafic réseau entre les zones de disponibilité. (Pour en savoir plus sur les tarifs de transfert de données pour tous Régions AWS, consultez les tarifs d'Amazon EC2 Data Transfer.)
> Par exemple, déployez votre agent dans la zone de disponibilité où se trouve votre système de stockage cloud autogéré.

1. Copiez l'URL suivante :

   ```
   https://console.aws.amazon.com/ec2/v2/home?region=agent-region#LaunchInstanceWizard:ami=ami-id
   ```

   - Remplacez *agent-region* par la région dans laquelle vous souhaitez déployer votre agent.
   - *ami-id*Remplacez-le par l'ID d' DataSync AMI que vous avez obtenu.
2. Collez l'URL dans un navigateur.

   La page de lancement de l' EC2 instance Amazon s' AWS Management Console affiche.
3. Pour le type d'instance, choisissez l'une des EC2 instances Amazon recommandées pour DataSync.
4. Pour Key pair, choisissez une paire de clés existante ou créez-en une nouvelle.
5. Pour les paramètres réseau, choisissez Modifier, puis procédez comme suit :

   a. Pour le VPC, choisissez un VPC sur lequel vous souhaitez déployer votre agent.

   b. Pour Attribuer automatiquement une adresse IP publique, indiquez si vous souhaitez que votre agent soit accessible depuis l'Internet public.

      Vous utiliserez l'adresse IP publique ou privée de l'instance ultérieurement pour activer votre agent.

c. Pour le pare-feu (groupes de sécurité), créez ou sélectionnez un groupe de sécurité qui effectue les opérations suivantes :

- Si nécessaire, autorise le trafic entrant vers l' EC2instance Amazon sur le port 80 (HTTP). Certaines options permettant d'obtenir une clé d'activation d'agent nécessitent cette connexion.
- Autorise le trafic entrant et sortant entre l' EC2 instance Amazon et le système de stockage vers lequel vous transférez des données ou à partir duquel vous transférez des données. Pour de plus amples informations, veuillez consulter Exigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie.

> **Note**
>
> Il existe des ports supplémentaires à configurer en fonction du type de point de terminaison de service utilisé par votre agent.

6. (Recommandé) Pour améliorer les performances lors du transfert depuis un système de fichiers basé sur le cloud, développez les détails avancés et choisissez une valeur de groupe de placement dans laquelle se trouve votre stockage.
7. Choisissez Launch instance pour lancer votre EC2 instance Amazon.
8. Une fois que le statut de votre instance est En cours d'exécution, choisissez l'instance.
9. Si vous avez configuré votre instance pour qu'elle soit accessible depuis l'Internet public, prenez note de l'adresse IP publique de l'instance. Si ce n'est pas le cas, notez l'adresse IP privée.

   Vous avez besoin de cette adresse IP pour activer votre agent.

Exemples : déploiement de votre EC2 agent dans un Région AWS

Les conseils suivants peuvent vous aider à résoudre les scénarios courants si vous déployez un DataSync agent dans un Région AWS.

Rubriques

- Déploiement de votre agent pour les transferts entre le stockage dans le cloud et les services AWS de stockage
- Déploiement de votre agent pour les transferts entre Amazon S3 et les systèmes de AWS fichiers

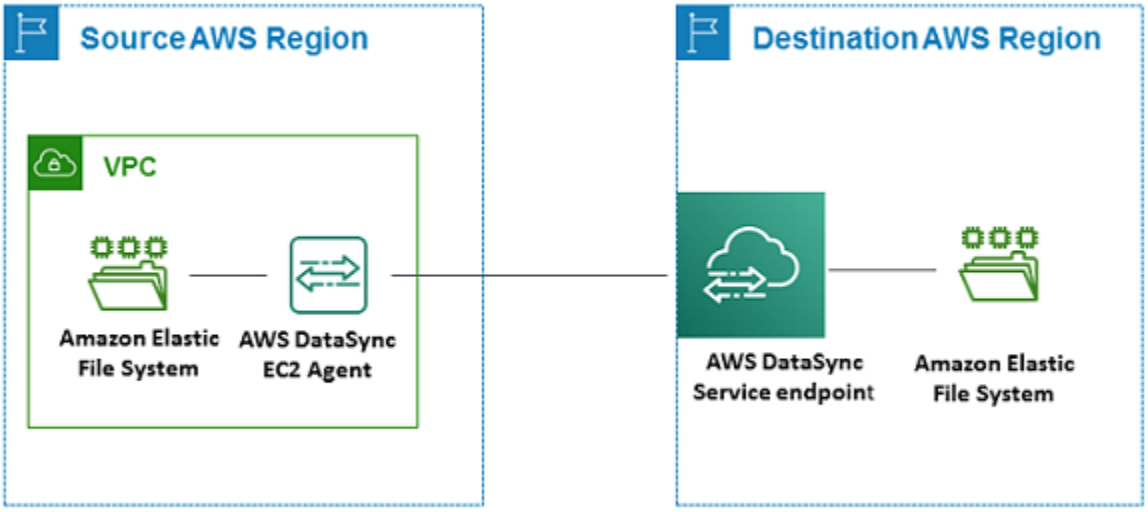
Déploiement de votre agent pour les transferts entre le stockage dans le cloud et les services AWS de stockage

Pour transférer des données entre Comptes AWS ou entre des systèmes de stockage dans le cloud, l' DataSync agent doit se trouver dans le même Région AWS et Compte AWS là où réside le système de fichiers source. Ce type de transfert inclut les éléments suivants :

- Transferts entre Amazon EFS ou Amazon FSx vers un AWS stockage dans un autre Compte AWS
- Transferts de systèmes de fichiers autogérés vers des services AWS de stockage.

> **Important**
>
> Déployez votre agent de telle sorte qu'il n'ait pas besoin de trafic réseau entre les zones de disponibilité (afin d'éviter les frais liés à ce trafic).
>
> - Pour accéder à votre système de fichiers Amazon EFS ou FSx Windows File Server, déployez l'agent dans une zone de disponibilité dotée d'une cible de montage sur votre système de fichiers.
> - Pour les systèmes de fichiers autogérés, déployez l'agent dans la zone de disponibilité où se trouve votre système de fichiers.
>
> Pour en savoir plus sur les tarifs de transfert de données pour tous Régions AWS, consultez les tarifs Amazon EC2 On-Demand.

Par exemple, le schéma suivant montre une vue de haut niveau de l' DataSync architecture permettant de transférer des données du système de fichiers réseau (NFS) dans le cloud vers le cloud NFS ou Amazon S3.

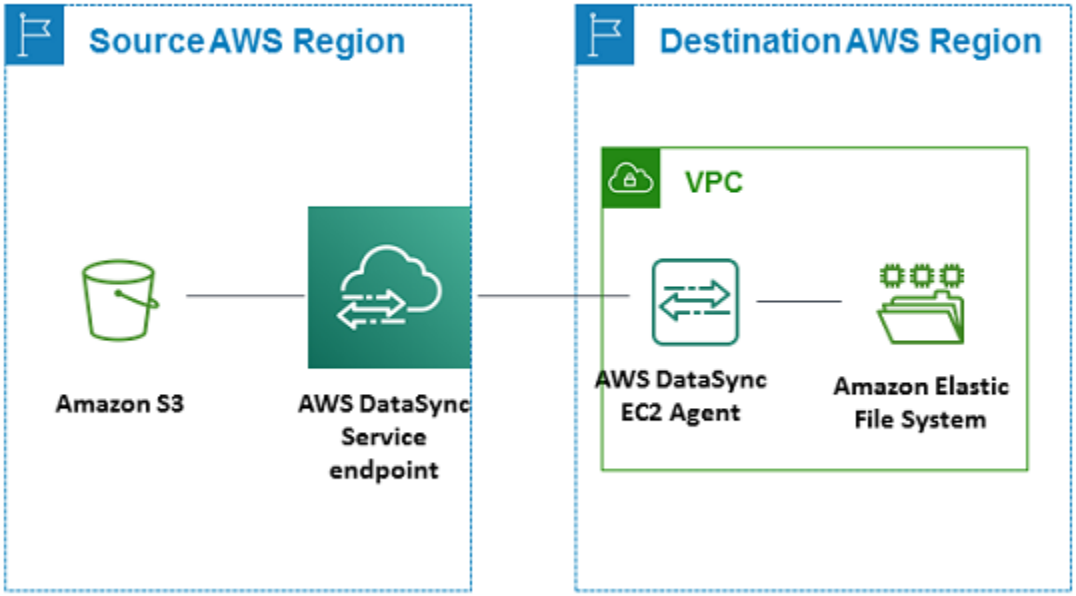


N'oubliez pas les points suivants lors du transfert entre les services AWS de stockage Comptes AWS :

- Lorsque vous effectuez un transfert entre des systèmes de fichiers Amazon EFS ou des systèmes de FSx fichiers Amazon à l'aide du protocole NFS, configurez votre système de fichiers source en tant qu'emplacement NFS.
- Lorsque vous effectuez un transfert entre des systèmes de FSx fichiers Amazon à l'aide du protocole SMB, configurez votre système de fichiers source en tant qu'emplacement SMB.

Déploiement de votre agent pour les transferts entre Amazon S3 et les systèmes de AWS fichiers

Le schéma suivant fournit une vue détaillée de l' DataSyncarchitecture permettant de transférer des données d'Amazon S3 vers un système de AWS fichiers, tel qu'Amazon EFS ou Amazon FSx. Vous pouvez utiliser cette architecture pour transférer des données de l'un Compte AWS à l'autre, ou pour transférer des données d'Amazon S3 vers un système de fichiers dans le cloud autogéré.



Déploiement de votre agent sur AWS Snowball Edge

Pour plus d'informations et d'instructions, consultez la section Création d'un DataSync agent dans votre environnement de stockage sur site relative au stockage compatible avec Amazon S3.

Déploiement de votre agent sur AWS Outposts

Vous pouvez lancer une EC2 instance DataSync Amazon sur votre Outpost. Pour en savoir plus sur le lancement d'une AMI sur AWS Outposts, consultez la section Lancer une instance sur votre Outpost dans le guide de l'AWS Outposts utilisateur.

Lorsque vous l'utilisez DataSync pour accéder à Amazon S3 sur Outposts, vous devez lancer l'agent dans un VPC autorisé à accéder à votre point d'accès Amazon S3 et activer l'agent dans la région parent de l'Outpost. L'agent doit également être en mesure d'acheminer le bucket vers le point de terminaison Amazon S3 on Outposts. Pour en savoir plus sur l'utilisation d'Amazon S3 sur les points de terminaison d'Outposts, consultez la section Utilisation d'Amazon S3 sur les Outposts dans le guide de l'utilisateur d'Amazon S3.

Choisir un point de terminaison de service pour votre AWS DataSync agent

Un point de terminaison de service est la façon dont votre AWS DataSync agent communique avec le DataSync service. DataSync prend en charge les types de points de terminaison de service suivants :

- Point de terminaison du service public — Les données sont envoyées via l'Internet public.
- Point de terminaison du service FIPS (Federal Information Processing Standard) : les données sont envoyées via l'Internet public à l'aide de processus conformes à la norme FIPS.
- Point de terminaison du service de cloud privé virtuel (VPC) : les données sont envoyées via votre VPC plutôt que via Internet public, ce qui renforce la sécurité des données transférées.

Vous avez besoin d'un point de terminaison de service pour activer votre agent. Lorsque vous choisissez un point de terminaison de service, n'oubliez pas les points suivants :

- Un agent ne peut utiliser qu'un seul type de point de terminaison. Si vous devez transférer des données à l'aide de différents types de terminaux, créez un agent pour chaque type.
- La manière dont vous connectez votre réseau de stockage AWS détermine les points de terminaison de service que vous pouvez utiliser.

Choisir un point de terminaison de service public

Si vous utilisez un point de terminaison de service public, toutes les communications entre votre DataSync agent et le DataSync service se font via l'Internet public.

1. Déterminez le point de terminaison de service DataSync public que vous souhaitez utiliser.
2. Configurez votre réseau pour autoriser le trafic nécessaire à l'utilisation des points de terminaison du service DataSync public.

Étape suivante : Activation de votre AWS DataSync agent

Choix d'un point de terminaison de service FIPS

DataSync fournit certains points de terminaison de service conformes à la norme FIPS. Pour plus d'informations, consultez la section Points de terminaison FIPS dans le. Références générales AWS

1. Déterminez le point de terminaison du service DataSync FIPS que vous souhaitez utiliser.
2. Configurez votre réseau pour autoriser le trafic requis pour utiliser les points de terminaison du service DataSync FIPS.

Étape suivante : Activation de votre AWS DataSync agent

Choix d'un point de terminaison de service VPC

Si vous utilisez un point de terminaison de service VPC, vos données ne sont pas transférées via l'Internet public. DataSync transfère plutôt les données via un VPC basé sur le service Amazon VPC.

Table des matières

- Comment les DataSync agents travaillent avec les points de terminaison de service VPC
- DataSync limitations avec VPCs
- Création d'un point de terminaison de service VPC pour DataSync

Comment les DataSync agents travaillent avec les points de terminaison de service VPC

Les points de terminaison du service VPC sont fournis par. AWS PrivateLink Ces types de points de terminaison vous permettent de vous connecter de manière privée Services AWS à votre VPC pris en charge. Lorsque vous utilisez un point de terminaison de service VPC avec DataSync, toutes les communications entre votre DataSync agent et le DataSync service restent dans votre VPC.

Le point de terminaison du service VPC (ainsi que les interfaces réseau DataSync créées pour le trafic de transfert de données) sont des adresses IP privées accessibles uniquement depuis votre VPC. Pour de plus amples informations, veuillez consulter Connecter votre réseau pour les AWS DataSync transferts.

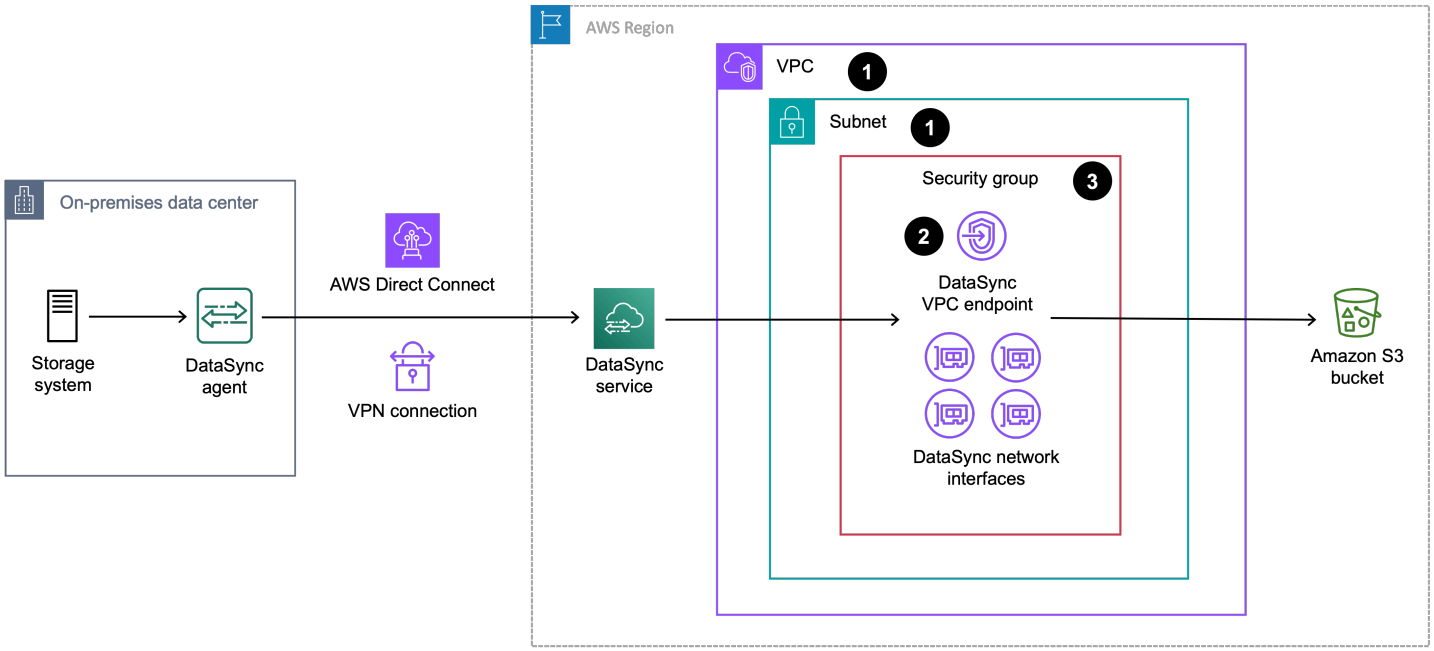
DataSync limitations avec VPCs

- VPCs que vous utilisez avec DataSync doit avoir une location par défaut. VPCs avec location dédiée ne sont pas pris en charge.
- DataSync ne prend pas en charge le partage VPCs.

Création d'un point de terminaison de service VPC pour DataSync

Vous créez un point de terminaison de service VPC pour DataSync un VPC que vous gérez. Votre point de terminaison de service, votre VPC et votre DataSync agent doivent appartenir au même. Compte AWS

Le schéma suivant montre un exemple d' DataSync utilisation d'un point de terminaison de service VPC pour le transfert d'un système de stockage sur site vers un compartiment Amazon S3. Les légendes numérotées correspondent aux étapes de création d'un point de terminaison de service VPC.



Pour créer un point de terminaison de service VPC pour DataSync

1. Créez ou déterminez un VPC et un sous-réseau dans lesquels vous souhaitez créer votre point de terminaison de service VPC.

   Si vous effectuez un transfert vers ou depuis un stockage externe AWS, le VPC doit s'étendre à cet environnement de stockage (par exemple, votre environnement de stockage peut être un centre de données dans lequel se trouve votre serveur de fichiers NFS sur site). Vous pouvez le faire en utilisant des règles de routage AWS Direct Connectou un VPN.

2. Créez un point de terminaison de service DataSync VPC en procédant comme suit :

   a. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

   b. Dans le volet de navigation de gauche, choisissez Endpoints, puis Create endpoint.

c. Pour Service category (Catégorie de service), choisissez Services AWS.

d. Pour les services, recherchez **`datasync`** et choisissez le point de terminaison correspondant à la région dans laquelle vous vous trouvez (par exemple,`com.amazonaws.us-east-1.datasync`).

e. Pour le VPC, choisissez le VPC dans lequel vous souhaitez créer le point de terminaison du service VPC.

f. Développez les paramètres supplémentaires et décochez la case Activer le nom DNS privé pour désactiver ce paramètre.

   Nous vous recommandons de désactiver ce paramètre si vous avez des agents dans le même VPC qui doivent utiliser un point de terminaison de service public. Un agent ne peut pas accéder à un point de terminaison de service public via le réseau lorsque ce paramètre est activé.

g. Pour Sous-réseau, choisissez le sous-réseau dans lequel vous souhaitez créer le point de terminaison du service VPC. Prenez note de l'ARN du sous-réseau (vous en avez besoin pour activer votre agent).

h. Choisissez Créer un point de terminaison. Prenez note de l'identifiant du point de terminaison (vous en aurez besoin pour activer votre agent).

3. Dans votre VPC, configurez un groupe de sécurité qui autorise le trafic requis pour utiliser les points de terminaison du service DataSync VPC. Prenez note de l'ARN du groupe de sécurité (vous en avez besoin pour activer votre agent).

   Le groupe de sécurité doit autoriser votre agent à se connecter aux adresses IP privées du point de terminaison du service VPC et à vos interfaces réseau (qui sont créées lorsque vous créez votre tâche).

Étape suivante : Activation de votre AWS DataSync agent

Activation de votre AWS DataSync agent

Pour terminer la création de votre AWS DataSync agent, vous devez l'activer. Cette étape associe l'agent à votre Compte AWS.

> **Note**
>
> Vous ne pouvez pas activer un Compte AWS agent plusieurs fois. Région AWS

Prérequis

Pour activer votre DataSync agent, assurez-vous de disposer des informations suivantes :

- Le point DataSync de terminaison de service avec lequel vous activez votre agent.

  Si vous utilisez un point de terminaison de service VPC, vous avez besoin des informations suivantes :

  - L'ID du point de terminaison du service VPC.
  - Sous-réseau dans lequel se trouve le point de terminaison de votre service VPC.
  - Le groupe de sécurité qui autorise le trafic requis pour utiliser les points de terminaison du service DataSync VPC.
- Adresse IP ou nom de domaine de votre agent.

  La manière de le trouver dépend du type d'agent que vous déployez. Par exemple, si votre agent est une EC2 instance Amazon, vous pouvez trouver son adresse IP en vous rendant sur la page de l'instance sur la EC2 console Amazon.

Obtenir une clé d'activation

Vous pouvez obtenir une clé d'activation pour votre DataSync agent déployé de différentes manières. Certaines options nécessitent l'accès à votre agent sur le port 80 (HTTP). Si vous utilisez l'une de ces options, DataSync ferme le port une fois que vous avez activé l'agent.

> **Note**
>
> Les clés d'activation de l'agent expirent au bout de 30 minutes si elles ne sont pas utilisées.

DataSync console

Lorsque vous activez votre agent dans la DataSync console, vous DataSync pouvez obtenir la clé d'activation pour vous en utilisant l'option Obtenir automatiquement la clé d'activation auprès de votre agent.

Pour utiliser cette option, votre navigateur doit être en mesure de joindre votre agent sur le port 80.

Agent local console

Contrairement aux autres options permettant d'obtenir une clé d'activation, cette option ne nécessite pas que votre agent soit accessible sur le port 80.

1. Connectez-vous à la console locale de la machine virtuelle (VM) de votre agent ou de votre EC2 instance Amazon.
2. Dans le menu principal AWS DataSync Activation - Configuration, entrez **0** pour obtenir une clé d'activation.
3. Entrez le nom dans Région AWS lequel vous activez votre agent.
4. Entrez le type de point de terminaison de service utilisé par votre agent.
5. Copiez la clé d'activation qui s'affiche.

   Par exemple : `F0EFT-7FPPR-GG7MC-3I9R3-27DOH`

   Vous spécifiez cette clé lors de l'activation de votre agent.

CLI

Avec les outils Unix standard, vous pouvez envoyer une `curl` demande à l'adresse IP de votre agent pour obtenir sa clé d'activation.

Pour utiliser cette option, votre client doit pouvoir joindre votre agent sur le port 80. Vous pouvez exécuter la commande suivante pour vérifier :

```
nc -vz agent-ip-address 80
```

Une fois que vous avez confirmé que vous pouvez joindre l'agent, exécutez l'une des commandes suivantes en fonction du type de point de terminaison de service que vous utilisez :

- Points de terminaison du service public :

```
curl "http://agent-ip-address/?gatewayType=SYNC&activationRegion=your-
region&no_redirect"
```

- Points de terminaison du service FIPS :

```
curl "http://agent-ip-address/?gatewayType=SYNC&activationRegion=your-
region&endpointType=FIPS&no_redirect"
```

- Points de terminaison du service VPC :

```
curl "http://agent-ip-address/?gatewayType=SYNC&activationRegion=your-
region&privateLinkEndpoint=vpc-endpoint-ip-
address&endpointType=PRIVATE_LINK&no_redirect"
```

  Pour les trouver*vpc-endpoint-ip-address*, ouvrez la console Amazon VPC, choisissez Endpoints, puis sélectionnez le point de terminaison de votre service VPC DataSync . Dans l'onglet Sous-réseaux, recherchez l'adresse IP du sous-réseau du point de terminaison de votre service VPC. Il s'agit de l'adresse IP du terminal.

Cette commande renvoie une clé d'activation. Par exemple :

```
F0EFT-7FPPR-GG7MC-3I9R3-27DOH
```

Vous spécifiez cette clé lors de l'activation de votre agent.

Activation de votre agent

Plusieurs options s'offrent à vous pour activer votre DataSync agent. Une fois activé, il AWS gère l'agent pour vous.

DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Agents, puis Create agent.
3. Dans la section Point de terminaison de service, procédez comme suit pour spécifier le point de terminaison de service pour votre agent :

- Pour un point de terminaison de service public, choisissez Points de terminaison de service public dans ***your current Région AWS***.
- Pour un point de terminaison de service FIPS, choisissez les points de terminaison de service FIPS dans. *your current Région AWS*
- Pour un point de terminaison de service VPC, procédez comme suit :
  - Choisissez les points de terminaison VPC à l'aide de. AWS PrivateLink
  - Pour le point de terminaison VPC, choisissez le point de terminaison du service VPC que vous souhaitez que votre agent utilise.
  - Pour Sous-réseau, choisissez le sous-réseau dans lequel se trouve le point de terminaison de votre service VPC.
  - Pour Groupe de sécurité, choisissez le groupe de sécurité qui autorise le trafic requis pour utiliser les points de terminaison du service DataSync VPC.

4. Dans la section Clé d'activation, effectuez l'une des opérations suivantes pour spécifier la clé d'activation de votre agent :

   - Choisissez Obtenir automatiquement la clé d'activation auprès de votre agent DataSync pour obtenir la clé pour vous.
     - Pour Adresse de l'agent, entrez l'adresse IP ou le nom de domaine de votre agent.
     - Choisissez Obtenir la clé.

       Si l'activation échoue, vérifiez la configuration de votre réseau en fonction du type de point de terminaison de service que vous utilisez.
   - Choisissez Entrez manuellement la clé d'activation de votre agent si vous ne souhaitez pas établir de connexion entre votre navigateur et l'agent.
     - Obtenez la clé depuis la console locale de l'agent ou à l'aide d'une `curl` commande.
     - De retour dans la DataSync console, entrez la clé dans le champ Clé d'activation.
5. (Recommandé) Pour le nom de l'agent, attribuez à votre agent un nom dont vous vous souviendrez.
6. (Facultatif) Pour Tags, entrez des valeurs pour les champs Clé et Valeur pour étiqueter votre agent.

   Les balises vous aident à gérer, à filtrer et à rechercher vos AWS ressources.
7. Choisissez Create agent (Créer un agent).

8. Sur la page Agents, vérifiez que votre agent utilise le type de point de terminaison de service approprié.

> **Note**
>
> À ce stade, vous remarquerez peut-être que votre agent est hors ligne. Cela se produit brièvement après l'activation d'un agent.

AWS CLI

1. Une fois que vous avez obtenu votre clé d'activation, copiez l'une des `create-agent` commandes suivantes en fonction du type de point de terminaison de service que vous utilisez :

   - Point de terminaison du service public ou FIPS :

   ```
   aws datasync create-agent \
     --activation-key activation-key \
     --agent-name name-for-agent
   ```

   - Point de terminaison du service VPC :

   ```
   aws datasync create-agent \
     --activation-key activation-key \
     --agent-name name-for-agent \
     --vpc-endpoint-id vpc-endpoint-id \
     --subnet-arns subnet-arn \
     --security-group-arns security-group-arn
   ```

2. Pour `--activation-key`, spécifiez la clé d'activation de votre agent.
3. (Recommandé) Pour `--agent-name`, spécifiez un nom mémorisable pour votre agent.
4. Si vous utilisez un point de terminaison de service VPC, spécifiez les options suivantes :

   - Pour `--vpc-endpoint-id`, spécifiez l'ID du point de terminaison du service VPC que vous utilisez.
   - Pour `--subnet-arns`, spécifiez l'ARN du sous-réseau où se trouve le point de terminaison de votre service VPC.

- Pour `--security-group-arns`, spécifiez l'ARN du groupe de sécurité qui autorise le trafic requis pour utiliser les points de terminaison du service DataSync VPC.

5. Exécutez la commande `create-agent`.

   Vous obtenez une réponse avec l'ARN de l'agent que vous venez d'activer. Par exemple :

```
{
    "AgentArn": "arn:aws:datasync:us-east-1:111222333444:agent/
agent-0b0addbeef44baca3"
}
```

6. Vérifiez que votre agent est activé en exécutant la `list-agents` commande suivante :

```
aws datasync list-agents
```

> **Note**
>
> À ce stade, vous remarquerez peut-être que votre agent l'`Status`est`OFFLINE`. Cela se produit brièvement après l'activation d'un agent.

DataSync API

Une fois que vous avez obtenu votre clé d'activation, activez votre agent en utilisant l'CreateAgentopération.

> **Note**
>
> Lorsque vous aurez terminé, vous remarquerez peut-être que votre agent est hors ligne. Cela se produit brièvement après l'activation d'un agent.

Étapes suivantes

- Vérifiez la connexion de votre agent à votre système de stockage et au DataSync service.
- Si vous rencontrez des problèmes lors de l'activation de votre agent, demandez de l'aide pour résoudre les problèmes.

- Créez l' DataSync emplacement que vous souhaitez utiliser avec votre agent. Il peut s'agir d'un site sur site ou d'un autre emplacement dans le cloud.

Vérification des connexions réseau de votre agent

Une fois que vous avez activé votre AWS DataSync agent, assurez-vous qu'il dispose d'une connectivité réseau avec votre système de stockage et le DataSync service.

Accès à la console locale de votre agent

La manière dont vous accédez à la console locale de votre agent dépend du type d'agent que vous utilisez.

Accès à la console locale (VMware ESXiLinux KVM ou Microsoft Hyper-V)

Pour des raisons de sécurité, vous ne pouvez pas vous connecter à distance à la console locale de la machine virtuelle (VM) de l' DataSync agent.

- Si c'est la première fois que vous utilisez la console locale, connectez-vous avec les informations d'identification par défaut. Par défaut, le nom d'utilisateur est **`admin`** et le mot de passe est **`password`**.

> **Note**
>
> Nous vous recommandons de changer le mot de passe par défaut. Pour ce faire, dans le menu principal de la console, entrez **5** (ou **6** pour VMware VMs), puis exécutez la `passwd` commande pour modifier le mot de passe.

Accès à la console locale (Amazon EC2)

Pour vous connecter à la console locale d'un EC2 agent Amazon, vous devez utiliser SSH.

Avant de commencer : assurez-vous que le groupe de sécurité de votre EC2 instance autorise l'accès via SSH (port TCP 22).

1. Ouvrez un terminal et copiez la `ssh` commande suivante :

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

- Pour*/path/key-pair-name*, spécifiez le chemin et le nom de fichier (`.pem`) de la clé privée requise pour vous connecter à votre instance.
- Pour *instance-user-name*, spécifiez `admin`.
- Pour*instance-public-ip-address*, spécifiez l'adresse IP publique de votre instance.

2. Exécutez la `ssh` commande pour vous connecter à l'instance.

Une fois connecté, le menu principal de la console locale de l'agent s'affiche.

Vérification de la connexion de votre agent à votre système de stockage

Vérifiez si votre DataSync agent peut se connecter à votre système de stockage. Pour de plus amples informations, veuillez consulter 1. Connexion réseau entre votre système de stockage et l'agent.

1. Accédez à la console locale de votre agent.
2. Dans le menu principal AWS DataSync Activation - Configuration, entrez**3**.
3. Entrez l'une des options suivantes :
   a. Entrez **1** pour tester une connexion au serveur NFS.
   b. Entrez **2** pour tester une connexion à un serveur SMB.
   c. Entrez **3** pour tester une connexion à un serveur de stockage d'objets.
   d. Entrez **4** pour tester une connexion HDFS.
   e. Entrez **5** pour tester une Microsoft Azure Blob Storage connexion.
4. Entrez l'adresse IP ou le nom de domaine du serveur de stockage.

   N'oubliez pas les points suivants lorsque vous entrez l'adresse IP ou le nom de domaine :

   - N'incluez pas de protocole. Par exemple, entrez **`mystorage.com`** au lieu de**`https://mystorage.com`**.
   - Pour HDFS, entrez l'adresse IP ou le nom de domaine du NameNode ou DataNode dans le cluster Hadoop.
5. Sur demande, entrez le port TCP pour la connexion au serveur de stockage (par exemple,**443**).

Vérifiez si le test de connectivité a réussi ou échoué.

Vérification de la connexion de votre agent au DataSync service

Vérifiez si votre DataSync agent peut se connecter au DataSync service. Pour de plus amples informations, veuillez consulter 2. Connexion réseau entre votre agent et le DataSync service.

1. Accédez à la console locale de votre agent.
2. Dans le menu principal AWS DataSync Activation - Configuration, entrez **2** pour commencer à tester la connectivité réseau.

   Si votre agent est activé, l'option Tester la connectivité réseau peut être lancée sans intervention supplémentaire de l'utilisateur, car la région et le type de point de terminaison sont extraits des informations de l'agent activé.
3. Entrez le type de point de terminaison de DataSync service utilisé par votre agent :

   a. Pour les terminaux de service public, entrez **1** et l' Région AWS endroit où votre agent est activé.

   b. Pour les points de terminaison du service FIPS, entrez **2** la région dans laquelle votre agent est activé.

   c. Pour les points de terminaison du service VPC, entrez. **3**

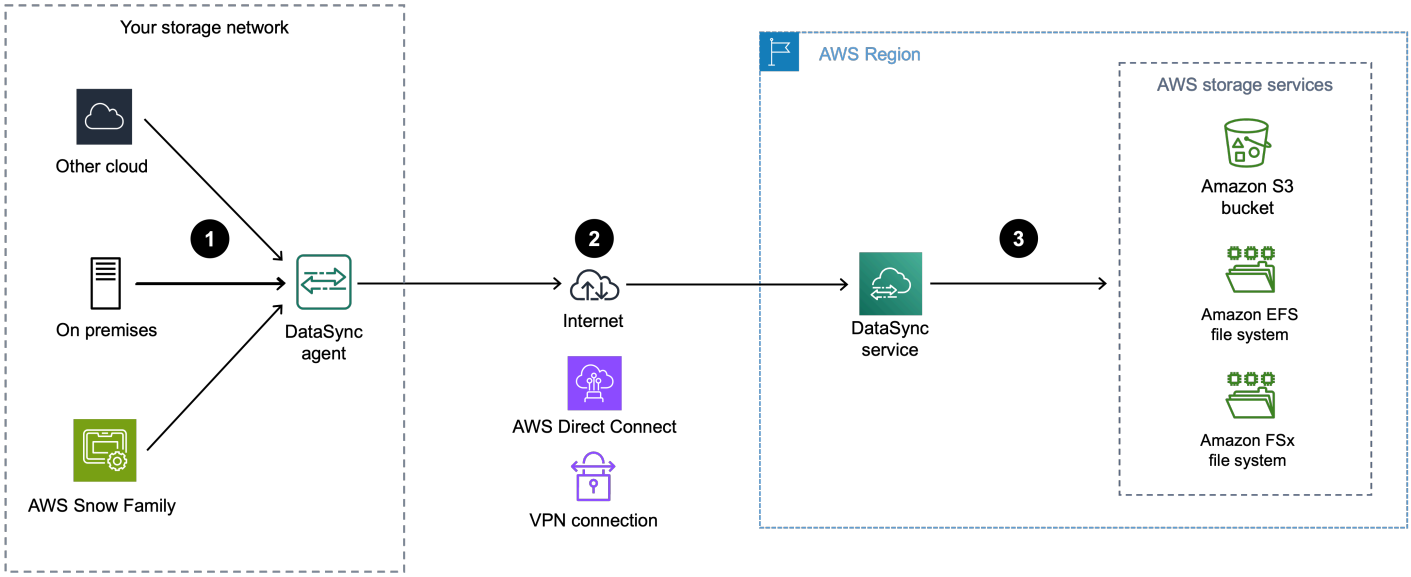
   Le message « RÉUSSI » ou « ÉCHEC » s'affiche.
4. Si le message FAILED s'affiche, vérifiez la configuration de votre réseau. Pour de plus amples informations, veuillez consulter AWS DataSync exigences du réseau.

Étapes suivantes

Créez l' DataSync emplacement que vous souhaitez utiliser avec votre agent. Il peut s'agir d'un site sur site ou d'un autre emplacement dans le cloud.

Connecter votre réseau pour les AWS DataSync transferts

Si vous avez besoin d'un AWS DataSync agent, vous devez établir plusieurs connexions réseau pour le transfert de données. Le schéma suivant montre les trois connexions réseau lors d'un DataSync transfert d'un système de stockage (qui peut être sur site, dans un autre cloud ou à la périphérie) vers un service AWS de stockage.



1. Connexion réseau entre votre système de stockage et l'agent

Votre DataSync agent se connecte à votre système de stockage sur site, à un autre cloud ou à un système de stockage périphérique. Pour de plus amples informations, veuillez consulter Exigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie.

2. Connexion réseau entre votre agent et le DataSync service

La connexion de votre agent au DataSync service comporte quelques aspects. Vous devez d'abord connecter votre réseau de stockage à AWS. Ensuite, votre agent a besoin d'un point de terminaison de service avec lequel communiquer DataSync.

Table des matières

- Connexion de votre réseau de stockage à AWS
- Choix d'un point de terminaison de service

Connexion de votre réseau de stockage à AWS

Lors de l'utilisation DataSync, considérez les options suivantes pour connecter votre réseau de stockage à AWS :

- AWS Direct Connect- Avec Direct Connect, vous pouvez créer une connexion dédiée entre votre réseau de stockage et AWS. D'un DataSync point de vue, cela vous permet de :
  - Transférez les données via un chemin privé vers votre cloud privé virtuel (VPC), ce qui évite le routage via l'Internet public.
  - Bénéficiez d'une connexion plus prévisible que l'utilisation d'un réseau privé virtuel (VPN) pour connecter votre réseau de stockage AWS (en particulier si votre agent est une EC2 instance Amazon).
  - Utilisez n'importe quel type de point de terminaison de DataSync service, y compris les points de terminaison publics, FIPS (Federal Information Processing Standard) ou VPC.

  Pour de plus amples informations, veuillez consulter DataSync exemples d'architecture et de routage avec AWS Direct Connect.
- VPN - Vous pouvez connecter votre réseau de stockage à AWS l'aide d'un VPN (tel que AWS Site-to-Site VPN).
- Internet public : vous pouvez connecter votre réseau de stockage directement à DataSync Internet en utilisant un point de terminaison de service public ou FIPS.

Choix d'un point de terminaison de service

Votre agent utilise un point de terminaison de service avec lequel il communique DataSync. Pour de plus amples informations, veuillez consulter Choisir un point de terminaison de service pour votre AWS DataSync agent.

3. Connexion réseau entre le DataSync service et le service AWS de stockage

Pour vous connecter DataSync à un service AWS de stockage, vous devez simplement vous assurer que le DataSync service peut accéder à votre compartiment ou système de fichiers S3. Pour de plus amples informations, veuillez consulter Configuration réseau requise pour les services AWS de stockage.

Réseauter lorsque vous n'avez pas besoin d'un DataSync agent

Pour les transferts qui ne nécessitent pas DataSync l'intervention d'un agent, vous devez simplement vous assurer que le DataSync service peut accéder aux systèmes AWS de stockage entre lesquels vous effectuez le transfert. Pour de plus amples informations, veuillez consulter Configuration réseau requise pour les services AWS de stockage.

Comment et où DataSync le trafic circule sur le réseau

DataSync a un trafic sur le plan de données et sur le plan de contrôle. Il est important de savoir comment chacun de ces éléments circule sur le réseau si vous souhaitez séparer votre DataSync trafic.

- Trafic du plan de données : inclut les données de fichiers ou d'objets qui se déplacent entre vos emplacements de stockage. Dans la plupart des cas, le trafic du plan de données est acheminé via des interfaces réseau qui génèrent et gèrent DataSync automatiquement lorsque vous créez une tâche. L'endroit où ces interfaces réseau sont créées dépend du type de service de AWS stockage vers ou depuis lequel vous effectuez le transfert et du point de terminaison de service utilisé par votre DataSync agent.
- Contrôlez le trafic aérien : inclut les activités de gestion de vos DataSync ressources. Ce trafic passe par le point de terminaison de service utilisé par votre agent.

Sécurité du réseau pour DataSync

Pour plus d'informations sur la manière dont vos données de stockage (y compris les métadonnées) sont sécurisées lors d'un transfert, consultezAWS DataSync chiffrement en transit.

AWS DataSync exigences du réseau

La configuration de votre réseau est une étape importante de la configuration AWS DataSync. La configuration de votre réseau dépend de plusieurs facteurs, tels que le type de système de stockage avec lequel vous travaillez. Cela dépend également du type de point de terminaison de DataSync service que vous prévoyez d'utiliser.

IPv6 soutien

DataSync dispose d'un support à double pile pour une compatibilité à la fois avec IPv4 les IPv6 réseaux. IPv6 le support est disponible partout Régions AWS où le service est offert. DataSync prend en charge l'utilisation d' IPv6 adresses avec les sources de données suivantes :

- Système de fichiers réseau (NFS)
- Bloc de messages du serveur (SMB)
- Stockage d'objets

IPv6-agents compatibles

Pour pouvoir l'utiliser DataSync dans un environnement IPv6 réseau, vous devez utiliser des agents IPv6 compatibles. Ces agents prennent en charge à la fois IPv6 la connectivité IPv4 et s'adaptent aux différents environnements réseau.

- Pour les réseaux IPv6 uniquement, aucune modification de configuration n'est requise.
- Pour les réseaux IPv4 uniquement, aucune modification de configuration n'est requise.
- Pour les réseaux à double pile (à la fois IPv4 IPv6), laissez l'agent sélectionner le protocole ou configurez-le manuellement selon vos préférences.

Considérations relatives aux réseaux à double pile

Vous pouvez personnaliser le comportement de votre agent via la console locale de la manière suivante :

- IPv6 Désactivez-la afin que l'agent ne puisse pas accéder IPv6 aux systèmes de fichiers locaux ou au DataSync service.
- Définissez la version IP de l'agent à utiliser pour les transferts de données :
  - Définissez cette valeur pour IPv6 que l'agent ne l'utilise que IPv6 pour les transferts de données.
  - Défini de IPv4 telle sorte que l'agent ne l'utilise que IPv4 pour les transferts de données.
  - Réglez sur Auto (restaure la valeur par défaut) afin que l'agent choisisse automatiquement la version du protocole (IPv4 ou IPv6) pour les transferts de données.

Pour plus d'informations sur la gestion des paramètres de version IP de l'agent, consultezthe section called “Effectuer la maintenance de votre agent”.

> **Important**
>
> Les agents créés à partir d'images téléchargées avant le 16 juillet 2025 ne sont pas pris en charge IPv6.

Exigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie

Les exigences réseau suivantes peuvent s'appliquer aux systèmes de stockage sur site, autogérés, dans le cloud et en périphérie. Il s'agit généralement de systèmes de stockage que vous gérez ou qui peuvent être gérés par un autre fournisseur de cloud.

> **Note**
>
> En fonction de votre réseau, vous devrez peut-être autoriser le trafic sur des ports autres que ceux répertoriés ici pour que votre DataSync agent puisse se connecter à votre système de stockage.

De	Pour	Protocole	Port	Comment il est utilisé par DataSync
DataSync agent	serveur de fichiers NFS	TCP	2049 (pour les versions NFS 4.1 et 4.0) 111 et 2049 (pour la version 3.x de NFS)	Monte le serveur de fichiers NFS. DataSync prend en charge les versions NFS 3.x, 4.0 et 4.1.
DataSync agent	Serveur de fichiers SMB	TCP	139 ou 445	Monte le serveur de fichiers SMB.

De	Pour	Protocole	Port	Comment il est utilisé par DataSync
				DataSync prend en charge les versions SMB 1.0 et ultérieures. Pour des raisons de sécurité, nous recommandons d'utiliser SMB version 3.0.2 ou ultérieure. Les versions antérieures, telles que SMB 1.0, contiennent des failles de sécurité connues que les attaquants peuvent exploiter pour compromet tre vos données.

De	Pour	Protocole	Port	Comment il est utilisé par DataSync
DataSync agent	Stockage d'objets	TCP	443 (HTTPS) ou 80 (HTTP) **Note** En fonction de votre stockage d'objets vous devrez peut-être autoriser le trafic sur des ports HTTPS et HTTP non standard (tels que 8443 ou 8080).	Accède à votre stockage d'objets compatible avec Amazon S3 sur site ou dans d'autres clouds.

De	Pour	Protocole	Port	Comment il est utilisé par DataSync
DataSync agent	Cluster Hadoop	TCP	NameNode port (le port par défaut est 8020) Dans la plupart des clusters, vous pouvez trouver ce numéro de port dans le `core-site.xml` fichier sous la `fs.default.name` propriété `fs.default` or (selon la distribution Hadoop).	Accède au NameNodes dans votre cluster Hadoop. Spécifiez le port utilisé lors de la création d'un emplacement HDFS.

De	Pour	Protocole	Port	Comment il est utilisé par DataSync
DataSync agent	Cluster Hadoop	TCP	DataNode port (la valeur par défaut est 50010) Dans la plupart des clusters, vous pouvez trouver ce numéro de port dans le `hdfs-site.xml` fichier situé sous la `dfs.datanode.address` propriété.	Accède au DataNodes dans votre cluster Hadoop. L' DataSynca gent détermine automatiq uement le port à utiliser.
DataSync agent	Serveur de gestion des clés Hadoop (KMS)	TCP	Port KMS (le port par défaut est 9600)	Accède au KMS de votre cluster Hadoop.

De	Pour	Protocole	Port	Comment il est utilisé par DataSync
DataSync agent	Serveur du centre de distribution de clés (KDC) Kerberos	TCP	Port KDC (la valeur par défaut est 88)	S'authentifie auprès du domaine Kerberos. Ce port est utilisé uniquement avec les emplacements HDFS et SMB qui utilisent l'authentification Kerberos.
DataSync agent	Interface de gestion du système de stockage	TCP	Cela dépend de votre réseau	Se connecte à votre système de stockage.

Configuration réseau requise pour les services AWS de stockage

Les ports réseau requis pour se connecter DataSync à un service AWS de stockage lors d'un transfert varient.

De	Pour	Protocole	Port
DataSync service	Amazon EFS	TCP	2049
DataSync service	FSx pour le serveur de fichiers Windows	Voir contrôle d'accès au système de fichiers FSx pour Windows File Server.	
DataSync service	FSx pour Lustre	Voir le contrôle d'accès au système de fichiers FSx pour Lustre.	
DataSync service	FSx pour OpenZFS	Voir contrôle d'accès au système de fichiers FSx pour OpenZFS.	
DataSync service	FSx pour ONTAP	TCP	111, 635 et 2049 (NFS)

De	Pour	Protocole	Port
			445 (PME)
DataSync service	Amazon S3	N/A (DataSync se connecte aux compartiments S3 en votre nom)	

Exigences réseau pour les points de terminaison publics ou de service FIPS

Votre DataSync agent a besoin de l'accès réseau suivant lorsqu'il utilise des points de terminaison publics ou de service FIPS. Si vous utilisez un pare-feu ou un routeur pour filtrer ou limiter le trafic réseau, configurez votre pare-feu ou routeur pour autoriser ces points de terminaison.

De	Pour	Protocole	Port	Comment il est utilisé	Endpoints consultés
Votre navigateur web	DataSync agent	TCP	80 (HTTP)	Permet à votre navigateur d'obtenir la clé d'activation de l' DataSync agent. Une fois activé, DataSync ferme le port 80 de l'agent. Votre agent n'a pas besoin que le port 80 soit accessible au public. Le niveau requis de l'accès au port 80 dépend de la configura	N/A

De	Pour	Protocole	Port	Comment il est utilisé	Endpoints consultés
				tion de votre réseau. Note Vous pouvez obtenir la clé d'activation sans connexion entre votre navigateur et l'agent. Pour de plus amples informations, veuillez consulter Obtenir une clé d'activation.	

De	Pour	Protocole	Port	Comment il est utilisé	Endpoints consultés
DataSync agent	Amazon CloudFront	TCP	443 (HTTPS)	Permet de démarrer votre DataSync agent avant son activation.	Régions AWS: • `d3dvvaliwoko8h.cloudfront.net` AWS GovCloud (US) Régions : • `s3.us-gov-west-1.amazonaws.com/fmrsendpoints-endpoints bucket-go4p5gpna6sk`
DataSync agent	AWS	TCP	443 (HTTPS)	Active votre DataSync agent et l'associe à votre Compte AWS. Vous pouvez bloquer le point de terminaison public après l'activation.	*`activation-region`* C'est Région AWS là que vous activez votre DataSync agent. Activation du point de terminaison public : • `activation.datasync.` *`activation-region`*`.amazonaws.com` Activation du terminal FIPS : • `activation.datasync-fips.` *`activation-region`*`.amazonaws.com`

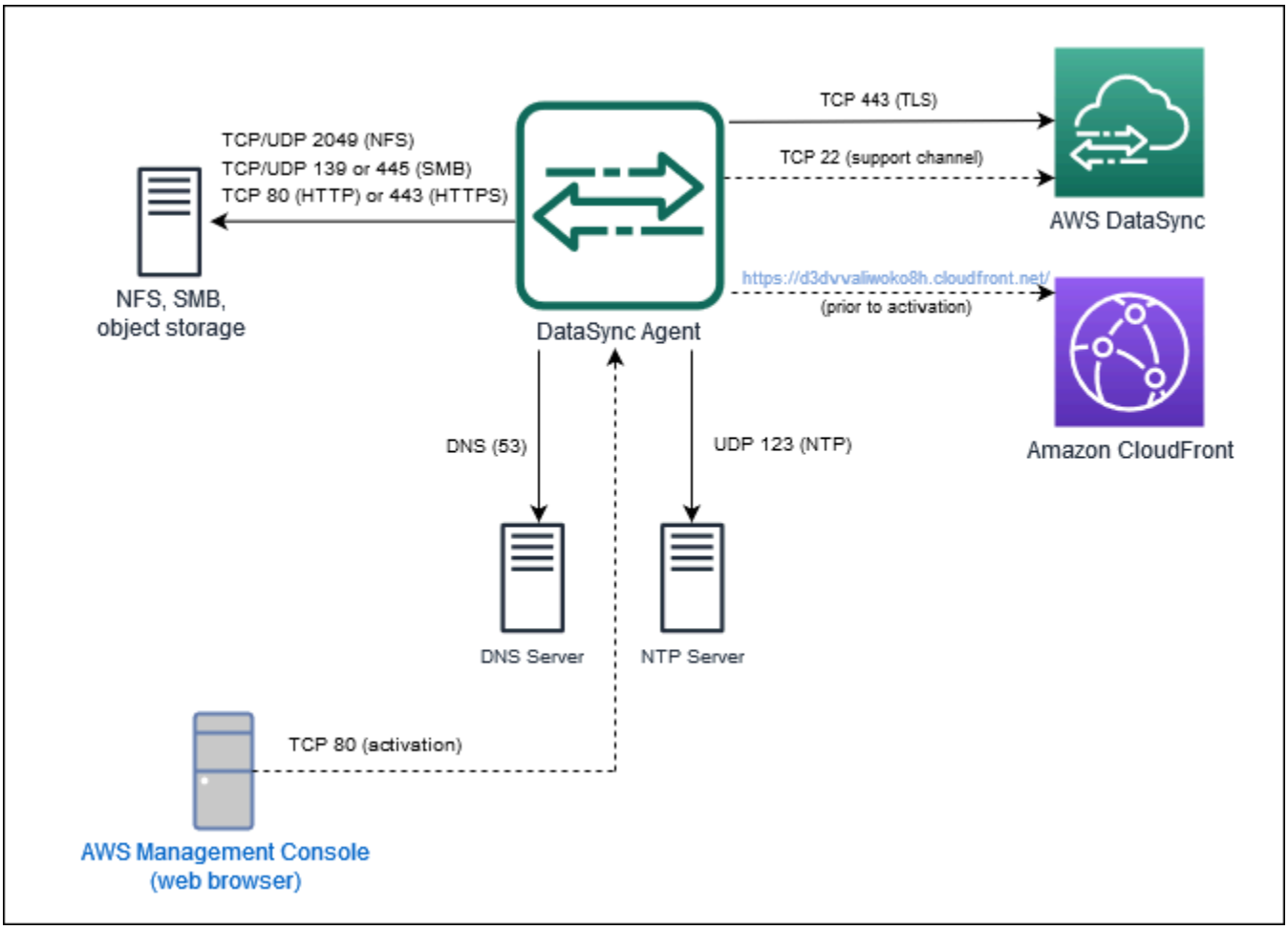
De	Pour	Protocole	Port	Comment il est utilisé	Endpoints consultés
DataSync agent	AWS	TCP	443 (HTTPS)	Permet la communication entre l' DataSync agent et le point de terminaison DataSync du service. Pour plus d'informations, consultez Choisir un point de terminaison de service pour votre AWS DataSync agent.	*activation-region* C'est Région AWS là que vous activez votre DataSync agent. Selon l'usage DataSync que vous en faites, il se peut que vous n'ayez pas besoin d'autoriser l'accès à tous les points de terminaison répertoriés ici. DataSync extrémités du plan de contrôle : • Point de terminaison public : `cp.datasync.` *activation-region* `.amazonaws.com` • Point de terminaison FIPS : `cp.datasync-fips.`*activation-region*`.amazonaws.com` DataSync point de terminaison du plan de données (pour les tâches de transfert uniquement) : • *your-task-id* `.datasync-dp.` *activation-region*`.amazonaws.com`

De	Pour	Protocole	Port	Comment il est utilisé	Endpoints consultés
Votre client	AWS	TCP	443 (HTTPS)	Vous permet de faire des demandes DataSync d'API.	*activation-region* C'est Région AWS là que vous activez votre DataSync agent. Point de terminaison public : • datasync. *activation-region*.amazonaws.com Point de terminaison FIPS : • datasync-fips. *activation-region* .amazonaws.com

De	Pour	Protocole	Port	Comment il est utilisé	Endpoints consultés
DataSync agent	AWS	TCP	443 (HTTPS)	Permet à l' DataSync agent d'obtenir des mises à jour auprès de AWS. Pour de plus amples informations, veuillez consulter Gérer votre AWS DataSync agent.	*activation-region* C'est Région AWS là que vous activez votre DataSync agent. • amazonlinux.default.amazonaws.com • cdn.amazonlinux.com • amazonlinux-2-repos- *activation-region* .s3.dualstack. *activation-region*.amazonaws.com • amazonlinux-2-repos- *activation-region*.s3.*activation-region*.amazonaws.com • *.s3.*activation-region*.amazonaws.com • *.s3.dualstack. *activation-region*.amazonaws.com
DataSync agent	Serveur DNS (Domain Name Service)	TCP/UDP	53 (DNS)	Permet la communication entre l' DataSync agent et le serveur DNS.	N/A

De	Pour	Protocole	Port	Comment il est utilisé	Endpoints consultés
DataSync agent	AWS	TCP	22 (canal de support)	Permet d'accéder AWS Support à votre DataSync agent pour vous aider à résoudre les problèmes . Il n'est pas nécessaire que ce port soit ouvert pour un fonctionnement normal.	AWS Support canal : • `54.201.223.107`
DataSync agent	Serveur NTP (Network Time Protocol)	UDP	123 (NTP)	Permet aux systèmes locaux de synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte.	NTP : • `0.amazon.pool.ntp.org` • `1.amazon.pool.ntp.org` • `2.amazon.pool.ntp.org` • `3.amazon.pool.ntp.org` **Note** Pour modifier la configuration NTP par défaut de votre agent de machine virtuelle afin d'utiliser un autre serveur NTP à l'aide de la console locale, consultez. Synchronisation de l'heure de votre agent VMware

Le schéma suivant montre les ports requis DataSync lors de l'utilisation de points de terminaison publics ou de service FIPS.



Configuration réseau requise pour les points de terminaison de service VPC

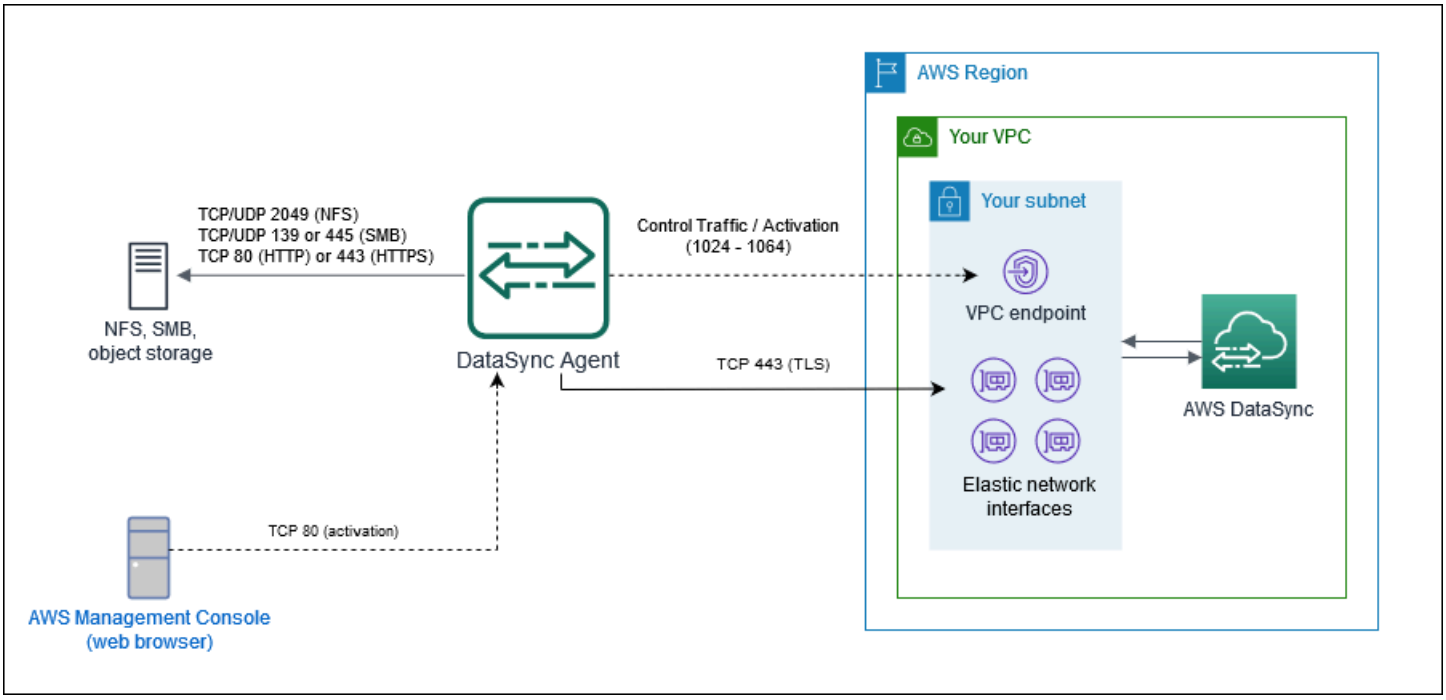
Un point de terminaison de cloud privé virtuel (VPC) fournit une connexion privée entre votre agent, AWS qui ne traverse pas Internet et n'utilise pas d'adresses IP publiques. Cela permet également d'empêcher les paquets d'entrer ou de sortir du réseau. Pour de plus amples informations, veuillez consulter Choix d'un point de terminaison de service VPC.

DataSync nécessite les ports suivants pour que votre agent utilise un point de terminaison de service VPC.

De	Pour	Protocole	Port	Comment il est utilisé
Votre navigateur web	Votre DataSync agent	TCP	80 (HTTP)	Permet à votre navigateur d'obtenir la clé d'activation de l'agent. Une fois activé, DataSync ferme le port 80 de l'agent. Votre agent n'a pas besoin que le port 80 soit accessible au public. Le niveau requis de l'accès au port 80 dépend de la configuration de votre réseau. **Note** Vous pouvez obtenir la clé d'activation sans connexion entre votre navigateur et l'agent. Pour de plus amples informations, veuillez consulter Obtenir une clé d'activation.
DataSync agent	Votre point de DataSync terminaison de service VPC Pour trouver l'adresse IP du point de terminaison, ouvrez la console	TCP	1024-1064	Pour le trafic des avions de contrôle.

De	Pour	Protocole	Port	Comment il est utilisé
	Amazon VPC, choisissez Endpoints, puis sélection nez le point de terminais on de votre service VPC DataSync . Dans l'onglet Sous-réseaux, recherchez l'adresse IP du sous-réseau du point de terminaison de votre service VPC. Il s'agit de l'adresse IP du terminal.			
DataSync agent	Les interfaces réseau de votre DataSync tâche Pour trouver les adresses IP de ces interfaces, consultezAffichage de vos interfaces réseau.	TCP	443 (HTTPS)	Pour le trafic des avions de données.
DataSync agent	Votre point de DataSync terminaison de service VPC	TCP	22 (canal de support)	Pour autoriser AWS Support l'accès à votre DataSync agent à des fins de dépannage. Il n'est pas nécessaire que ce port soit ouvert pour un fonctionnement normal.

Le schéma suivant montre les ports requis DataSync lors de l'utilisation des points de terminaison de service VPC.



Interfaces réseau pour les AWS DataSync transferts

Pour chaque tâche que vous créez, génère et gère AWS DataSync automatiquement des interfaces réseau pour le trafic de transfert de données. Le nombre d'interfaces réseau DataSync créées et leur emplacement dépendent des informations suivantes concernant votre tâche de transfert :

- Si votre tâche nécessite un DataSync agent.
- Vos emplacements source et de destination (d'où vous copiez des données et vers lesquels vous copiez des données).
- Type de point de terminaison de service utilisé par votre agent.

Chaque interface réseau utilise une adresse IP unique dans votre sous-réseau (plus il y a d'interfaces réseau, plus vous avez besoin d'adresses IP). Utilisez les tableaux suivants pour vous assurer que votre sous-réseau possède suffisamment d'adresses IP pour effectuer votre tâche.

Interfaces réseau pour les transferts avec les agents

En général, vous avez besoin d'un DataSync agent pour copier des données entre un service AWS de stockage et un système de stockage qui ne l'est pas AWS.

Emplacement	Interfaces réseau créées par défaut	Où les interfaces réseau sont créées lors de l'utilisation d'un point de terminaison public ou FIPS	Où les interfaces réseau sont créées lors de l'utilisation d'un point de terminaison privé (VPC)
Amazon S3	4	N/A [1]	Le sous-réseau que vous spécifiez lors de l'activation de votre DataSync agent.
Amazon EFS	4	Le sous-réseau que vous spécifiez lors de la création de l'emplacement Amazon EFS.	
Serveur FSx de fichiers Amazon pour Windows	4	Le même sous-réseau que le serveur de fichiers préféré du système de fichiers.	
Amazon FSx pour Lustre	4	Le même sous-réseau que le système de fichiers.	
Amazon FSx pour OpenZFS	4	Le même sous-réseau que le système de fichiers.	
Amazon FSx pour NetApp ONTAP	4	Le même sous-réseau que le système de fichiers.	

[1] Les interfaces réseau ne sont pas nécessaires car le DataSync service communique directement avec le compartiment S3.

Interfaces réseau pour les transferts sans agents

Vous n'avez pas besoin d'un DataSync agent pour copier des données entre deux Services AWS.

Le nombre total d'interfaces réseau dépend des DataSync emplacements de votre transfert. Par exemple, le transfert entre les systèmes de fichiers Amazon EFS et FSx Lustre nécessite quatre

interfaces réseau. Dans le même temps, le transfert entre FSx un serveur de fichiers Windows et un compartiment S3 nécessite deux interfaces réseau.

Emplacement	Interfaces réseau créées par défaut	Où les interfaces réseau sont créées
Amazon S3	N/A [1]	N/A [1]
Amazon EFS	2	Le sous-réseau que vous spécifiez lors de la création de l'emplacement Amazon EFS.
FSx pour le serveur de fichiers Windows	2	Le même sous-réseau que le serveur de fichiers préféré pour le système de fichiers.
FSx pour Lustre	2	Le même sous-réseau que le système de fichiers.
FSx pour OpenZFS	2	Le même sous-réseau que le système de fichiers.
FSx pour ONTAP	2	Le même sous-réseau que le système de fichiers.

[1] Les interfaces réseau ne sont pas nécessaires car le DataSync service communique directement avec le compartiment S3.

Affichage de vos interfaces réseau

Pour voir les interfaces réseau allouées à votre tâche de DataSync transfert, effectuez l'une des opérations suivantes :

- Utilisez l'DescribeTaskopération. L'opération renvoie `SourceNetworkInterfaceArns` et `DestinationNetworkInterfaceArns` avec des réponses qui ressemblent à ceci :

```
arn:aws:ec2:your-region:your-account-id:network-interface/eni-f012345678abcdef0
```

Dans cet exemple, l'ID de l'interface réseau est `eni-f012345678abcdef0`.

- Dans la EC2 console Amazon, recherchez votre ID de tâche (tel que `task-f012345678abcdef0`) pour trouver ses interfaces réseau.

DataSync exemples d'architecture et de routage avec AWS Direct Connect

Tenez compte des architectures réseau suivantes lors de l'utilisation AWS Direct Connectde vos AWS DataSync transferts.

> **Tip**
>
> Si votre réseau utilise une passerelle de transit, nous vous recommandons de séparer le chemin logique de votre DataSync transfert afin d'optimiser les coûts (en particulier si vous migrez une grande quantité de données).
> Par exemple, si vous utilisez AWS Transit Gatewaypour le trafic normal entre vos réseaux locaux et vos clouds privés virtuels (VPCs), vous pouvez configurer votre réseau de manière à ce que le DataSync trafic contourne la passerelle de transit et ses frais de traitement des données.

Utilisation de Direct Connect avec un point de terminaison de DataSync service VPC

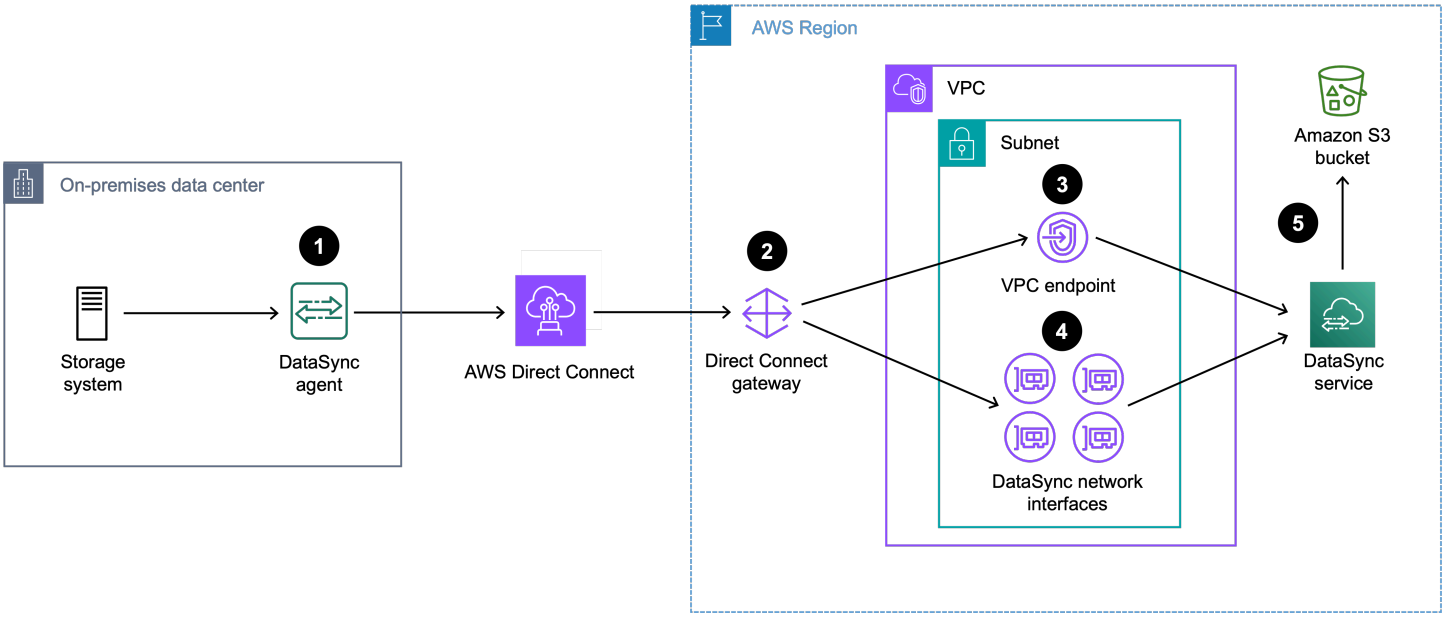
Si votre DataSync agent utilise un point de terminaison de service VPC, vous avez besoin d'une passerelle Direct Connect pour vous connecter à votre VPC.

Table des matières

- Architecture Direct Connect avec point de terminaison VPC et destination S3
- Architecture Direct Connect avec point de terminaison VPC et destination du système de fichiers dans le même sous-réseau
- Architecture Direct Connect avec point de terminaison VPC et destination du système de fichiers dans différents sous-réseaux

Architecture Direct Connect avec point de terminaison VPC et destination S3

L'architecture Direct Connect suivante illustre un DataSync transfert d'un système de stockage sur site vers un compartiment S3.

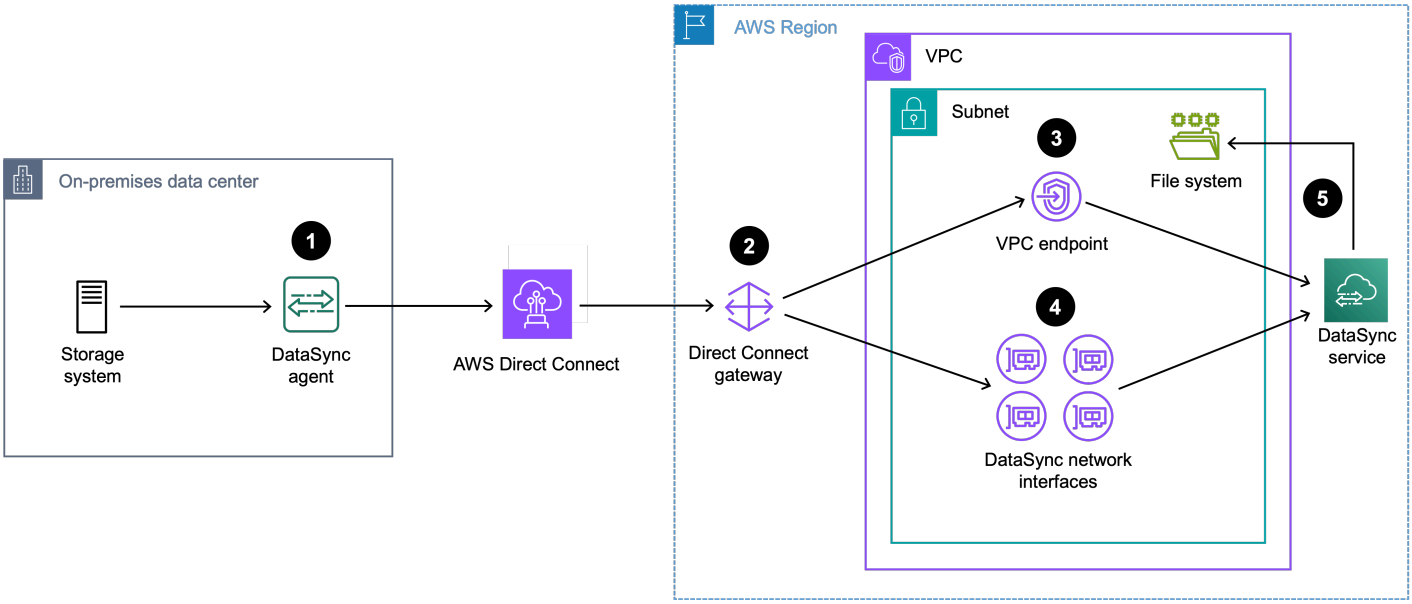


1. L' DataSync agent achemine le DataSync trafic depuis le système de stockage sur site (emplacement source) vers la connexion Direct Connect.
2. DataSync le trafic est acheminé vers une passerelle Direct Connect utilisée pour votre transfert. Pour configurer cela, vous devez :
   a. Associez la passerelle Direct Connect à une passerelle privée virtuelle pour le VPC. Il s'agit du VPC où se trouve le point de terminaison du DataSync VPC et où la DataSync tâche crée des interfaces réseau.
   b. Créez une interface virtuelle privée qui connecte ce VPC à la passerelle Direct Connect.
3. DataSync itinéraires de trafic (plan de contrôle) via le point de DataSync terminaison du VPC.
4. DataSync le trafic (plan de données) passe par les interfaces DataSync réseau du sous-réseau que vous spécifiez lors de la création de l' DataSync agent.
5. DataSync le trafic est acheminé via le DataSync service vers le compartiment S3 (emplacement de destination).

Architecture Direct Connect avec point de terminaison VPC et destination du système de fichiers dans le même sous-réseau

Lors du transfert vers ou depuis un système de FSx fichiers Amazon EFS ou Amazon, votre système de fichiers et votre point de terminaison DataSync VPC peuvent se trouver dans le même sous-réseau.

L'architecture Direct Connect suivante illustre un DataSync transfert d'un système de stockage sur site vers un système de FSx fichiers Amazon EFS ou Amazon.



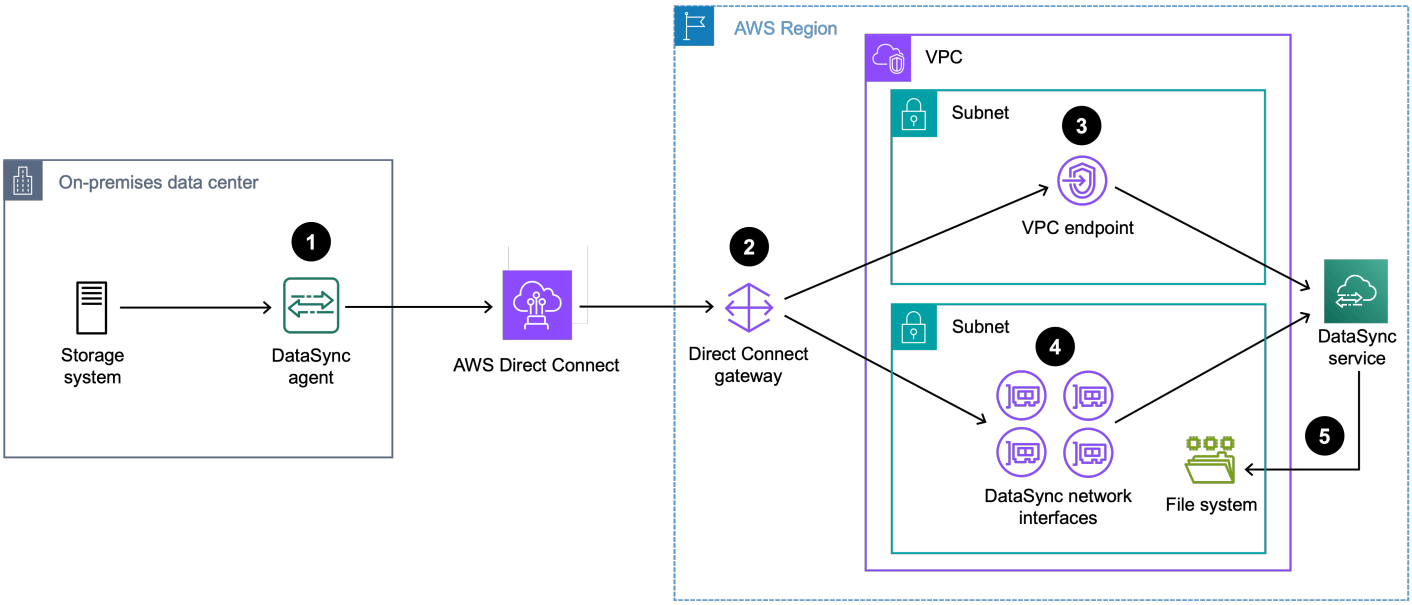
1. L' DataSync agent achemine le DataSync trafic depuis le système de stockage sur site (emplacement source) vers la connexion Direct Connect.
2. DataSync le trafic est acheminé vers une passerelle Direct Connect utilisée pour votre transfert. Pour configurer cela, vous devez :
   a. Associez la passerelle Direct Connect à une passerelle privée virtuelle pour le VPC. Il s'agit du VPC où se trouve le point de terminaison du DataSync VPC et où la DataSync tâche crée des interfaces réseau pour le système de fichiers (emplacement de destination).
   b. Créez une interface virtuelle privée qui connecte ce VPC à la passerelle Direct Connect.
3. DataSync itinéraires de trafic (plan de contrôle) via le point de DataSync terminaison du VPC.
4. DataSync le trafic (plan de données) est acheminé via les interfaces DataSync réseau du sous-réseau du système de fichiers. Il s'agit du même sous-réseau où se trouve le point de terminaison du DataSync VPC.

5. DataSync le trafic est acheminé via le DataSync service vers le système de fichiers (emplacement de destination).

Architecture Direct Connect avec point de terminaison VPC et destination du système de fichiers dans différents sous-réseaux

Lors du transfert vers ou depuis un système de FSx fichiers Amazon EFS ou Amazon, votre système de fichiers et votre point de terminaison DataSync VPC peuvent se trouver dans des sous-réseaux différents.

L'architecture Direct Connect suivante illustre un DataSync transfert d'un système de stockage sur site vers un système de FSx fichiers Amazon EFS ou Amazon.



1. L' DataSync agent achemine le DataSync trafic depuis le système de stockage sur site (emplacement source) vers la connexion Direct Connect.
2. DataSync le trafic est acheminé vers une passerelle Direct Connect utilisée pour votre transfert. Pour configurer cela, vous devez :
   a. Associez la passerelle Direct Connect à une passerelle privée virtuelle pour le VPC. Il s'agit du VPC où se trouve le point de terminaison du DataSync VPC et où la DataSync tâche crée des interfaces réseau pour le système de fichiers (emplacement de destination).
   b. Créez une interface virtuelle privée qui les connecte VPCs à la passerelle Direct Connect.
3. DataSync itinéraires de trafic (plan de contrôle) via le point de DataSync terminaison du VPC.

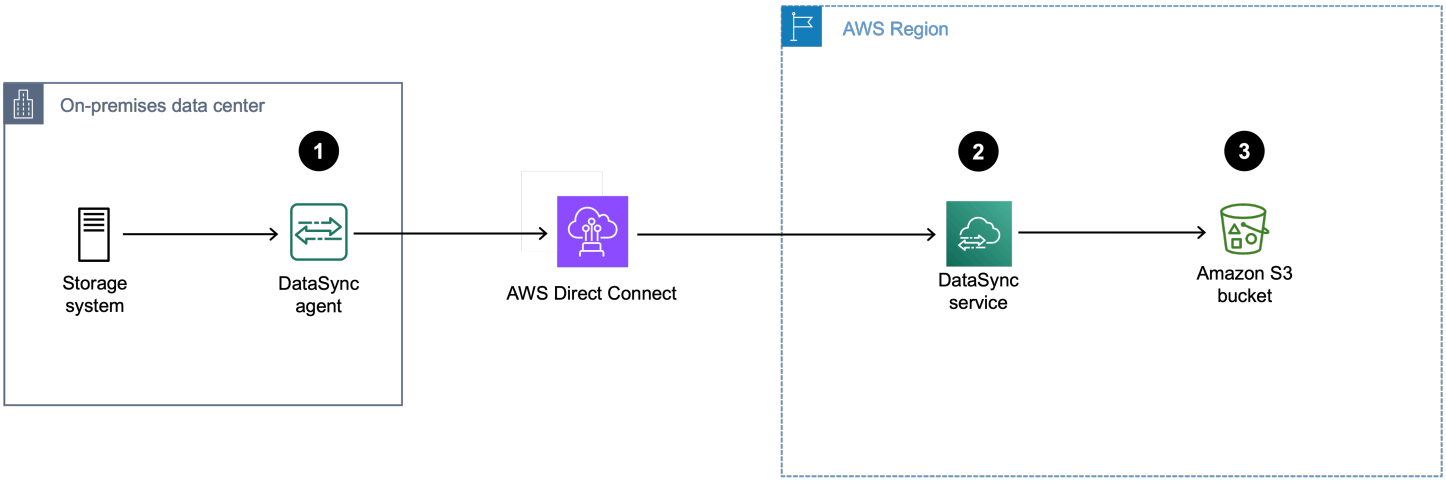
4. DataSync le trafic (plan de données) est acheminé via les interfaces DataSync réseau du sous-réseau du système de fichiers. Il s'agit d'un sous-réseau différent de celui dans lequel se trouve le point de terminaison du DataSync VPC.
5. DataSync le trafic est acheminé via le DataSync service vers le système de fichiers (emplacement de destination).

Utilisation de Direct Connect avec un point de terminaison de service DataSync public ou FIPS

Si votre DataSync agent utilise un point de terminaison de service public ou FIPS (Federal Information Processing Standard), vous pouvez acheminer votre trafic de transfert de données via une connexion Direct Connect à l'aide d'une interface virtuelle publique.

Bien que Direct Connect annonce tous les Région AWS préfixes locaux et distants par défaut, vous pouvez utiliser les balises communautaires BGP pour contrôler l'étendue (régionale ou mondiale) et les préférences d'itinéraire du trafic sur l'interface virtuelle publique. Vous devez publier au moins un préfixe public pour créer votre DataSync agent.

L'architecture Direct Connect suivante montre un DataSync transfert depuis un système de stockage sur site via un point de terminaison public ou FIPS vers un compartiment S3.



1. L' DataSync agent achemine le DataSync trafic depuis le système de stockage sur site (emplacement source) vers la connexion Direct Connect.
2. DataSync le trafic est acheminé vers le DataSync service via une interface virtuelle publique.
3. DataSync trafic vers le compartiment S3 (emplacement de destination).

Étapes suivantes

Si vous avez besoin d'un DataSync agent et que vous n'en avez pas encore créé, déployez l'agent, choisissez un point de terminaison de service pour l'agent, puis activez l'agent.

Une fois que vous avez créé l'agent, vous pouvez configurer votre réseau pour DataSync.

Configuration de votre AWS DataSync agent pour plusieurs NICs

Si vous configurez votre AWS DataSync agent pour utiliser plusieurs adaptateurs réseau (NICs), l'agent est accessible par plusieurs adresses IP. Cela peut être utile dans les cas suivants :

- Maximisation du débit : vous souhaiterez peut-être optimiser le débit vers un agent lorsque les adaptateurs réseau constituent un goulot d'étranglement.
- Isolation du réseau : votre système de fichiers réseau (NFS), votre serveur de messages (SMB), votre système de fichiers distribué Hadoop (HDFS) ou votre serveur de stockage d'objets peuvent résider sur un réseau local virtuel (VLAN) dépourvu de connectivité Internet pour des raisons de sécurité.

Dans un cas d'utilisation typique de plusieurs adaptateurs, un adaptateur est configuré comme route par laquelle l'agent communique AWS (en tant qu'agent par défaut). À l'exception de cet adaptateur, les emplacements de stockage d'objets NFS, SMB, HDFS ou autogérés doivent se trouver dans le même sous-réseau que l'adaptateur qui s'y connecte.

Dans le cas contraire, la communication avec les emplacements NFS, SMB, HDFS ou de stockage d'objets prévus risque de ne pas être possible. Dans certains cas, vous pouvez configurer un emplacement de stockage NFS, SMB, HDFS ou objet sur le même adaptateur que celui utilisé pour communiquer avec. AWS Dans ces cas, le trafic NFS, SMB, HDFS ou de stockage d'objets pour ce serveur et le AWS trafic circulent via le même adaptateur.

Dans certains cas, vous pouvez configurer un adaptateur pour le connecter à la AWS DataSync console, puis ajouter un second adaptateur. Dans ce cas, configure DataSync automatiquement la table de routage pour utiliser le second adaptateur comme route préférée.

Transférer vos données avec AWS DataSync

Avec AWS DataSync, vous pouvez transférer des données vers ou depuis un stockage sur site AWS, dans ou dans d'autres clouds, et en périphérie.

La configuration d'un DataSync transfert implique généralement les étapes suivantes :

1. Déterminez si votre transfert est pris DataSync en charge.
2. Si vous avez besoin d'un DataSync agent pour votre transfert, déployez et activez un agent le plus près possible de l'un de vos systèmes de stockage.

   Par exemple, si vous effectuez un transfert depuis un serveur de fichiers NFS (Network File System) sur site, déployez l'agent le plus près possible de ce serveur de fichiers.
3. Donnez DataSync accès à votre système de stockage.

   DataSync a besoin d'une autorisation pour lire ou écrire dans votre espace de stockage (selon qu'il s'agit d'un emplacement source ou de destination). Découvrez, par exemple, comment fournir un DataSync accès aux serveurs de fichiers NFS.
4. Connectez votre réseau pour le trafic entre votre système de stockage et DataSync.
5. Créez un emplacement pour votre système de stockage à l'aide de la DataSync console ou de DataSync l'API. AWS CLI

   Découvrez par exemple comment créer un emplacement NFS ou un emplacement Amazon S3.
6. Répétez les étapes 3 à 5 pour créer l'autre emplacement de votre transfert.
7. Créez et lancez une tâche de DataSync transfert qui inclut vos emplacements source et de destination.

Rubriques

- Où puis-je transférer mes données AWS DataSync ?
- Transfert vers ou depuis le stockage sur site avec AWS DataSync
- Transfert vers ou depuis un AWS espace de stockage avec AWS DataSync
- Transfert vers ou depuis un autre stockage dans le cloud avec AWS DataSync
- Transfert vers ou depuis un stockage compatible S3 sur Snowball Edge
- Création d'une tâche pour le transfert de vos données
- Lancer une tâche pour transférer vos données

Où puis-je transférer mes données AWS DataSync ?

L'endroit où vous pouvez transférer vos données AWS DataSync dépend des facteurs suivants :

- Emplacements d'origine et de destination de votre transfert
- Si vos sites sont situés dans des lieux différents Comptes AWS
- Si vos sites sont situés dans des lieux différents Régions AWS

Transferts pris en charge dans le même Compte AWS

DataSync prend en charge les transferts entre les ressources de stockage suivantes qui leur sont associées Compte AWS.

Source (de)	Destination (vers)
• NFS • SMB • HDFS • Stockage d'objets	• Amazon S3 (en Régions AWS) • Amazon EFS • Serveur FSx de fichiers Amazon pour Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP
• Amazon S3 (en Régions AWS) • Amazon EFS • FSx pour le serveur de fichiers Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP	• NFS • SMB • HDFS • Stockage d'objets
• Google Cloud Storage • Microsoft Azure Blob Storage • Microsoft Azure Files • Wasabi Cloud Storage • DigitalOcean Spaces	• Amazon S3 (en Régions AWS) • Amazon EFS • Serveur FSx de fichiers Amazon pour Windows • FSx pour Lustre • FSx pour OpenZFS

Source (de)	Destination (vers)
• Oracle Cloud Infrastructure Object Storage • Cloudflare R2 Storage • Backblaze B2 Cloud Storage • NAVER Cloud Object Storage • Alibaba Cloud Object Storage Service • IBM Cloud Object Storage • Seagate Lyve Cloud	• FSx pour ONTAP
• Amazon S3 (en Régions AWS) • Amazon EFS • Serveur FSx de fichiers Amazon pour Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP	• Google Cloud Storage • Microsoft Azure Blob Storage • Microsoft Azure Files • Wasabi Cloud Storage • DigitalOcean Spaces • Oracle Cloud Infrastructure Object Storage • Cloudflare R2 Storage • Backblaze B2 Cloud Storage • NAVER Cloud Object Storage • Alibaba Cloud Object Storage Service • IBM Cloud Object Storage • Seagate Lyve Cloud
• Stockage compatible avec Amazon S3 sur AWS Snowball Edge	• Amazon S3 (en Régions AWS) • Amazon EFS • Serveur FSx de fichiers Amazon pour Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP

Source (de)	Destination (vers)
• Amazon S3 (en Régions AWS) • Amazon EFS • FSx pour le serveur de fichiers Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP	• Stockage compatible avec Amazon S3 sur Snowball Edge
• Amazon S3 (en Régions AWS) • Amazon EFS • FSx pour le serveur de fichiers Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP	• Amazon S3 (en Régions AWS) • Amazon EFS • FSx pour le serveur de fichiers Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP
• Amazon S3 (par AWS régions)	• Amazon S3 sur AWS Outposts
• Amazon S3 sur AWS Outposts	• Amazon S3 (en Régions AWS)

Transferts pris en charge entre Comptes AWS

DataSync prend en charge certains transferts entre des ressources de stockage associées à des ressources différentes Comptes AWS.

Source (de)	Destination (vers)
• Amazon EFS [1] • FSx pour Windows File Server [2]	• Amazon EFS • FSx pour le serveur de fichiers Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP

Source (de)	Destination (vers)
• Amazon S3 (en Régions AWS)	• Amazon S3 (en Régions AWS) • Amazon EFS • FSx pour le serveur de fichiers Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP
• Amazon S3 (en Régions AWS) • Amazon EFS • FSx pour le serveur de fichiers Windows • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP	• Amazon S3 (en Régions AWS)
• NFS • SMB • HDFS • Stockage d'objets	• Amazon S3 (en Régions AWS)

[1] Configuré en tant qu'emplacement NFS.

[2] Configuré en tant qu'emplacement SMB.

Transferts pris en charge dans le même Région AWS

Il n'y a aucune restriction lors du transfert de données au sein d'une même région Région AWS (y compris les régions optionnelles). Pour plus d'informations, consultez la section Régions AWS prise en charge par DataSync.

Transferts pris en charge entre Régions AWS

Tenez compte des points suivants lors du transfert de données entre des supports Régions AWS pris en charge par DataSync :

- Lors du transfert entre des services de AWS stockage situés dans des lieux différents Régions AWS, l'un des deux sites doit se trouver dans la région que vous utilisez DataSync.
- Vous ne pouvez pas effectuer de transfert entre régions dotées d'un emplacement de stockage NFS, SMB, HDFS ou objet. Dans ces situations, vos deux points de transfert doivent se trouver dans la même région où vous activez votre DataSync agent.
- Avec AWS GovCloud (US) Regions, vous pouvez :
  - Transfert entre les régions AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest).
  - Transfert entre une AWS GovCloud (US) région et une zone commerciale Région AWS, telle que l'est des États-Unis (Virginie du Nord). Ce type de transfert nécessite un agent lors du transfert entre les systèmes de FSx fichiers Amazon EFS ou Amazon.

> **Important**
>
> Vous payez pour les données transférées entre Régions AWS. Ce transfert est facturé comme un transfert de données depuis la région source vers la région de destination. Pour plus d'informations, consultez Tarification d'AWS DataSync.

Déterminer si votre transfert nécessite un DataSync agent

Selon votre scénario de transfert, il se peut que vous ayez besoin d'un DataSync agent. Pour de plus amples informations, veuillez consulter Ai-je besoin d'un AWS DataSync agent ?.

Transfert vers ou depuis le stockage sur site avec AWS DataSync

Vous pouvez ainsi transférer des AWS DataSync fichiers et des objets entre un certain nombre de systèmes de stockage sur site ou autogérés et les services de AWS stockage suivants :

- Amazon S3
- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows

- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Rubriques

- Configuration des AWS DataSync transferts avec un serveur de fichiers NFS
- Configuration des AWS DataSync transferts avec un serveur de fichiers SMB
- Configuration des AWS DataSync transferts avec un cluster HDFS
- Configuration des DataSync transferts avec un système de stockage d'objets

Configuration des AWS DataSync transferts avec un serveur de fichiers NFS

Vous pouvez ainsi transférer des données entre votre serveur de fichiers NFS (Network File System) et l'un des services de AWS stockage suivants : AWS DataSync

- Amazon S3
- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Pour configurer ce type de transfert, vous devez créer un emplacement pour votre serveur de fichiers NFS. Vous pouvez utiliser cet emplacement comme source ou destination de transfert.

Fournir un DataSync accès aux serveurs de fichiers NFS

Pour accéder DataSync à votre serveur de fichiers NFS, vous avez besoin d'un DataSync agent. L'agent monte une exportation sur votre serveur de fichiers à l'aide du protocole NFS.

Rubriques

- Configuration de votre exportation NFS
- Versions NFS prises en charge

Configuration de votre exportation NFS

L'exportation requise pour DataSync votre transfert dépend du type d'emplacement source ou de destination de votre serveur de fichiers NFS et de la manière dont les autorisations de votre serveur de fichiers sont configurées.

Si votre serveur de fichiers est un emplacement source, DataSync il vous suffit de lire et de parcourir vos fichiers et dossiers. S'il s'agit d'un emplacement de destination, un accès root est DataSync nécessaire pour y écrire et définir la propriété, les autorisations et les autres métadonnées des fichiers et dossiers que vous copiez. Vous pouvez utiliser `no_root_squash` cette option pour autoriser l'accès root pour votre exportation.

Les exemples suivants décrivent comment configurer une exportation NFS donnant accès à DataSync.

Lorsque votre serveur de fichiers NFS est un emplacement source (accès root)

Configurez votre exportation à l'aide de la commande suivante, qui fournit des autorisations en DataSync lecture seule (`ro`) et un accès root (`no_root_squash`) :

```
export-path datasync-agent-ip-address(ro,no_root_squash)
```

Lorsque votre serveur de fichiers NFS est un emplacement de destination

Configurez votre exportation à l'aide de la commande suivante, qui fournit des autorisations d' DataSyncécriture (`rw`) et un accès root (`no_root_squash`) :

```
export-path datasync-agent-ip-address(rw,no_root_squash)
```

Lorsque votre serveur de fichiers NFS est un emplacement source (pas d'accès root)

Configurez votre exportation à l'aide de la commande suivante, qui spécifie l'ID utilisateur POSIX (UID) et l'ID de groupe (GID) dont vous savez qu'ils fourniront des autorisations en DataSync lecture seule sur l'exportation :

```
export-path datasync-agent-ip-address(ro,all_squash,anonuid=uid,anongid=gid)
```

Versions NFS prises en charge

Par défaut, DataSync utilise la version 4.1 de NFS. DataSync prend également en charge NFS 4.0 et 3.x.

Configuration de votre réseau pour les transferts NFS

Pour votre DataSync transfert, vous devez configurer le trafic pour quelques connexions réseau :

1. Autorisez le trafic sur les ports suivants entre votre DataSync agent et votre serveur de fichiers NFS :

   - Pour les versions NFS 4.1 et 4.0 — port TCP 2049
   - Pour NFS version 3.x : ports TCP 111 et 2049

   Les autres clients NFS de votre réseau devraient être en mesure de monter l'exportation NFS que vous utilisez pour transférer des données. L'exportation doit également être accessible sans authentification Kerberos.
2. Configurez le trafic pour la connexion de votre point de terminaison de service (tel qu'un point de terminaison VPC, public ou FIPS).
3. Autorisez le trafic du DataSync service vers le service AWS de stockage vers ou depuis lequel vous effectuez le transfert.

Création de votre lieu de transfert NFS

Avant de commencer, prenez note des éléments suivants :

- Vous avez besoin d'un serveur de fichiers NFS à partir duquel vous souhaitez transférer des données.
- Vous avez besoin d'un DataSync agent capable d'accéder à votre serveur de fichiers.
- DataSync ne prend pas en charge la copie des listes de contrôle d'accès de la version 4 de NFS (ACLs).

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour le type d'emplacement, choisissez Network File System (NFS).
4. Pour les agents, choisissez l' DataSync agent qui peut se connecter à votre serveur de fichiers NFS.

Vous pouvez choisir plusieurs agents. Pour de plus amples informations, veuillez consulter Utilisation de plusieurs DataSync agents.

5. Pour le serveur NFS, entrez le nom du système de noms de domaine (DNS) ou l'adresse IP du serveur de fichiers NFS auquel votre DataSync agent se connecte.
6. Dans le champ Chemin de montage, entrez le chemin d'exportation NFS que vous DataSync souhaitez monter.

   Ce chemin (ou un sous-répertoire du chemin) est l'endroit où les données sont DataSync transférées depuis ou vers. Pour de plus amples informations, veuillez consulter Configuration de votre exportation NFS.
7. (Facultatif) Développez les paramètres supplémentaires et choisissez une version NFS spécifique DataSync à utiliser lors de l'accès à votre serveur de fichiers.

   Pour de plus amples informations, veuillez consulter Versions NFS prises en charge.
8. (Facultatif) Choisissez Ajouter une balise pour étiqueter votre position NFS.

   Les tags sont des paires clé-valeur qui vous permettent de gérer, de filtrer et de rechercher vos emplacements. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.
9. Choisissez Créer un emplacement.

À l'aide du AWS CLI

- Utilisez la commande suivante pour créer un emplacement NFS.

```
aws datasync create-location-nfs \
    --server-hostname nfs-server-address \
    --on-prem-config AgentArns=datasync-agent-arns \
    --subdirectory nfs-export-path
```

  Pour plus d'informations sur la création de l'emplacement, consultezFournir un DataSync accès aux serveurs de fichiers NFS.

  DataSync choisit automatiquement la version NFS qu'il utilise pour lire à partir d'un emplacement NFS. Pour spécifier une version NFS, utilisez le paramètre `Version` facultatif dans l'opération d'API NfsMountOptions.

Cette commande renvoie l'Amazon Resource Name (ARN) de l'emplacement NFS, similaire à l'ARN indiqué ci-après.

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0f01451b140b2af49"
}
```

Pour vérifier que le répertoire peut être monté, vous pouvez vous connecter à n'importe quel ordinateur possédant la même configuration réseau que votre agent et exécuter la commande suivante.

```
mount -t nfs -o nfsvers=<nfs-server-version <nfs-server-address:<nfs-export-path <test-
folder
```

Voici un exemple de la commande.

```
mount -t nfs -o nfsvers=3 198.51.100.123:/path_for_sync_to_read_from /
temp_folder_to_test_mount_on_local_machine
```

Configuration des AWS DataSync transferts avec un serveur de fichiers SMB

Vous pouvez ainsi transférer des données entre votre serveur de fichiers SMB (Server Message Block) et l'un des services de AWS stockage suivants : AWS DataSync

- Amazon S3
- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Pour configurer ce type de transfert, vous devez créer un emplacement pour votre serveur de fichiers SMB. Vous pouvez l'utiliser comme source ou destination de transfert.

Fournir un DataSync accès aux serveurs de fichiers des PME

DataSync se connecte à votre serveur de fichiers via le protocole SMB et peut s'authentifier avec NTLM ou Kerberos.

Rubriques

- Versions SMB prises en charge
- Utilisation de l'authentification NTLM
- Utilisation de l'authentification Kerberos
- Autorisations requises
- Espaces de noms DFS

Versions SMB prises en charge

Par défaut, choisit DataSync automatiquement une version du protocole SMB en fonction de la négociation avec votre serveur de fichiers SMB.

Vous pouvez également configurer DataSync pour utiliser une version SMB spécifique, mais nous vous recommandons de le faire uniquement si DataSync vous rencontrez des difficultés pour négocier automatiquement avec le serveur de fichiers SMB. DataSync prend en charge les versions SMB 1.0 et ultérieures. Pour des raisons de sécurité, nous vous recommandons d'utiliser SMB version 3.0.2 ou ultérieure. Les versions antérieures, telles que SMB 1.0, contiennent des failles de sécurité connues que les attaquants peuvent exploiter pour compromettre vos données.

Consultez le tableau suivant pour obtenir la liste des options de la DataSync console et de l'API :

Option console	Option d'API	Description
Automatique	`AUTOMATIC`	DataSync et le serveur de fichiers SMB négocient la version la plus élevée de SMB qu'ils supportent mutuellement entre 2.1 et 3.1.1. Il s'agit de l'option recommandée par défaut. Si vous optez pour une version spécifique que votre serveur de fichiers ne prend pas en charge, vous risquez de recevoir une erreur `Operation Not Supported` .

Option console	Option d'API	Description
SMB 3.0.2	`SMB3`	Limite la négociation du protocole à la version SMB 3.0.2 uniquement.
SMB 2.1	`SMB2`	Limite la négociation du protocole à la version 2.1 de SMB uniquement.
SMB 2.0	`SMB2_0`	Limite la négociation du protocole à la version 2.0 de SMB uniquement.
SMB 1.0	`SMB1`	Limite la négociation du protocole à la version 1.0 de SMB uniquement.

Utilisation de l'authentification NTLM

Pour utiliser l'authentification NTLM, vous devez fournir un nom d'utilisateur et un mot de passe qui permettent d'accéder DataSync au serveur de fichiers SMB vers ou depuis lequel vous effectuez le transfert. L'utilisateur peut être un utilisateur local sur votre serveur de fichiers ou un utilisateur de domaine dans votre Microsoft Active Directory.

Utilisation de l'authentification Kerberos

Pour utiliser l'authentification Kerberos, vous devez fournir un fichier principal Kerberos, un fichier de table de clés Kerberos (keytab) et un fichier de configuration Kerberos qui permettent d'accéder DataSync au serveur de fichiers SMB vers ou depuis lequel vous effectuez le transfert.

Rubriques

- Prérequis
- DataSync options de configuration pour Kerberos

Prérequis

Vous devez créer quelques artefacts Kerberos et configurer votre réseau de manière à DataSync pouvoir accéder à votre serveur de fichiers SMB.

- Créez un fichier keytab Kerberos à l'aide de l'utilitaire ktpass ou kutil.

L'exemple suivant crée un fichier keytab à l'aide `ktpass` de. Le domaine Kerberos que vous spécifiez (`MYDOMAIN.ORG`) doit être en majuscules.

```
ktpass /out C:\YOUR_KEYTAB.keytab /princ HOST/kerberosuser@MYDOMAIN.ORG /mapuser
 kerberosuser /pass * /crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL
```

- Préparez une version simplifiée du fichier de configuration Kerberos ()`krb5.conf`. Incluez des informations sur le domaine, l'emplacement des serveurs d'administration du domaine et les mappages des noms d'hôtes sur un domaine Kerberos.

  Vérifiez que le `krb5.conf` contenu est formaté avec le bon boîtier mixte pour les domaines et les noms de domaine. Par exemple :

```
[libdefaults]
  dns_lookup_realm = true
  dns_lookup_kdc = true
  forwardable = true
  default_realm = MYDOMAIN.ORG

[realms]
  MYDOMAIN.ORG = {
    kdc = mydomain.org
    admin_server = mydomain.org
  }

[domain_realm]
  .mydomain.org = MYDOMAIN.ORG
  mydomain.org = MYDOMAIN.ORG
```

- Dans votre configuration réseau, assurez-vous que le port du serveur du centre de distribution de clés Kerberos (KDC) est ouvert. Le port KDC est généralement le port TCP 88.

DataSync options de configuration pour Kerberos

Lorsque vous créez un emplacement SMB utilisant Kerberos, vous configurez les options suivantes.

Option console	Option d'API	Description
Serveur SMB	`ServerHostName`	Le nom de domaine du serveur de fichiers SMB

Option console	Option d'API	Description
		que votre DataSync agent va monter. Pour Kerberos, vous ne pouvez pas spécifier l'adresse IP du serveur de fichiers.
Kerberos principal	`KerberosPrincipal`	Identité dans votre domaine Kerberos autorisée à accéder aux fichiers, aux dossiers et aux métadonnées des fichiers sur votre serveur de fichiers SMB. Un principal Kerberos peut ressembler à. `HOST/kerberosuser@MYDOMAIN.ORG` Les noms principaux distinguent les majuscules et minuscules.
fichier Keytab	`KerberosKeytab`	Un fichier de table de clés Kerberos (keytab), qui inclut les mappages entre votre clé principale Kerberos et vos clés de chiffrement.
Fichier de configuration Kerberos	`KerberosKrbConf`	`krb5.conf` Fichier qui définit la configuration de votre domaine Kerberos.

Option console	Option d'API	Description
Adresses IP DNS (facultatif)	`DnsIpAddresses`	Les IPv4 adresses des serveurs DNS auxquels appartient votre serveur de fichiers SMB. Si votre environnement comporte plusieurs domaines, sa configuration garantit la DataSync connexion au bon serveur de fichiers SMB.

Autorisations requises

L'identité que vous fournissez DataSync doit être autorisée à monter et à accéder aux fichiers, dossiers et métadonnées de fichiers de votre serveur de fichiers SMB.

Si vous fournissez une identité dans votre Active Directory, celle-ci doit être membre d'un groupe Active Directory avec l'un des droits d'utilisateur suivants ou les deux (selon les métadonnées que vous DataSync souhaitez copier) :

Droit de l'utilisateur	Description
Restaurer des fichiers et des répertoires (`SE_RESTORE_NAME`)	Permet DataSync de copier la propriété des objets, les autorisations, les métadonnées des fichiers et les listes d'accès discrétionnaires NTFS ()DACLs. Ce droit d'utilisateur est généralement accordé aux membres des groupes Domain Admins et Backup Operators (qui sont tous deux des groupes Active Directory par défaut).
Gérer le journal d'audit et de sécurité (`SE_SECURITY_NAME`)	Permet DataSync de copier les listes de contrôle d'accès au système NTFS (SACLs).

Droit de l'utilisateur	Description
	Ce droit d'utilisateur est généralement accordé aux membres du groupe des administrateurs de domaine.

Si vous souhaitez copier Windows ACLs et effectuez un transfert entre un serveur de fichiers SMB et un autre système de stockage utilisant SMB (tel qu'Amazon FSx pour Windows File Server ou FSx ONTAP), l'identité que vous fournissez DataSync doit appartenir au même domaine Active Directory ou avoir une relation de confiance Active Directory entre leurs domaines.

Espaces de noms DFS

DataSync ne prend pas en charge les espaces de noms Microsoft Distributed File System (DFS). Nous vous recommandons de spécifier un serveur de fichiers ou un partage sous-jacent lors de la création de votre DataSync emplacement.

Création de votre lieu de transfert pour PME

Avant de commencer, vous avez besoin d'un serveur de fichiers SMB à partir duquel vous souhaitez transférer des données.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour Location type (Type d'emplacement), choisissez Server Message Block (SMB).

   Vous configurerez cet emplacement comme source ou destination plus tard.
4. Pour les agents, choisissez l' DataSync agent qui peut se connecter à votre serveur de fichiers SMB.

   Vous pouvez choisir plusieurs agents. Pour de plus amples informations, veuillez consulter Utilisation de plusieurs DataSync agents.
5. Pour le serveur SMB, entrez le nom de domaine ou l'adresse IP du serveur de fichiers SMB que votre DataSync agent va monter.

   N'oubliez pas ce qui suit avec ce paramètre :

- Vous ne pouvez pas spécifier d'adresse IP version 6 (IPv6).
- Si vous utilisez l'authentification Kerberos, vous devez spécifier un nom de domaine.

6. Dans Nom du partage, entrez le nom du partage exporté par votre serveur de fichiers SMB où les données DataSync seront lues ou écrites.

   Vous pouvez inclure un sous-répertoire dans le chemin de partage (par exemple,`/path/to/subdirectory`). Assurez-vous que les autres clients SMB de votre réseau peuvent également monter ce chemin.

   Pour copier toutes les données du sous-répertoire, vous DataSync devez être en mesure de monter le partage SMB et d'accéder à toutes ses données. Pour de plus amples informations, veuillez consulter Autorisations requises.

7. (Facultatif) Développez les paramètres supplémentaires et choisissez une version SMB DataSync à utiliser lors de l'accès à votre serveur de fichiers.

   Par défaut, choisit DataSync automatiquement une version en fonction de la négociation avec le serveur de fichiers SMB. Pour plus d'informations, consultez Versions SMB prises en charge.

8. Pour le type d'authentification, choisissez NTLM ou Kerberos.

9. Procédez de l'une des manières suivantes en fonction de votre type d'authentification :

   NTLM

   - Dans Utilisateur, entrez un nom d'utilisateur capable de monter votre serveur de fichiers SMB et autorisé à accéder aux fichiers et dossiers concernés par votre transfert.

     Pour de plus amples informations, veuillez consulter Autorisations requises.

   - Dans Mot de passe, entrez le mot de passe de l'utilisateur qui peut monter votre serveur de fichiers SMB et qui est autorisé à accéder aux fichiers et dossiers concernés par votre transfert.
   - (Facultatif) Dans le champ Domaine, entrez le nom de domaine Windows auquel appartient votre serveur de fichiers SMB.

     Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion au bon serveur de fichiers SMB.

Kerberos

- Pour le principal Kerberos, spécifiez un principal dans votre domaine Kerberos autorisé à accéder aux fichiers, aux dossiers et aux métadonnées des fichiers sur votre serveur de fichiers SMB.

  Un principal Kerberos peut ressembler à. `HOST/kerberosuser@MYDOMAIN.ORG`

  Les noms principaux distinguent les majuscules et minuscules. L'exécution de votre DataSync tâche échouera si le principal que vous spécifiez pour ce paramètre ne correspond pas exactement au principal que vous avez utilisé pour créer le fichier keytab.
- Pour le fichier Keytab, téléchargez un fichier keytab qui inclut les mappages entre votre clé principale Kerberos et votre clé de chiffrement.
- Pour le fichier de configuration Kerberos, téléchargez un **`krb5.conf`** fichier qui définit la configuration de votre domaine Kerberos.
- (Facultatif) Pour les adresses IP DNS, spécifiez jusqu'à deux IPv4 adresses pour les serveurs DNS auxquels appartient votre serveur de fichiers SMB.

  Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion au bon serveur de fichiers SMB.

10. (Facultatif) Choisissez Ajouter un tag pour étiqueter l'emplacement de votre PME.

    Les tags sont des paires clé-valeur qui vous permettent de gérer, de filtrer et de rechercher vos emplacements. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.
11. Choisissez Créer un emplacement.

À l'aide du AWS CLI

Les instructions suivantes décrivent comment créer des emplacements SMB avec l'authentification NTLM ou Kerberos.

NTLM

1. Copiez la `create-location-smb` commande suivante.

```
aws datasync create-location-smb \
```

```
    --agent-arns datasync-agent-arns \
    --server-hostname smb-server-address \
    --subdirectory smb-export-path \
    --authentication-type "NTLM" \
    --user user-who-can-mount-share \
    --password user-password \
    --domain windows-domain-of-smb-server
```

2. Pour`--agent-arns`, spécifiez l' DataSync agent qui peut se connecter à votre serveur de fichiers SMB.

   Vous pouvez choisir plusieurs agents. Pour de plus amples informations, veuillez consulter Utilisation de plusieurs DataSync agents.

3. Pour`--server-hostname`, spécifiez le nom de domaine ou l' IPv4 adresse du serveur de fichiers SMB que votre DataSync agent installera.

4. Pour`--subdirectory`, spécifiez le nom du partage exporté par votre serveur de fichiers SMB où les données DataSync seront lues ou écrites.

   Vous pouvez inclure un sous-répertoire dans le chemin de partage (par exemple,`/path/to/subdirectory`). Assurez-vous que les autres clients SMB de votre réseau peuvent également monter ce chemin.

   Pour copier toutes les données du sous-répertoire, vous DataSync devez être en mesure de monter le partage SMB et d'accéder à toutes ses données. Pour de plus amples informations, veuillez consulter Autorisations requises.

5. Pour`--user`, spécifiez un nom d'utilisateur capable de monter votre serveur de fichiers SMB et autorisé à accéder aux fichiers et dossiers concernés par votre transfert.

   Pour de plus amples informations, veuillez consulter Autorisations requises.

6. Pour`--password`, spécifiez le mot de passe de l'utilisateur qui peut monter votre serveur de fichiers SMB et qui est autorisé à accéder aux fichiers et dossiers concernés par votre transfert.

7. (Facultatif) Pour`--domain`, spécifiez le nom de domaine Windows auquel appartient votre serveur de fichiers SMB.

   Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion au bon serveur de fichiers SMB.

8. (Facultatif) Ajoutez `--version` cette option si vous DataSync souhaitez utiliser une version SMB spécifique. Pour de plus amples informations, veuillez consulter Versions SMB prises en charge.
9. Exécutez la commande `create-location-smb`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de l'emplacement que vous avez créé. Par exemple :

```
{
    "arn:aws:datasync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Kerberos

1. Copiez la `create-location-smb` commande suivante.

```
aws datasync create-location-smb \
    --agent-arns datasync-agent-arns \
    --server-hostname smb-server-address \
    --subdirectory smb-export-path \
    --authentication-type "KERBEROS" \
    --kerberos-principal "HOST/kerberosuser@EXAMPLE.COM" \
    --kerberos-keytab "fileb://path/to/file.keytab" \
    --kerberos-krb5-conf "file://path/to/krb5.conf" \
    --dns-ip-addresses array-of-ipv4-addresses
```

2. Pour`--agent-arns`, spécifiez l' DataSync agent qui peut se connecter à votre serveur de fichiers SMB.

   Vous pouvez choisir plusieurs agents. Pour de plus amples informations, veuillez consulter Utilisation de plusieurs DataSync agents.
3. Pour`--server-hostname`, spécifiez le nom de domaine du serveur de fichiers SMB que votre DataSync agent va monter.
4. Pour`--subdirectory`, spécifiez le nom du partage exporté par votre serveur de fichiers SMB où les données DataSync seront lues ou écrites.

   Vous pouvez inclure un sous-répertoire dans le chemin de partage (par exemple,`/path/to/subdirectory`). Assurez-vous que les autres clients SMB de votre réseau peuvent également monter ce chemin.

Pour copier toutes les données du sous-répertoire, vous DataSync devez être en mesure de monter le partage SMB et d'accéder à toutes ses données. Pour de plus amples informations, veuillez consulter Autorisations requises.

5. Pour les options Kerberos, procédez comme suit :

   - `--kerberos-principal`: Spécifiez un principal dans votre domaine Kerberos autorisé à accéder aux fichiers, aux dossiers et aux métadonnées des fichiers sur votre serveur de fichiers SMB.

     Un principal Kerberos peut ressembler à. `HOST/kerberosuser@MYDOMAIN.ORG`

     Les noms principaux distinguent les majuscules et minuscules. L'exécution de votre DataSync tâche échouera si le principal que vous spécifiez pour cette option ne correspond pas exactement au principal que vous avez utilisé pour créer le fichier keytab.
   - `--kerberos-keytab`: Spécifiez un fichier keytab qui inclut les mappages entre votre clé principale Kerberos et vos clés de chiffrement.
   - `--kerberos-krb5-conf`: Spécifiez un `krb5.conf` fichier qui définit la configuration de votre domaine Kerberos.
   - (Facultatif) `--dns-ip-addresses` : Spécifiez jusqu'à deux IPv4 adresses pour les serveurs DNS auxquels appartient votre serveur de fichiers SMB.

     Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion au bon serveur de fichiers SMB.
6. (Facultatif) Ajoutez `--version` cette option si vous DataSync souhaitez utiliser une version SMB spécifique. Pour de plus amples informations, veuillez consulter Versions SMB prises en charge.
7. Exécutez la commande `create-location-smb`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de l'emplacement que vous avez créé. Par exemple :

```
{
    "arn:aws:datasync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Configuration des AWS DataSync transferts avec un cluster HDFS

Vous pouvez ainsi transférer des données entre votre cluster Hadoop Distributed File System (HDFS) et l'un des services de stockage suivants : AWS DataSync AWS

- Amazon S3
- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Pour configurer ce type de transfert, vous devez créer un emplacement pour votre cluster HDFS. Vous pouvez utiliser cet emplacement comme source ou destination de transfert.

Fournir un DataSync accès aux clusters HDFS

Pour vous connecter à votre cluster HDFS, utilisez DataSync un agent que vous déployez le plus près possible de votre cluster HDFS. L' DataSyncagent agit comme un client HDFS et communique avec le NameNodes et DataNodes dans votre cluster.

Lorsque vous lancez une tâche de DataSync transfert, NameNode demande l'emplacement des fichiers et des dossiers du cluster. Si vous configurez votre emplacement HDFS comme emplacement source, DataSync lit les données des fichiers et des dossiers depuis votre cluster et copie ces données vers la destination. DataNodes Si vous configurez votre emplacement HDFS comme emplacement de destination, il DataSync écrit les fichiers et les dossiers de la source vers le contenu DataNodes de votre cluster.

Authentification

Lors de la connexion à un cluster HDFS, DataSync prend en charge l'authentification simple ou l'authentification Kerberos. Pour utiliser l'authentification simple, indiquez le nom d'utilisateur d'un utilisateur autorisé à lire et à écrire sur le cluster HDFS. Pour utiliser l'authentification Kerberos, fournissez un fichier de configuration Kerberos, un fichier de table de clés Kerberos (keytab) et un nom principal Kerberos. Les informations d'identification du principal Kerberos doivent figurer dans le fichier keytab fourni.

Chiffrement

Lorsque vous utilisez l'authentification Kerberos, DataSync prend en charge le chiffrement des données lors de leur transmission entre l' DataSync agent et votre cluster HDFS. Chiffrez vos données en utilisant les paramètres de configuration de qualité de protection (QOP) de votre cluster HDFS et en spécifiant les paramètres QOP lors de la création de votre emplacement HDFS. La configuration QOP inclut les paramètres de protection du transfert de données et de protection RPC (Remote Procedure Call).

DataSync prend en charge les types de chiffrement Kerberos suivants :

- `des-cbc-crc`
- `des-cbc-md4`
- `des-cbc-md5`
- `des3-cbc-sha1`
- `arcfour-hmac`
- `arcfour-hmac-exp`
- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`
- `aes128-cts-hmac-sha256-128`
- `aes256-cts-hmac-sha384-192`
- `camellia128-cts-cmac`
- `camellia256-cts-cmac`

Vous pouvez également configurer des clusters HDFS pour le chiffrement au repos à l'aide du chiffrement transparent des données (TDE). Lors de l'utilisation de l'authentification simple, DataSync lit et écrit sur des clusters compatibles TDE. Si vous utilisez DataSync pour copier des données vers un cluster compatible TDE, configurez d'abord les zones de chiffrement sur le cluster HDFS. DataSync ne crée pas de zones de chiffrement.

Fonctionnalités HDFS non prises en charge

Les fonctionnalités HDFS suivantes ne sont actuellement pas prises en charge par DataSync :

- Chiffrement transparent des données (TDE) lors de l'utilisation de l'authentification Kerberos

- Configuration de plusieurs NameNodes
- Hadoop HDFS sur HTTP (HttpFS)
- listes de contrôle d'accès POSIX () ACLs
- Attributs étendus HDFS (xattrs)
- Clusters HDFS utilisant Apache HBase

Création de votre emplacement de transfert HDFS

Vous pouvez utiliser votre position comme source ou destination pour votre DataSync transfert.

Avant de commencer : vérifiez la connectivité réseau entre votre agent et le cluster Hadoop en procédant comme suit :

- Testez l'accès aux ports TCP répertoriés dansExigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie.
- Testez l'accès entre votre agent local et votre cluster Hadoop. Pour obtenir des instructions, veuillez consulter Vérification de la connexion de votre agent à votre système de stockage.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour le type d'emplacement, choisissez Hadoop Distributed File System (HDFS).

   Vous pouvez configurer cet emplacement comme source ou destination ultérieurement.
4. Pour les agents, choisissez l'agent qui peut se connecter à votre cluster HDFS.

   Vous pouvez choisir plusieurs agents. Pour de plus amples informations, veuillez consulter Utilisation de plusieurs DataSync agents.
5. Pour NameNode, indiquez le nom de domaine ou l'adresse IP du cluster HDFS principal NameNode de votre cluster HDFS.
6. Dans le champ Dossier, entrez le dossier de votre cluster HDFS que vous souhaitez utiliser DataSync pour le transfert de données.

Si votre emplacement HDFS est une source, DataSync copie les fichiers de ce dossier vers la destination. Si votre emplacement est une destination, DataSync écrit des fichiers dans ce dossier.

7. Pour définir la taille du bloc ou le facteur de réplication, sélectionnez Paramètres supplémentaires.

   La taille de bloc par défaut est de 128 MiB. La taille de bloc que vous indiquez doit être un multiple de 512 octets.

   Le facteur de réplication par défaut est de trois DataNodes lors du transfert vers le cluster HDFS.

8. Dans la section Sécurité, choisissez le type d'authentification utilisé sur votre cluster HDFS.

   - Simple — Pour l'utilisateur, spécifiez le nom d'utilisateur avec les autorisations suivantes sur le cluster HDFS (en fonction de votre cas d'utilisation) :
     - Si vous envisagez d'utiliser cet emplacement comme emplacement source, spécifiez un utilisateur disposant uniquement d'autorisations de lecture.
     - Si vous prévoyez d'utiliser cet emplacement comme emplacement de destination, spécifiez un utilisateur disposant d'autorisations de lecture et d'écriture.

     Spécifiez éventuellement l'URI du serveur de gestion des clés (KMS) de votre cluster HDFS.
   - Kerberos — Spécifiez le principal Kerberos ayant accès à votre cluster HDFS. Indiquez ensuite le KeyTabfichier contenant le principal Kerberos fourni. Fournissez ensuite le fichier de configuration Kerberos. Enfin, spécifiez le type de chiffrement pour la protection du transit dans les listes déroulantes Protection RPC et Protection contre le transfert de données.

9. (Facultatif) Choisissez Ajouter une balise pour baliser votre emplacement HDFS.

   Les tags sont des paires clé-valeur qui vous permettent de gérer, de filtrer et de rechercher vos emplacements. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

10. Choisissez Créer un emplacement.

À l'aide du AWS CLI

1. Copiez la `create-location-hdfs` commande suivante.

```
aws datasync create-location-hdfs --name-nodes [{"Hostname":"host1", "Port": 8020}]
 \
    --authentication-type "SIMPLE|KERBEROS" \
    --agent-arns [arn:aws:datasync:us-east-1:123456789012:agent/
agent-01234567890example] \
    --subdirectory "/path/to/my/data"
```

2. Pour le `--name-nodes` paramètre, spécifiez le nom d'hôte ou l'adresse IP du principal de votre cluster HDFS NameNode et le port TCP sur lequel il écoute NameNode .
3. Pour le `--authentication-type` paramètre, spécifiez le type d'authentification à utiliser lors de la connexion au cluster Hadoop. Vous pouvez spécifier `SIMPLE` ou `KERBEROS`.

   Si vous utilisez `SIMPLE` l'authentification, utilisez le `--simple-user` paramètre pour spécifier le nom d'utilisateur de l'utilisateur. Si vous utilisez `KERBEROS` l'authentification, utilisez les `--kerberos-principal` `--kerberos-krb5-conf` paramètres`--kerberos-keytab`, et. Pour de plus amples informations, veuillez consulter create-location-hdfs.
4. Pour le `--agent-arns` paramètre, spécifiez l'ARN de l' DataSync agent qui peut se connecter à votre cluster HDFS.

   Vous pouvez choisir plusieurs agents. Pour de plus amples informations, veuillez consulter Utilisation de plusieurs DataSync agents.
5. (Facultatif) Pour le `--subdirectory` paramètre, spécifiez le dossier de votre cluster HDFS que vous souhaitez utiliser DataSync pour le transfert de données.

   Si votre emplacement HDFS est une source, DataSync copie les fichiers de ce dossier vers la destination. Si votre emplacement est une destination, DataSync écrit des fichiers dans ce dossier.
6. Exécutez la commande `create-location-hdfs`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de l'emplacement que vous avez créé. Par exemple :

```
{
    "arn:aws:datasync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Configuration des DataSync transferts avec un système de stockage d'objets

Vous pouvez ainsi transférer des données entre votre système de stockage d'objets et l'un des services de AWS stockage suivants : AWS DataSync

- Amazon S3
- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Pour configurer ce type de transfert, vous devez créer un emplacement pour votre système de stockage d'objets. Vous pouvez utiliser cet emplacement comme source ou destination de transfert. Le transfert de données vers ou depuis votre stockage d'objets sur site nécessite un DataSync agent.

Prérequis

Votre système de stockage d'objets doit être compatible avec les opérations d'API Amazon S3 suivantes DataSync pour pouvoir vous y connecter :

- `AbortMultipartUpload`
- `CompleteMultipartUpload`
- `CopyObject`
- `CreateMultipartUpload`
- `DeleteObject`
- `DeleteObjects`
- `DeleteObjectTagging`
- `GetBucketLocation`
- `GetObject`
- `GetObjectTagging`
- `HeadBucket`
- `HeadObject`

- `ListObjectsV2`
- `PutObject`
- `PutObjectTagging`
- `UploadPart`

Création de votre lieu de transfert de stockage d'objets

Avant de commencer, vous avez besoin d'un système de stockage d'objets vers ou à partir duquel vous comptez transférer des données.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour Type d'emplacement, choisissez Stockage d'objets.

   Vous configurerez cet emplacement comme source ou destination plus tard.
4. Pour Serveur, indiquez le nom de domaine ou l'adresse IP du serveur de stockage d'objets.
5. Dans le champ Nom du compartiment, entrez le nom du compartiment de stockage d'objets impliqué dans le transfert.
6. Pour Dossier, entrez un préfixe d'objet.

   DataSync copie uniquement les objets portant ce préfixe.
7. Si votre transfert nécessite un agent, choisissez Utiliser des agents, puis choisissez l' DataSync agent qui se connecte à votre système de stockage d'objets.

   Certains transferts ne nécessitent pas d'agents. Dans d'autres scénarios, vous souhaiterez peut-être utiliser plusieurs agents. Pour plus d'informations, consultez Situations dans lesquelles vous n'avez pas besoin d'un DataSync agent et Utilisation de plusieurs DataSync agents.
8. Pour configurer la connexion au serveur de stockage d'objets, développez Paramètres supplémentaires et procédez comme suit :

   a. Pour le protocole du serveur, choisissez HTTP ou HTTPS.
   b. Pour le port du serveur, utilisez un port par défaut (80 pour HTTP ou 443 pour HTTPS) ou spécifiez un port personnalisé si nécessaire.

c. Pour Certificat, si votre système de stockage d'objets utilise une autorité de certification (CA) privée ou autosignée, sélectionnez Choisir un fichier et spécifiez un seul `.pem` fichier avec une chaîne de certificats complète.

La chaîne de certificats peut inclure :

- Le certificat du système de stockage d'objets
- Tous les certificats intermédiaires (s'il y en a)
- Le certificat racine de l'autorité de certification signataire

Vous pouvez concaténer vos certificats dans un `.pem` fichier (dont la taille peut atteindre 32 768 octets avant le codage base64). L'exemple de `cat` commande suivant crée un *`object_storage_certificates`*`.pem` fichier contenant trois certificats :

```
cat object_server_certificate.pem intermediate_certificate.pem ca_root_certificate.pem
 > object_storage_certificates.pem
```

9. Si le serveur de stockage d'objets a besoin d'informations d'identification pour accéder, sélectionnez Requiert des informations d'identification et entrez la clé d'accès que vous utilisez pour accéder au bucket. Entrez ensuite directement la clé secrète ou spécifiez un AWS Secrets Manager secret contenant la clé. Pour plus d'informations, consultez la section Fourniture d'informations d'identification pour les emplacements de stockage.

   La clé d'accès et la clé secrète peuvent être respectivement un nom d'utilisateur et un mot de passe.

10. (Facultatif) Choisissez Ajouter une étiquette pour étiqueter l'emplacement de stockage de vos objets.

    Les tags sont des paires clé-valeur qui vous permettent de gérer, de filtrer et de rechercher vos emplacements. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

11. Choisissez Créer un emplacement.

À l'aide du AWS CLI

1. Copiez la `create-location-object-storage` commande suivante :

```
aws datasync create-location-object-storage \
    --server-hostname object-storage-server.example.com \
    --bucket-name your-bucket \
    --agent-arns arn:aws:datasync:us-east-1:123456789012:agent/
agent-01234567890deadfb
```

2. Spécifiez les paramètres obligatoires suivants dans la commande :

   - `--server-hostname`— Spécifiez le nom de domaine ou l'adresse IP de votre serveur de stockage d'objets.
   - `--bucket-name`— Spécifiez le nom du bucket sur votre serveur de stockage d'objets vers ou depuis lequel vous effectuez le transfert.

3. (Facultatif) Ajoutez l'un des paramètres suivants à la commande :

   - `--agent-arns`— Spécifiez les DataSync agents que vous souhaitez connecter à votre serveur de stockage d'objets.
   - `--server-port`— Spécifie le port sur lequel votre serveur de stockage d'objets accepte le trafic réseau entrant (par exemple, port`443`).
   - `--server-protocol`— Spécifie le protocole (`HTTP`ou`HTTPS`) que votre serveur de stockage d'objets utilise pour communiquer.
   - `--access-key`— Spécifie la clé d'accès (par exemple, un nom d'utilisateur) si des informations d'identification sont requises pour s'authentifier auprès du serveur de stockage d'objets.
   - `--secret-key`— Spécifie la clé secrète (par exemple, un mot de passe) si des informations d'identification sont requises pour s'authentifier auprès du serveur de stockage d'objets.

     Vous pouvez également fournir des paramètres supplémentaires pour sécuriser vos clés à l'aide de AWS Secrets Manager. Pour plus d'informations, consultez la section Fourniture d'informations d'identification pour les emplacements de stockage.
   - `--server-certificate`— Spécifie une chaîne de certificats DataSync pour l'authentification auprès de votre système de stockage d'objets si celui-ci utilise une autorité de certification (CA) privée ou auto-signée. Vous devez spécifier un seul `.pem` fichier avec une chaîne de certificats complète (par exemple,`file:///home/user/.ssh/object_storage_certificates.pem`).

     La chaîne de certificats peut inclure :

- Le certificat du système de stockage d'objets
- Tous les certificats intermédiaires (s'il y en a)
- Le certificat racine de l'autorité de certification signataire

Vous pouvez concaténer vos certificats dans un `.pem` fichier (dont la taille peut atteindre 32 768 octets avant le codage base64). L'exemple de `cat` commande suivant crée un *`object_storage_certificates`*`.pem` fichier contenant trois certificats :

```
cat object_server_certificate.pem intermediate_certificate.pem ca_root_certificate.pem
 > object_storage_certificates.pem
```

- `--subdirectory`— Spécifie le préfixe d'objet pour votre serveur de stockage d'objets.

  DataSync copie uniquement les objets portant ce préfixe.
- `--tags`— Spécifie la paire clé-valeur qui représente une balise que vous souhaitez ajouter à la ressource de localisation.

  Les balises vous aident à gérer, filtrer et rechercher vos ressources. Nous vous recommandons de créer une balise de nom pour votre emplacement.

4. Exécutez la commande `create-location-object-storage`.

   Vous obtenez une réponse qui indique l'ARN de localisation que vous venez de créer.

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-01234567890abcdef"
}
```

Transfert vers ou depuis un AWS espace de stockage avec AWS DataSync

Avec AWS DataSync, vous pouvez transférer des données vers ou depuis un certain nombre de services de AWS stockage. Pour plus d'informations, consultez Où puis-je transférer mes données DataSync ?

Rubriques

- Configuration des AWS DataSync transferts avec Amazon S3

- Configuration des AWS DataSync transferts avec Amazon EFS
- Configuration des transferts avec FSx pour Windows File Server
- Configuration des DataSync transferts avec FSx for Lustre
- Configuration des DataSync transferts avec Amazon FSx pour OpenZFS
- Configuration des transferts avec Amazon FSx pour NetApp ONTAP

Configuration des AWS DataSync transferts avec Amazon S3

Pour transférer des données vers ou depuis votre compartiment Amazon S3, vous devez créer un lieu AWS DataSync de transfert. DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Fournir DataSync un accès aux compartiments S3

DataSync a besoin d'accéder au compartiment S3 vers lequel vous effectuez le transfert ou à partir duquel vous effectuez le transfert. Pour ce faire, vous devez créer un rôle AWS Identity and Access Management (IAM) DataSync doté des autorisations requises pour accéder au bucket. Vous spécifiez ensuite ce rôle lors de la création de votre emplacement Amazon S3 pour DataSync.

Table des matières

- Autorisations requises
- Création d'un rôle IAM pour accéder DataSync à votre position Amazon S3
- Accès aux compartiments S3 à l'aide du chiffrement côté serveur
- Accès aux compartiments S3 restreints
- Accès aux compartiments S3 avec un accès VPC restreint

Autorisations requises

Les autorisations dont votre rôle IAM a besoin peuvent varier selon que le bucket est un emplacement DataSync source ou de destination. Amazon S3 on Outposts nécessite un ensemble d'autorisations différent.

Amazon S3 (source location)

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

```
    "Statement": [
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts"
              ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Amazon S3 (destination location)

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Action": [
             "s3:GetBucketLocation",
             "s3:ListBucket",
             "s3:ListBucketMultipartUploads"
         ],
         "Effect": "Allow",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition": {
             "StringEquals": {
                 "aws:ResourceAccount": "123456789012"
             }
         }
```

```
    },
    {
        "Action": [
            "s3:AbortMultipartUpload",
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:GetObjectTagging",
            "s3:GetObjectVersion",
            "s3:GetObjectVersionTagging",
            "s3:ListMultipartUploadParts",
            "s3:PutObject",
            "s3:PutObjectTagging"
          ],
        "Effect": "Allow",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "123456789012"
            }
        }
    }
 ]
}
```

Amazon S3 on Outposts

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3-outposts:ListBucket",
                "s3-outposts:ListBucketMultipartUploads"
            ],
            "Effect": "Allow",
            "Resource": [
            "arn:aws:s3-outposts:us-east-1:123456789012:outpost/outpost-id/
bucket/amzn-s3-demo-bucket",
    "arn:aws:s3-outposts:us-east-1:123456789012:outpost/outpost-id/
accesspoint/bucket-access-point-name"
            ]
        },
        {
```

```
            "Action": [
                "s3-outposts:AbortMultipartUpload",
                "s3-outposts:DeleteObject",
                "s3-outposts:GetObject",
                "s3-outposts:GetObjectTagging",
                "s3-outposts:GetObjectVersion",
                "s3-outposts:GetObjectVersionTagging",
                "s3-outposts:ListMultipartUploadParts",
                "s3-outposts:PutObject",
                "s3-outposts:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": [
            "arn:aws:s3-outposts:us-east-1:123456789012:outpost/outpost-id/
bucket/amzn-s3-demo-bucket/*",
    "arn:aws:s3-outposts:us-east-1:123456789012:outpost/outpost-id/
accesspoint/bucket-access-point-name/*"
            ]
        },
        {
            "Action": "s3-outposts:GetAccessPoint",
            "Effect": "Allow",
            "Resource": "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/outpost-id/accesspoint/bucket-access-point-name"
        }
    ]
}
```

Création d'un rôle IAM pour accéder DataSync à votre position Amazon S3

Lorsque vous créez votre emplacement Amazon S3 dans la console, DataSync vous pouvez automatiquement créer et assumer un rôle IAM qui dispose normalement des autorisations nécessaires pour accéder à votre compartiment S3.

Dans certains cas, vous devrez peut-être créer ce rôle manuellement (par exemple, pour accéder à des compartiments dotés de niveaux de sécurité supplémentaires ou pour effectuer un transfert vers ou depuis un compartiment situé dans un autre Comptes AWS).

Création manuelle d'un rôle IAM pour DataSync

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.

2. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles, puis sélectionnez Créer un rôle.
3. Sur la page Sélectionner une entité de confiance, pour Type d'entité fiable, sélectionnez Service AWS.
4. Pour Cas d'utilisation, choisissez DataSyncdans la liste déroulante et sélectionnez DataSync. Choisissez Suivant.
5. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant). Donnez un nom à votre rôle et choisissez Créer un rôle.
6. Sur la page Rôles, recherchez le rôle que vous venez de créer et choisissez son nom.
7. Sur la page de détails du rôle, choisissez l'onglet Autorisations. Choisissez Ajouter des autorisations, puis Créer une politique en ligne.
8. Choisissez l'onglet JSON et ajoutez les autorisations requises pour accéder à votre bucket dans l'éditeur de politiques.
9. Choisissez Suivant. Donnez un nom à votre politique et choisissez Create policy.
10. (Recommandé) Pour éviter le problème de confusion entre les services adjoints, procédez comme suit :

    a. Sur la page de détails du rôle, choisissez l'onglet Relations de confiance. Choisissez Edit trust policy (Modifier la politique d'approbation).

    b. Mettez à jour la politique de confiance en utilisant l'exemple suivant, qui inclut les clés de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale :

    JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
            "Service": "datasync.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
            "aws:SourceAccount": "444455556666"
            },
```

```
                "ArnLike": {
                "aws:SourceArn": "arn:aws:datasync:us-east-1:444455556666:*"
                }
            }
        }
    ]
}
```

c. Choisissez Mettre à jour une politique.

Vous pouvez spécifier ce rôle lors de la création de votre site Amazon S3.

Accès aux compartiments S3 à l'aide du chiffrement côté serveur

DataSync peut transférer des données vers ou depuis des compartiments S3 qui utilisent le chiffrement côté serveur. Le type de clé de chiffrement utilisé par un bucket peut déterminer si vous avez besoin d'une politique personnalisée DataSync permettant d'accéder au bucket.

Lorsque vous utilisez DataSync des compartiments S3 qui utilisent le chiffrement côté serveur, gardez à l'esprit les points suivants :

- Si votre compartiment S3 est chiffré à l'aide d'une clé AWS gérée, vous DataSync pouvez accéder aux objets du compartiment par défaut si toutes vos ressources sont identiques Compte AWS.
- Si votre compartiment S3 est chiffré à l'aide d'une clé gérée par le client AWS Key Management Service (AWS KMS) (SSE-KMS), la politique de la clé doit inclure le rôle IAM DataSync utilisé pour accéder au compartiment.
- Si votre compartiment S3 est chiffré avec une clé SSE-KMS gérée par le client et dans une autre, vous Compte AWS devez obtenir DataSync l'autorisation d'accéder au compartiment dans l'autre. Compte AWS Vous pouvez le configurer en procédant comme suit :
  - Dans le rôle IAM qui l' DataSync utilise, vous devez spécifier la clé SSE-KMS du compartiment multi-comptes en utilisant le nom de ressource Amazon (ARN) complet de la clé. Il s'agit du même ARN de clé que celui que vous utilisez pour configurer le chiffrement par défaut du compartiment. Vous ne pouvez pas spécifier d'ID de clé, de nom d'alias ou d'ARN d'alias dans ce cas.

    Voici un exemple d'ARN clé :

    ```
    arn:aws:kms:us-
    west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
    ```

Pour plus d'informations sur la spécification des clés KMS dans les déclarations de politique IAM, consultez le manuel du AWS Key Management Service développeur.

- Dans la politique clé SSE-KMS, spécifiez le rôle IAM utilisé par. DataSync

- Si votre compartiment S3 est chiffré à l'aide d'une AWS KMS clé gérée par le client (DSSE-KMS) pour un chiffrement double couche côté serveur, la politique de la clé doit inclure le rôle IAM utilisé pour accéder au compartiment. DataSync (N'oubliez pas que le DSSE-KMS ne prend pas en charge les clés de compartiment S3, ce qui peut réduire les coûts liés aux AWS KMS demandes.)
- Si votre compartiment S3 est chiffré à l'aide d'une clé de chiffrement fournie par le client (SSE-C), DataSync vous ne pouvez pas accéder à ce compartiment.

Exemple : politique clé SSE-KMS pour DataSync

L'exemple suivant est une politique clé pour une clé SSE-KMS gérée par le client. La politique est associée à un compartiment S3 qui utilise le chiffrement côté serveur.

Si vous souhaitez utiliser cet exemple, remplacez les valeurs suivantes par les vôtres :

- *account-id*— Votre Compte AWS.
- *admin-role-name*— Le nom du rôle IAM qui peut administrer la clé.
- *datasync-role-name*— Le nom du rôle IAM qui permet d' DataSync utiliser la clé pour accéder au bucket.

JSON

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
```

```
        {
            "Sid": "Allow access for Key Administrators",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/admin-role-name"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:TagResource",
                "kms:UntagResource",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/datasync-role-name"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Accès aux compartiments S3 restreints

Si vous devez effectuer un transfert vers ou depuis un compartiment S3 qui refuse généralement tout accès, vous pouvez modifier la politique du compartiment afin de ne DataSync pouvoir accéder au compartiment que pour votre transfert.

Exemple : Autoriser l'accès en fonction des rôles IAM

1. Copiez la politique de compartiment S3 suivante.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "Deny-access-to-bucket",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "StringNotLike": {
                "aws:userid": [
                    "datasync-iam-role-id:*",
                    "your-iam-role-id"
                ]
            }
        }
    }]
}
```

2. Dans la politique, remplacez les valeurs suivantes :

   - *amzn-s3-demo-bucket*— Spécifiez le nom du compartiment S3 restreint.
   - *datasync-iam-role-id*— Spécifiez l'ID du rôle IAM DataSync utilisé pour accéder au bucket.

     Exécutez la AWS CLI commande suivante pour obtenir l'ID du rôle IAM :

```
aws iam get-role --role-name datasync-iam-role-name
```

Dans le résultat, recherchez la `RoleId` valeur :

```
"RoleId": "ANPAJ2UCCR6DPCEXAMPLE"
```

- *your-iam-role-id*— Spécifiez l'ID du rôle IAM que vous utilisez pour créer l' DataSync emplacement du bucket.

  Exécutez la commande suivante pour obtenir l'ID du rôle IAM :

  ```
  aws iam get-role --role-name your-iam-role-name
  ```

  Dans le résultat, recherchez la `RoleId` valeur :

  ```
  "RoleId": "AIDACKCEVSQ6C2EXAMPLE"
  ```

3. Ajoutez cette politique à votre politique de compartiment S3.
4. Lorsque vous avez terminé DataSync d'utiliser le bucket restreint, supprimez les conditions relatives aux deux rôles IAM de la politique du bucket.

Accès aux compartiments S3 avec un accès VPC restreint

Un compartiment Amazon S3 qui limite l'accès à des points de terminaison de cloud privé virtuel (VPC) spécifiques ou VPCs qui refuse le transfert vers ou DataSync depuis ce compartiment. Pour activer les transferts dans ces situations, vous pouvez mettre à jour la politique du compartiment afin d'inclure le rôle IAM que vous spécifiez en fonction de votre DataSync position.

Option 1: Allowing access based on DataSync location role ARN

Dans la politique du compartiment S3, vous pouvez spécifier le nom de ressource Amazon (ARN) de votre rôle IAM de DataSync localisation.

L'exemple suivant est une politique de compartiment S3 qui refuse l'accès à tous sauf deux VPCs (`vpc-1234567890abcdef0`et`vpc-abcdef01234567890`). Toutefois, la politique inclut également la ArnNotLikeIfExistscondition et la clé aws : PrincipalArn condition, qui permettent à l'ARN d'un rôle de DataSync localisation d'accéder au compartiment.

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

```
    "Statement": [
        {
            "Sid": "Access-to-specific-VPCs-only",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": [
                        "vpc-1234567890abcdef0",
                        "vpc-abcdef01234567890"
                    ]
                },
                "ArnNotLikeIfExists": {
                    "aws:PrprincipalArn": [
                        "arn:aws:iam::111122223333:role/datasync-location-role-
name"
                    ]
                }
            }
        }
    ]
}
```

Option 2: Allowing access based on DataSync location role tag

Dans la politique du compartiment S3, vous pouvez spécifier une balise associée à votre rôle IAM de DataSync localisation.

L'exemple suivant est une politique de compartiment S3 qui refuse l'accès à tous sauf deux VPCs (`vpc-1234567890abcdef0`et`vpc-abcdef01234567890`). Cependant, la politique inclut également les clés StringNotEqualsIfExistscondition et aws : PrincipalTag condition, qui autorisent un mandant à avoir le tag key `exclude-from-vpc-restriction` et valuetrue. Vous pouvez essayer une approche similaire dans votre politique de compartiment en spécifiant une balise associée à votre rôle de DataSync localisation.

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

```
            "Sid": "Access-to-specific-VPCs-only",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": [
                        "vpc-1234567890abcdef0",
                        "vpc-abcdef01234567890"
                    ],
                    "aws:PrincipalTag/exclude-from-vpc-restriction": "true"
                }
            }
        }
    ]
}
```

Considérations relatives à la classe de stockage lors des transferts Amazon S3

Lorsque Amazon S3 est votre destination, DataSync vous pouvez transférer vos données directement vers une classe de stockage Amazon S3 spécifique.

Certaines classes de stockage ont des comportements qui peuvent avoir une incidence sur les coûts de stockage de votre Amazon S3. Lorsque vous utilisez des classes de stockage susceptibles d'entraîner des frais supplémentaires pour le remplacement, la suppression ou la récupération d'objets, les modifications apportées aux données ou aux métadonnées des objets entraînent de tels frais. Pour plus d'informations, consultez Tarification Amazon S3.

> **Important**
>
> Les nouveaux objets transférés vers votre emplacement de destination Amazon S3 sont stockés à l'aide de la classe de stockage que vous spécifiez lors de la création de votre emplacement.
> Par défaut, DataSync préserve la classe de stockage des objets existants dans votre emplacement de destination, sauf si vous configurez votre tâche pour transférer toutes les données. Dans ces situations, la classe de stockage que vous spécifiez lors de la création de votre position est utilisée pour tous les objets.

Classe de stockage Amazon S3	Considérations
S3 Standard	Choisissez S3 Standard pour stocker vos fichiers fréquemment consultés de manière redondante dans plusieurs zones de disponibilité séparées géographiquement. Il s'agit de la valeur par défaut si vous ne spécifiez pas de classe de stockage.
S3 Intelligent-Tiering	Choisissez S3 Intelligent-Tiering (Hiérarchisation intelligente S3) pour optimiser les coûts de stockage en transférant automatiquement les données vers le niveau d'accès de stockage le plus économique. Vous payez des frais mensuels par objet stocké dans la classe de stockage S3 Intelligent-Tiering. Ces frais Amazon S3 incluent la surveilla nce des modèles d'accès aux données et le déplacement d'objets entre les niveaux.
S3 standard – Accès peu fréquent	Choisissez S3 Standard-IA pour stocker de manière redondante vos objets rarement consultés dans plusieurs zones de disponibilité séparées géographiquement. Les objets stockés dans la classe de stockage S3 Standard-IA peuvent entraîner des frais supplémentaires pour le remplacement, la suppressi on ou la récupération. Prenez en compte la fréquence de changement de ces objets, la durée pendant laquelle vous prévoyez de les conserver et la fréquence à laquelle vous devez y accéder. Les modifications apportées aux données ou aux métadonnées d'un objet équivalent à la suppression d'un objet et à la création d'un nouvel objet pour le remplacer. Cela entraîne des frais supplémentaires pour les objets stockés dans la classe de stockage S3 Standard-IA. Les objets de moins de 128 Ko sont inférieurs à la capacité minimale facturée par objet dans la classe de stockage S3 Standard-IA. Ces objets sont stockés dans la classe de stockage S3 Standard.
S3 One Zone-IA	Choisissez S3 One Zone-IA pour stocker vos objets rarement consultés dans une seule zone de disponibilité.

Classe de stockage Amazon S3	Considérations
	Les objets stockés dans la classe de stockage S3 One Zone-IA peuvent entraîner des frais supplémentaires pour le remplacement, la suppressi on ou la récupération. Prenez en compte la fréquence de changement de ces objets, la durée pendant laquelle vous prévoyez de les conserver et la fréquence à laquelle vous devez y accéder. Les modifications apportées aux données ou aux métadonnées d'un objet équivalent à la suppression d'un objet et à la création d'un nouvel objet pour le remplacer. Cela entraîne des frais supplémentaires pour les objets stockés dans la classe de stockage S3 One Zone-IA. Les objets de moins de 128 Ko sont inférieurs à la capacité minimale facturée par objet dans la classe de stockage S3 One Zone-IA. Ces objets sont stockés dans la classe de stockage S3 Standard.

Classe de stockage Amazon S3	Considérations
S3 Glacier Instant Retrieval	Choisissez S3 Glacier Instant Retrieval pour archiver des objets rarement consultés mais nécessitant une extraction en quelques millisecondes. Les données stockées dans la classe de stockage S3 Glacier Instant Retrieval permettent de réaliser des économies par rapport à la classe de stockage S3 Standard-IA avec les mêmes performances de latence et de débit. S3 Glacier Instant Retrieval a cependant des coûts d'accès aux données plus élevés que S3 Standard-IA. Les objets stockés dans S3 Glacier Instant Retrieval peuvent entraîner des frais supplémentaires en cas de remplacement, de suppression ou de récupération. Prenez en compte la fréquence de changement de ces objets, la durée pendant laquelle vous prévoyez de les conserver et la fréquence à laquelle vous devez y accéder. Les modifications apportées aux données ou aux métadonnées d'un objet équivalent à la suppressi on d'un objet et à la création d'un nouvel objet pour le remplacer. Cela entraîne des frais supplémentaires pour les objets stockés dans la classe de stockage S3 Glacier Instant Retrieval. Les objets de moins de 128 Ko sont inférieurs à la capacité minimale facturée par objet dans la classe de stockage S3 Glacier Instant Retrieval. Ces objets sont stockés dans la classe de stockage S3 Standard.

Classe de stockage Amazon S3	Considérations
S3 Glacier Flexible Retri	Choisissez S3 Glacier Flexible Retrieval pour des archives plus actives. Les objets stockés dans S3 Glacier Flexible Retrieval peuvent entraîner des frais supplémentaires en cas de remplacement, de suppression ou de récupération. Prenez en compte la fréquence de changement de ces objets, la durée pendant laquelle vous prévoyez de les conserver et la fréquence à laquelle vous devez y accéder. Les modifications apportées aux données ou aux métadonnées d'un objet équivalent à la suppressi on d'un objet et à la création d'un nouvel objet pour le remplacer. Cela entraîne des frais supplémentaires pour les objets stockés dans la classe de stockage S3 Glacier Flexible Retrieval. La classe de stockage S3 Glacier Flexible Retrieval nécessite 40 Ko de métadonnées supplémentaires pour chaque objet archivé. DataSync place les objets dont la taille est inférieure à 40 Ko dans la classe de stockage S3 Standard. Vous devez restaurer les objets archivés dans cette classe de stockage avant de DataSync pouvoir les lire. Pour plus d'informations, consultez la section Travailler avec des objets archivés dans le guide de l'utilisa teur Amazon S3. Lorsque vous utilisez S3 Glacier Flexible Retrieval, choisissez l'option Vérifier uniquement les données transférées pour comparer les sommes de contrôle des données et des métadonnées à la fin du transfert. Vous ne pouvez pas utiliser l'option Vérifier toutes les données dans la destination pour cette classe de stockage car elle nécessite de récupérer tous les objets existants depuis la destination.

Classe de stockage Amazon S3	Considérations
S3 Glacier Deep Archive	Choisissez S3 Glacier Deep Archive pour archiver vos objets afin de les conserver à long terme et de les conserver sous forme numérique lorsque les données sont consultées une ou deux fois par an. Les objets stockés dans S3 Glacier Deep Archive peuvent entraîner des frais supplémentaires en cas de remplacement, de suppression ou de récupération. Prenez en compte la fréquence de changement de ces objets, la durée pendant laquelle vous prévoyez de les conserver et la fréquence à laquelle vous devez y accéder. Les modifications apportées aux données ou aux métadonnées d'un objet équivalent à la suppressi on d'un objet et à la création d'un nouvel objet pour le remplacer. Cela entraîne des frais supplémentaires pour les objets stockés dans la classe de stockage S3 Glacier Deep Archive. La classe de stockage S3 Glacier Deep Archive nécessite 40 Ko de métadonnées supplémentaires pour chaque objet archivé. DataSync place les objets dont la taille est inférieure à 40 Ko dans la classe de stockage S3 Standard. Vous devez restaurer les objets archivés dans cette classe de stockage avant de DataSync pouvoir les lire. Pour plus d'informations, consultez la section Travailler avec des objets archivés dans le guide de l'utilisa teur Amazon S3. Lorsque vous utilisez S3 Glacier Deep Archive, choisissez l'option Vérifier uniquement les données transférées pour comparer les sommes de contrôle des données et des métadonnées à la fin du transfert. Vous ne pouvez pas utiliser l'option Vérifier toutes les données dans la destination pour cette classe de stockage car elle nécessite de récupérer tous les objets existants depuis la destination.
S3 Outposts	Classe de stockage pour Amazon S3 on Outposts.

Évaluation des coûts des requêtes S3 lors de l'utilisation DataSync

Avec les sites Amazon S3, vous devez supporter des coûts liés aux demandes d'API S3 effectuées par DataSync. Cette section peut vous aider à comprendre comment ces demandes sont DataSync utilisées et comment elles peuvent affecter vos coûts Amazon S3.

Rubriques

- Demandes S3 effectuées par DataSync
- Considérations de coût

Demandes S3 effectuées par DataSync

Le tableau suivant décrit les demandes S3 que vous DataSync pouvez effectuer lorsque vous copiez des données depuis ou vers un emplacement Amazon S3.

Requête S3	Comment DataSync l'utilise
ListObjectV2	DataSync fait au moins une `LIST` demande pour chaque objet se terminant par une barre oblique (`/`) afin de répertorier les objets commençant par ce préfixe. Cette demande est appelée pendant la phase de préparation d'une tâche.
HeadObject	DataSync fait `HEAD` des demandes pour récupérer les métadonnées des objets pendant les phases de préparation et de vérification d'une tâche. Il peut y avoir plusieurs `HEAD` demandes par objet en fonction de la manière dont vous DataSync souhaitez vérifier l'intégrité des données transférées.
GetObject	DataSync fait `GET` des demandes pour lire les données d'un objet pendant la phase de transfert d'une tâche. Il peut y avoir plusieurs `GET` demandes pour des objets de grande taille.

Requête S3	Comment DataSync l'utilise
GetObjectTagging	Si vous configurez votre tâche pour copier des balises d'objet, DataSync envoyez ces `GET` demandes pour vérifier la présence de balises d'objet pendant les phases de préparation et de transfert de la tâche.
PutObject	DataSync fait des `PUT` demandes pour créer des objets et des préfixes dans un compartim ent S3 de destination pendant la phase de transfert d'une tâche. Comme il DataSync utilise la fonctionnalité de téléchargement partitionné d'Amazon S3, il peut y avoir plusieurs `PUT` demandes pour des objets volumineux. Pour minimiser les coûts de stockage, nous vous recommandons d'utiliser une configuration de cycle de vie pour arrêter les téléchargements partitionnés incomplets.
PutObjectTagging	Si vos objets source comportent des balises et que vous configurez votre tâche pour copier les balises des objets, DataSync effectuez ces `PUT` demandes lors du transfert de ces balises.
CopyObject	DataSync fait une `COPY` demande pour créer une copie d'un objet uniquement si les métadonnées de cet objet changent. Cela peut se produire si vous avez initialement copié des données dans le compartiment S3 à l'aide d'un autre service ou outil qui n'a pas transféré ses métadonnées.

Considérations de coût

DataSync effectue des requêtes S3 sur des compartiments S3 à chaque fois que vous exécutez votre tâche. Cela peut entraîner une augmentation des frais dans certaines situations. Par exemple :

- Vous transférez fréquemment des objets vers ou depuis un compartiment S3.
- Vous ne transférez peut-être pas beaucoup de données, mais votre compartiment S3 contient de nombreux objets. Vous pouvez toujours constater des frais élevés dans ce scénario, car DataSync il envoie des requêtes S3 sur chacun des objets du compartiment.
- Vous effectuez un transfert entre des compartiments S3, tout comme vous DataSync envoyez des requêtes S3 sur la source et la destination.

Pour aider à minimiser les coûts liés aux demandes S3 DataSync, tenez compte des points suivants :

Rubriques

- Quelles sont les classes de stockage S3 que j'utilise ?
- À quelle fréquence dois-je transférer mes données ?

Quelles sont les classes de stockage S3 que j'utilise ?

Les frais de demande S3 peuvent varier en fonction de la classe de stockage Amazon S3 utilisée par vos objets, en particulier pour les classes qui archivent des objets (telles que S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive).

Voici quelques scénarios dans lesquels les classes de stockage peuvent affecter les frais de vos demandes S3 lors de l'utilisation de DataSync :

- Chaque fois que vous exécutez une tâche, vous envoyez DataSync des `HEAD` demandes pour récupérer les métadonnées de l'objet. Ces demandes entraînent des frais même si vous ne déplacez aucun objet. L'impact de ces demandes sur votre facture dépend de la classe de stockage utilisée par vos objets et du nombre d'objets DataSync numérisés.
- Si vous avez déplacé des objets vers la classe de stockage S3 Glacier Instant Retrieval (soit directement, soit par le biais d'une configuration du cycle de vie des compartiments), les demandes sur les objets de cette classe sont plus coûteuses que les objets des autres classes de stockage.
- Si vous configurez votre DataSync tâche pour vérifier que vos emplacements source et de destination sont entièrement synchronisés, des `GET` demandes seront envoyées pour chaque objet dans toutes les classes de stockage (à l'exception de S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive).
- Outre les `GET` demandes, vous devez payer des frais de récupération de données pour les objets de la classe de stockage S3 Standard-IA, S3 One Zone-IA ou S3 Glacier Instant Retrieval.

Pour plus d'informations, consultez Tarification Amazon S3.

À quelle fréquence dois-je transférer mes données ?

Si vous devez déplacer des données de manière récurrente, pensez à un calendrier qui n'exécute pas plus de tâches que nécessaire.

Vous pouvez également envisager de limiter l'étendue de vos transferts. Par exemple, vous pouvez configurer DataSync pour vous concentrer sur les objets dans certains préfixes ou filtrer les données transférées. Ces options peuvent contribuer à réduire le nombre de demandes S3 effectuées chaque fois que vous exécutez votre DataSync tâche.

Considérations relatives aux objets lors des transferts Amazon S3

- Si vous effectuez un transfert depuis un compartiment S3, utilisez S3 Storage Lens pour déterminer le nombre d'objets que vous déplacez.
- Lorsque vous effectuez un transfert entre des compartiments S3, nous vous recommandons d'utiliser le mode tâche amélioré, car vous n'êtes pas soumis à des quotas de DataSync tâches.
- DataSync risque de ne pas transférer un objet dont le nom contient des caractères non standard. Pour plus d'informations, consultez les directives de dénomination des clés d'objet dans le guide de l'utilisateur Amazon S3.
- Lorsque vous utilisez DataSync un compartiment S3 qui utilise le versionnement, n'oubliez pas ce qui suit :
  - Lors du transfert vers un compartiment S3, DataSync crée une nouvelle version d'un objet si celui-ci est modifié à la source. Cela entraîne des frais supplémentaires.
  - La version d'un objet est différente IDs dans les compartiments source et de destination.
- Après avoir initialement transféré des données d'un compartiment S3 vers un système de fichiers (par exemple, NFS ou Amazon FSx), les exécutions suivantes de la même DataSync tâche n'incluront pas les objets qui ont été modifiés mais qui ont la même taille que lors du premier transfert.

Création de votre lieu de transfert pour un compartiment Amazon S3 à usage général

Pour créer un emplacement pour votre transfert, vous avez besoin d'un compartiment S3 à usage général existant. Si vous n'en avez pas, consultez le guide de l'utilisateur Amazon S3.

> **Important**
>
> Avant de créer votre position, assurez-vous de lire les sections suivantes :
>
> - Considérations relatives à la classe de stockage lors des transferts Amazon S3
> - Évaluation des coûts des requêtes S3 lors de l'utilisation DataSync

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour le type d'emplacement, choisissez Amazon S3, puis choisissez General Purpose bucket.
4. Pour l'URI S3, entrez ou choisissez le compartiment et le préfixe que vous souhaitez utiliser pour votre position.

   > **Warning**
   >
   > DataSync Impossible de transférer des objets dont le préfixe commence par une barre oblique (/) ou inclut `///./`, ou `/../` des motifs. Par exemple :
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`

5. Pour la classe de stockage S3 utilisée comme destination, choisissez la classe de stockage que vous souhaitez que vos objets utilisent lorsque Amazon S3 est une destination de transfert.

   Pour de plus amples informations, veuillez consulter Considérations relatives à la classe de stockage lors des transferts Amazon S3.
6. Pour IAM role (Rôle IAM), effectuez l'une des opérations suivantes :

   - Choisissez Autogenerate pour DataSync créer automatiquement un rôle IAM avec les autorisations requises pour accéder au compartiment S3.

Si un rôle IAM a DataSync déjà été créé pour ce compartiment S3, ce rôle est choisi par défaut.

- Choisissez un rôle IAM personnalisé que vous avez créé. Pour de plus amples informations, veuillez consulter Création d'un rôle IAM pour accéder DataSync à votre position Amazon S3.

7. (Facultatif) Choisissez Ajouter une nouvelle balise pour étiqueter votre position Amazon S3.

   Les balises vous aident à gérer, filtrer et rechercher vos ressources. Nous vous recommandons de créer une balise de nom pour votre emplacement.

8. Choisissez Créer un emplacement.

En utilisant le AWS CLI

1. Copiez la `create-location-s3` commande suivante :

```
aws datasync create-location-s3 \
    --s3-bucket-arn 'arn:aws:s3:::amzn-s3-demo-bucket' \
    --s3-storage-class 'your-S3-storage-class' \
    --s3-config 'BucketAccessRoleArn=arn:aws:iam::account-id:role/role-allowing-
datasync-operations' \
    --subdirectory /your-prefix-name
```

2. Pour`--s3-bucket-arn`, spécifiez l'ARN du compartiment S3 que vous souhaitez utiliser comme emplacement.
3. Pour`--s3-storage-class`, spécifiez la classe de stockage que vous souhaitez que vos objets utilisent lorsque Amazon S3 est une destination de transfert.
4. Pour`--s3-config`, spécifiez l'ARN du rôle IAM qui DataSync doit accéder à votre bucket.

   Pour de plus amples informations, veuillez consulter Création d'un rôle IAM pour accéder DataSync à votre position Amazon S3.

5. Pour`--subdirectory`, spécifiez un préfixe dans le compartiment S3 qui DataSync lit depuis ou vers lequel il écrit (selon que le compartiment est un emplacement source ou de destination).

   > **Warning**
   >
   > DataSync Impossible de transférer des objets dont le préfixe commence par une barre oblique (`/`) ou inclut `///./`, ou `/../` des motifs. Par exemple :

- /photos
- photos//2006/January
- photos/./2006/February
- photos/../2006/March

6. Exécutez la commande `create-location-s3`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de l'emplacement que vous avez créé. Par exemple :

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Vous pouvez utiliser cet emplacement comme source ou destination pour votre DataSync tâche.

Création de votre lieu de transfert pour un bucket S3 on Outposts

Pour créer un emplacement pour votre transfert, vous avez besoin d'un bucket Amazon S3 on Outposts existant. Si vous n'en avez pas, consultez le guide de l'utilisateur d'Amazon S3 on Outposts.

Vous avez également besoin d'un DataSync agent. Pour de plus amples informations, veuillez consulter Déploiement de votre agent sur AWS Outposts.

Lorsque vous effectuez un transfert depuis un préfixe de compartiment S3 on Outposts contenant un ensemble de données volumineux (par exemple des centaines de milliers ou des millions d'objets), votre DataSync tâche peut expirer. Pour éviter cela, pensez à utiliser un DataSync manifeste, qui vous permet de spécifier les objets exacts que vous devez transférer.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour le type d'emplacement, choisissez Amazon S3, puis choisissez Outposts bucket.

4. Pour le compartiment S3, choisissez un point d'accès Amazon S3 qui peut accéder à votre compartiment S3 on Outposts.

   Pour plus d'informations, consultez le guide de l'utilisateur Amazon S3.

5. Pour la classe de stockage S3 utilisée comme destination, choisissez la classe de stockage que vous souhaitez que vos objets utilisent lorsque Amazon S3 est une destination de transfert.

   Pour plus d'informations, consultezConsidérations relatives à la classe de stockage lors des transferts Amazon S3. DataSync utilise par défaut la classe de stockage S3 Outposts pour Amazon S3 on Outposts.

6. Pour les agents, spécifiez le nom de ressource Amazon (ARN) de l' DataSync agent de votre Outpost.

7. Pour Dossier, entrez un préfixe dans le compartiment S3 qui DataSync lit ou écrit dans le compartiment (selon que le compartiment est un emplacement source ou de destination).

   > **Warning**
   >
   > DataSync Impossible de transférer des objets dont le préfixe commence par une barre oblique (`/`) ou inclut `///./`, ou `/../` des motifs. Par exemple :
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`

8. Pour IAM role (Rôle IAM), effectuez l'une des opérations suivantes :

   - Choisissez Autogenerate pour DataSync créer automatiquement un rôle IAM avec les autorisations requises pour accéder au compartiment S3.

     Si un rôle IAM a DataSync déjà été créé pour ce compartiment S3, ce rôle est choisi par défaut.

   - Choisissez un rôle IAM personnalisé que vous avez créé. Pour de plus amples informations, veuillez consulter Création d'un rôle IAM pour accéder DataSync à votre position Amazon S3.

9. (Facultatif) Choisissez Ajouter une nouvelle balise pour étiqueter votre position Amazon S3.

Les balises vous aident à gérer, filtrer et rechercher vos ressources. Nous vous recommandons de créer une balise de nom pour votre emplacement.

10. Choisissez Créer un emplacement.

En utilisant le AWS CLI

1. Copiez la `create-location-s3` commande suivante :

```
aws datasync create-location-s3 \
    --s3-bucket-arn 'bucket-access-point' \
    --s3-storage-class 'your-S3-storage-class' \
    --s3-config 'BucketAccessRoleArn=arn:aws:iam::account-id:role/role-allowing-
datasync-operations' \
    --subdirectory /your-folder \
    --agent-arns 'arn:aws:datasync:your-region:account-id::agent/agent-agent-id'
```

2. Pour`--s3-bucket-arn`, spécifiez l'ARN d'un point d'accès Amazon S3 qui peut accéder à votre compartiment S3 on Outposts.

   Pour plus d'informations, consultez le guide de l'utilisateur Amazon S3.

3. Pour`--s3-storage-class`, spécifiez la classe de stockage que vous souhaitez que vos objets utilisent lorsque Amazon S3 est une destination de transfert.

   Pour plus d'informations, consultezConsidérations relatives à la classe de stockage lors des transferts Amazon S3. DataSync utilise par défaut la classe de stockage S3 Outposts pour S3 on Outposts.

4. Pour`--s3-config`, spécifiez l'ARN du rôle IAM qui DataSync doit accéder à votre bucket.

   Pour de plus amples informations, veuillez consulter Création d'un rôle IAM pour accéder DataSync à votre position Amazon S3.

5. Pour`--subdirectory`, spécifiez un préfixe dans le compartiment S3 qui DataSync lit depuis ou vers lequel il écrit (selon que le compartiment est un emplacement source ou de destination).

   > **Warning**
   >
   > DataSync Impossible de transférer des objets dont le préfixe commence par une barre oblique (`/`) ou inclut `///./`, ou `/../` des motifs. Par exemple :

- /photos
- photos//2006/January
- photos/./2006/February
- photos/../2006/March

6. Pour`--agent-arns`, spécifiez l'ARN de l' DataSync agent sur votre avant-poste.
7. Exécutez la commande `create-location-s3`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de l'emplacement que vous avez créé. Par exemple :

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Vous pouvez utiliser cet emplacement comme source ou destination pour votre DataSync tâche.

Amazon S3 effectue des transferts entre Comptes AWS

Avec DataSync, vous pouvez déplacer des données vers ou depuis des compartiments S3 de différentes Comptes AWS manières. Pour plus d'informations, consultez les didacticiels suivants :

- Transfert de données depuis le stockage sur site vers Amazon S3 via Comptes AWS
- Transfert de données d'Amazon S3 vers Amazon S3 via Comptes AWS

Amazon S3 effectue des transferts entre des sites commerciaux et AWS GovCloud (US) Regions

Par défaut, DataSync n'est pas transféré entre les compartiments S3 dans les environnements commerciaux et AWS GovCloud (US) Regions. Vous pouvez toutefois configurer ce type de transfert en créant un emplacement de stockage d'objets pour l'un des compartiments S3 de votre transfert. Vous pouvez effectuer ce type de transfert avec ou sans agent. Si vous utilisez un agent, votre tâche doit être configurée pour le mode de base. Pour effectuer un transfert sans agent, vous devez utiliser le mode amélioré.

Avant de commencer : assurez-vous de bien comprendre les implications financières du transfert entre les régions. Pour plus d'informations, consultez Tarification d'AWS DataSync.

Table des matières

- Fournir un DataSync accès au bucket de votre emplacement de stockage d'objets
- Création de votre DataSync agent (facultatif)
- Création d'un emplacement de stockage d'objets pour votre compartiment S3

Fournir un DataSync accès au bucket de votre emplacement de stockage d'objets

Lorsque vous créez l'emplacement de stockage d'objets pour ce transfert, vous devez fournir DataSync les informations d'identification d'un utilisateur IAM autorisé à accéder au compartiment S3 de l'emplacement. Pour de plus amples informations, veuillez consulter Autorisations requises.

> **Warning**
>
> Les utilisateurs IAM disposent d'informations d'identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu'elles ne sont plus nécessaires.

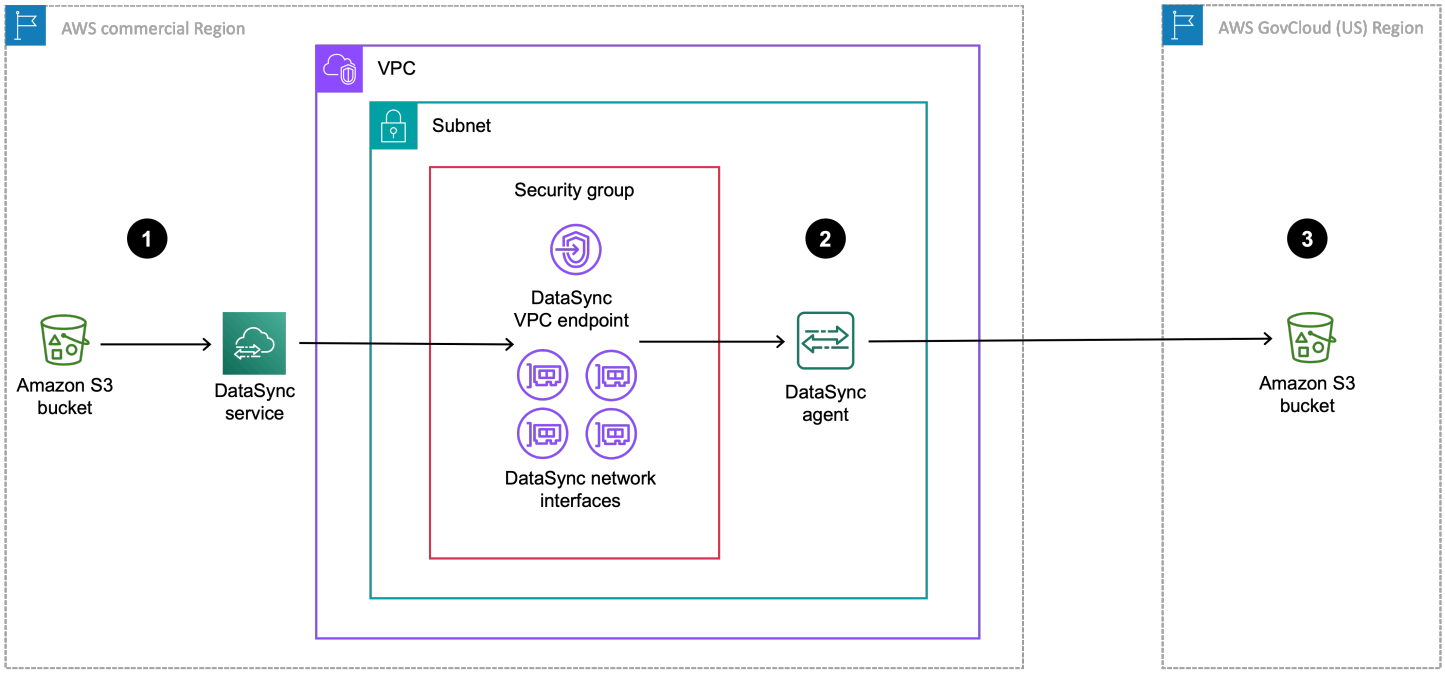
Création de votre DataSync agent (facultatif)

Si vous souhaitez effectuer votre transfert en mode Basic, vous devez utiliser un agent. Dans la mesure où vous passez d'une version commerciale à une instance Amazon AWS GovCloud (US) Region, vous déployez votre DataSync agent en tant qu' EC2 instance Amazon dans l'une des régions. Nous recommandons à votre agent d'utiliser un point de terminaison de service VPC pour éviter les frais de transfert de données vers l'Internet public. Pour plus d'informations, consultez les tarifs d'Amazon EC2 Data Transfer.

Choisissez l'un des scénarios suivants qui décrivent comment créer un agent en fonction de la région dans laquelle vous prévoyez d'exécuter votre DataSync tâche.

Lors de l'exécution d'une DataSync tâche dans une région commerciale

Le schéma suivant montre un transfert où votre DataSync tâche et votre agent se trouvent dans la région commerciale.



Référence	Description
1	Dans la région commerciale dans laquelle vous exécutez une DataSync tâche, les données sont transférées depuis le compartiment S3 source. Le compartiment source est configuré comme un emplacement Amazon S3 dans la région commercia le.
2	Les données sont transférées via l' DataSync agent, qui se trouve dans le même VPC et le même sous-réseau où se trouvent le point de terminaison du service VPC et les interfaces réseau.
3	Transferts de données vers le compartiment S3 de destinati on dans le AWS GovCloud (US) Region. Le compartiment de destination est configuré comme emplacement de stockage d'objets dans la région commerciale.

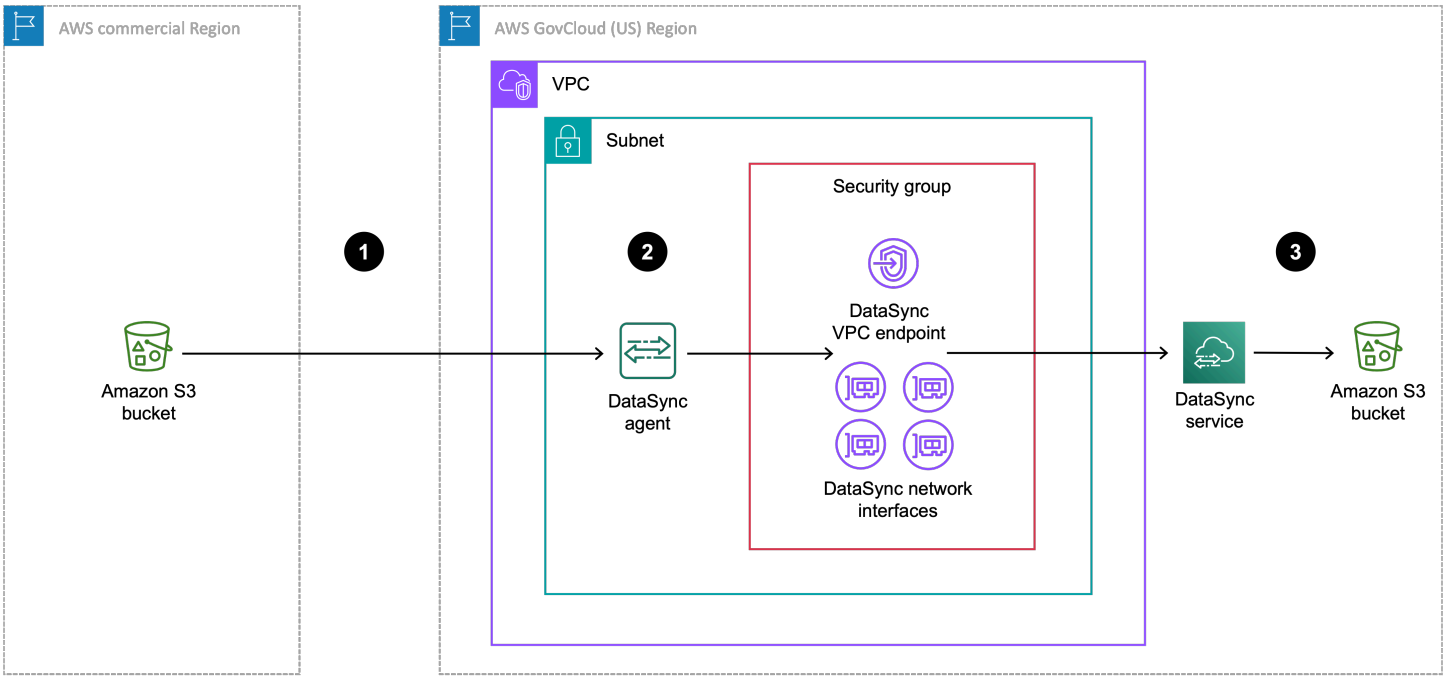
Vous pouvez également utiliser cette même configuration pour transférer la direction opposée de la région AWS GovCloud (US) Region vers la région commerciale.

Pour créer votre DataSync agent

1. Déployez un EC2 agent Amazon dans votre région commerciale.
2. Configurez votre agent pour utiliser un point de terminaison de service VPC.
3. Activez votre agent.

Lors de l'exécution d'une DataSync tâche dans une région GovCloud (États-Unis)

Le schéma suivant montre un transfert dans lequel se trouvent votre DataSync tâche et votre agent AWS GovCloud (US) Region.



Référence	Description
1	Transferts de données depuis le compartiment S3 source de la région commerciale vers AWS GovCloud (US) Region celui où vous exécutez une DataSync tâche. Le compartiment source est configuré comme emplacement de stockage d'objets dans le AWS GovCloud (US) Region.
2	Dans le AWS GovCloud (US) Region, les données sont transférées via l' DataSync agent dans le même VPC et le

Référence	Description
	même sous-réseau où se trouvent le point de terminaison du service VPC et les interfaces réseau.
3	Transferts de données vers le compartiment S3 de destinati on dans le AWS GovCloud (US) Region. Le compartiment de destination est configuré comme un emplacement Amazon S3 dans le AWS GovCloud (US) Region.

Vous pouvez également utiliser cette même configuration pour transférer la direction opposée de la région AWS GovCloud (US) Region vers la région commerciale.

Pour créer votre DataSync agent

1. Déployez un EC2 agent Amazon dans votre AWS GovCloud (US) Region.
2. Configurez votre agent pour utiliser un point de terminaison de service VPC.
3. Activez votre agent.

Si votre ensemble de données est hautement compressible, vous pouvez réduire les coûts en créant plutôt votre agent dans une région commerciale tout en exécutant une tâche dans un AWS GovCloud (US) Region. La configuration de cet agent est plus complexe que d'habitude, y compris la préparation de l'agent pour une utilisation dans une région commerciale. Pour plus d'informations sur la création d'un agent pour cette configuration, consultez le AWS DataSync blog Déplacer des données vers et AWS GovCloud (US) depuis avec.

Création d'un emplacement de stockage d'objets pour votre compartiment S3

Vous avez besoin d'un emplacement de stockage d'objets pour le compartiment S3 situé dans la région où vous n'exécutez pas votre DataSync tâche.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Assurez-vous que vous vous trouvez dans la même région que celle dans laquelle vous prévoyez d'exécuter votre tâche.
3. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.

4. Pour Type d'emplacement, choisissez Stockage d'objets.
5. Pour les agents, choisissez l' DataSync agent que vous avez créé pour ce transfert.
6. Pour Server, entrez un point de terminaison Amazon S3 pour votre compartiment en utilisant l'un des formats suivants :

   - Compartiment de la région commerciale : `s3.your-region.amazonaws.com`
   - AWS GovCloud (US) Region seau : `s3.your-gov-region.amazonaws.com`

   Pour obtenir la liste des points de terminaison Amazon S3, consultez le Références générales AWS.
7. Dans le champ Nom du compartiment, entrez le nom du compartiment S3.
8. Pour Dossier, entrez un préfixe dans le compartiment S3 qui DataSync lit ou écrit dans le compartiment (selon que le compartiment est un emplacement source ou de destination).

   > **Warning**
   >
   > DataSync Impossible de transférer des objets dont le préfixe commence par une barre oblique (/) ou inclut `///./`, ou `/../` des motifs. Par exemple :
   >
   > - `/photos`
   > - `photos//2006/January`
   > - `photos/./2006/February`
   > - `photos/../2006/March`
9. Sélectionnez Requiert des informations d'identification et procédez comme suit :

   - Pour Clé d'accès, entrez la clé d'accès d'un utilisateur IAM autorisé à accéder au compartiment.
   - Pour Clé secrète, entrez la clé secrète du même utilisateur IAM.
10. (Facultatif) Choisissez Ajouter un tag pour marquer votre position.

    Les balises vous aident à gérer, filtrer et rechercher vos ressources. Nous vous recommandons de créer une balise de nom pour votre emplacement.
11. Choisissez Créer un emplacement.

Utilisation de l' AWS CLI

1. Copiez la `create-location-object-storage` commande suivante :

```
aws datasync create-location-object-storage \
    --server-hostname s3-endpoint \
    --bucket-name amzn-s3-demo-bucket \
    --agent-arns arn:aws:datasync:your-region:123456789012:agent/
agent-01234567890deadfb
```

2. Pour le `--server-hostname` paramètre, spécifiez un point de terminaison Amazon S3 pour votre compartiment en utilisant l'un des formats suivants :

   - Compartiment de la région commerciale : `s3.your-region.amazonaws.com`
   - AWS GovCloud (US) Region seau : `s3.your-gov-region.amazonaws.com`

   Pour la région du point de terminaison, assurez-vous de spécifier la même région dans laquelle vous prévoyez d'exécuter votre tâche.

   Pour obtenir la liste des points de terminaison Amazon S3, consultez le Références générales AWS.
3. Pour le `--bucket-name` paramètre, spécifiez le nom du compartiment S3.
4. Pour le `--agent-arns` paramètre, spécifiez l' DataSyncagent que vous avez créé pour ce transfert.
5. Pour le `--access-key` paramètre, spécifiez la clé d'accès pour un utilisateur IAM autorisé à accéder au bucket.
6. Pour le `--secret-key` paramètre, entrez la clé secrète du même utilisateur IAM.
7. (Facultatif) Pour le `--subdirectory` paramètre, spécifiez un préfixe dans le compartiment S3 qui DataSync lit ou écrit dans le compartiment (selon que le compartiment est un emplacement source ou de destination).

   > **Warning**
   >
   > DataSync Impossible de transférer des objets dont le préfixe commence par une barre oblique (/) ou inclut `///./`, ou `/../` des motifs. Par exemple :
   >
   > - `/photos`
   > - `photos//2006/January`

- `photos/./2006/February`
- `photos/../2006/March`

8. (Facultatif) Pour le `--tags` paramètre, spécifiez des paires clé-valeur qui représentent les balises de la ressource de localisation.

   Les balises vous aident à gérer, filtrer et rechercher vos ressources. Nous vous recommandons de créer une balise de nom pour votre emplacement.

9. Exécutez la commande `create-location-object-storage`.

   Vous obtenez une réponse qui indique l'ARN de localisation que vous venez de créer.

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-01234567890abcdef"
}
```

Vous pouvez utiliser cet emplacement comme source ou destination pour votre DataSync tâche. Pour l'autre compartiment S3 concerné par ce transfert, créez un emplacement Amazon S3.

Étapes suivantes

Parmi les prochaines étapes possibles, citons :

1. Si nécessaire, créez votre autre emplacement. Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.
2. Configurez les paramètres des DataSync tâches, tels que les fichiers à transférer, la manière de gérer les métadonnées, entre autres options.
3. Définissez un calendrier pour votre DataSync tâche.
4. Configurez la surveillance pour votre DataSync tâche.
5. Commencez votre tâche.

Configuration des AWS DataSync transferts avec Amazon EFS

Pour transférer des données vers ou depuis votre système de fichiers Amazon EFS, vous devez créer un emplacement AWS DataSync de transfert. DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Fournir un DataSync accès aux systèmes de fichiers Amazon EFS

La création d'un emplacement implique de comprendre comment DataSync accéder à votre espace de stockage. Pour Amazon EFS, DataSync monte votre système de fichiers en tant qu'utilisateur root depuis votre cloud privé virtuel (VPC) à l'aide d'interfaces réseau.

Table des matières

- Déterminer le sous-réseau et les groupes de sécurité pour votre cible de montage
- Accès aux systèmes de fichiers restreints
  - Création d'un rôle DataSync IAM pour l'accès au système de fichiers
  - Exemple de politique de système de fichiers autorisant DataSync l'accès

Déterminer le sous-réseau et les groupes de sécurité pour votre cible de montage

Lorsque vous créez votre emplacement, vous spécifiez le sous-réseau et les groupes de sécurité qui permettent de vous connecter DataSync à l'une des cibles de montage de votre système de fichiers Amazon EFS.

Le sous-réseau que vous spécifiez doit être situé :

- Dans le même VPC que votre système de fichiers.
- Dans la même zone de disponibilité qu'au moins une cible de montage pour votre système de fichiers.

> **Note**
>
> Vous n'avez pas besoin de spécifier un sous-réseau incluant une cible de montage de système de fichiers.

Les groupes de sécurité que vous spécifiez doivent autoriser le trafic entrant sur le port 2049 du système de fichiers réseau (NFS). Pour plus d'informations sur la création et la mise à jour de groupes de sécurité pour vos cibles de montage, consultez le guide de l'utilisateur Amazon EFS.

Spécification des groupes de sécurité associés à une cible de montage

Vous pouvez spécifier un groupe de sécurité associé à l'une des cibles de montage de votre système de fichiers. Nous recommandons cette approche du point de vue de la gestion du réseau.

Spécifier les groupes de sécurité qui ne sont pas associés à une cible de montage

Vous pouvez également spécifier un groupe de sécurité qui n'est pas associé à l'une des cibles de montage de votre système de fichiers. Toutefois, ce groupe de sécurité doit être en mesure de communiquer avec le groupe de sécurité d'une cible de montage.

Par exemple, voici comment créer une relation entre le groupe de sécurité D (pour DataSync) et le groupe de sécurité M (pour la cible de montage) :

- Le groupe de sécurité D, que vous spécifiez lors de la création de votre position, doit disposer d'une règle autorisant les connexions sortantes sur le port NFS 2049 vers le groupe de sécurité M.
- Le groupe de sécurité M, que vous associez à la cible de montage, doit autoriser l'accès entrant sur le port NFS 2049 à partir du groupe de sécurité D.

Pour trouver le groupe de sécurité d'une cible de montage

Les instructions suivantes peuvent vous aider à identifier le groupe de sécurité d'une cible de montage du système de fichiers Amazon EFS que vous DataSync souhaitez utiliser pour votre transfert.

1. Dans le AWS CLI, exécutez la `describe-mount-targets` commande suivante.

```
aws efs describe-mount-targets \
    --region file-system-region  \
    --file-system-id file-system-id
```

Cette commande renvoie des informations sur les cibles de montage de votre système de fichiers (comme dans l'exemple de sortie suivant).

```
{
    "MountTargets": [
        {
            "OwnerId": "111222333444",
            "MountTargetId": "fsmt-22334a10",
```

```
            "FileSystemId": "fs-123456ab",
            "SubnetId": "subnet-f12a0e34",
            "LifeCycleState": "available",
            "IpAddress": "11.222.0.123",
            "NetworkInterfaceId": "eni-1234a044"
        }
    ]
}
```

2. Prenez note de la `MountTargetId` valeur que vous souhaitez utiliser.
3. Exécutez la `describe-mount-target-security-groups` commande suivante en utilisant le `MountTargetId` pour voir le groupe de sécurité de votre cible de montage.

```
aws efs describe-mount-target-security-groups \
    --region file-system-region \
    --mount-target-id mount-target-id
```

Vous spécifiez ce groupe de sécurité lors de la création de votre position.

Accès aux systèmes de fichiers restreints

DataSync peut être transféré vers ou depuis les systèmes de fichiers Amazon EFS qui limitent l'accès via des points d'accès et des politiques IAM.

> **Note**
>
> Si vous DataSync accédez à un système de fichiers de destination via un point d'accès qui applique l'identité de l'utilisateur, l'utilisateur et le groupe POSIX de vos données sources ne sont pas préservés si vous configurez votre DataSync tâche IDs pour en copier la propriété. Au lieu de cela, les fichiers et dossiers transférés sont définis en fonction de l'utilisateur et du groupe du point d'accès IDs. Dans ce cas, la vérification des tâches échoue car elle DataSync détecte une incompatibilité entre les métadonnées des emplacements source et de destination.

Table des matières

- Création d'un rôle DataSync IAM pour l'accès au système de fichiers
- Exemple de politique de système de fichiers autorisant DataSync l'accès

Création d'un rôle DataSync IAM pour l'accès au système de fichiers

Si votre système de fichiers Amazon EFS restreint l'accès par le biais d'une politique IAM, vous pouvez créer un rôle IAM qui DataSync autorise la lecture ou l'écriture de données dans le système de fichiers. Il se peut que vous deviez ensuite spécifier ce rôle dans la politique de votre système de fichiers.

Pour créer le rôle DataSync IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles, puis sélectionnez Créer un rôle.
3. Sur la page Sélectionner une entité de confiance, pour Type d'entité fiable, choisissez Politique de confiance personnalisée.
4. Collez le code JSON suivant dans l'éditeur de règles :

   JSON

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

5. Choisissez Suivant. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant).
6. Donnez un nom à votre rôle et choisissez Créer un rôle.

Vous spécifiez ce rôle lors de la création de votre position.

Exemple de politique de système de fichiers autorisant DataSync l'accès

L'exemple de politique de système de fichiers suivant montre comment l'accès à un système de fichiers Amazon EFS (identifié dans la politique comme `fs-1234567890abcdef0`) est restreint tout en autorisant l'accès DataSync via un rôle IAM nommé `MyDataSyncRole` :

JSON

```
{
    "Version": "2012-10-17",
    "Id": "ExampleEFSFileSystemPolicy",
    "Statement": [{
        "Sid": "AccessEFSFileSystem",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/MyDataSyncRole"
        },
        "Action": [
            "elasticfilesystem:ClientMount",
            "elasticfilesystem:ClientWrite",
            "elasticfilesystem:ClientRootAccess"
        ],
        "Resource": "arn:aws:elasticfilesystem:us-east-1:111122223333:file-
system/fs-1234567890abcdef0",
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "true"
            },
            "StringEquals": {
                "elasticfilesystem:AccessPointArn":
 "arn:aws:elasticfilesystem:us-east-1:111122223333:access-point/
fsap-abcdef01234567890"
            }
        }
    }]
}
```

- `Principal`— Spécifie un rôle IAM qui donne DataSync l'autorisation d'accéder au système de fichiers.

- `Action`— Donne un accès DataSync root et lui permet de lire et d'écrire dans le système de fichiers.
- `aws:SecureTransport`— Nécessite que les clients NFS utilisent le protocole TLS lors de la connexion au système de fichiers.
- `elasticfilesystem:AccessPointArn`— Autorise l'accès au système de fichiers uniquement via un point d'accès spécifique.

Considérations relatives au réseau liées aux transferts Amazon EFS

VPCs que vous utilisez avec DataSync doit avoir une location par défaut. VPCs avec location dédiée ne sont pas pris en charge.

Considérations relatives aux performances liées aux transferts Amazon EFS

Le mode de débit de votre système de fichiers Amazon EFS peut affecter la durée du transfert et les performances du système de fichiers pendant le transfert. Éléments à prendre en compte :

- Pour de meilleurs résultats, nous vous recommandons d'utiliser le mode débit élastique. Si vous n'utilisez pas le mode débit élastique, votre transfert peut prendre plus de temps.
- Si vous utilisez le mode débit en rafale, les performances des applications de votre système de fichiers peuvent être affectées en raison de la consommation de crédits en rafale DataSync du système de fichiers.
- La façon dont vous configurez DataSync pour vérifier les données transférées peut affecter les performances du système de fichiers et les coûts d'accès aux données.

Pour plus d'informations, consultez les performances d'Amazon EFS dans le guide de l'utilisateur d'Amazon Elastic File System et sur la page de tarification d'Amazon EFS.

Création de votre lieu de transfert Amazon EFS

Pour créer le lieu de transfert, vous avez besoin d'un système de fichiers Amazon EFS existant. Si vous n'en avez pas, consultez Getting started with Amazon EFS dans le manuel Amazon Elastic File System User Guide.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.

2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour le type d'emplacement, choisissez le système de fichiers Amazon EFS.

   Vous configurerez cet emplacement comme source ou destination plus tard.
4. Pour Système de fichiers, choisissez le système de fichiers Amazon EFS que vous souhaitez utiliser comme emplacement.
5. Pour Chemin de montage, entrez un chemin de montage pour votre système de fichiers Amazon EFS.

   Cela DataSync indique où les données sont lues ou écrites (selon qu'il s'agit d'un emplacement source ou de destination) sur votre système de fichiers.

   Par défaut, DataSync utilise le répertoire racine (ou le point d'accès si vous en fournissez un pour le paramètre du point d'accès EFS). Vous pouvez également spécifier des sous-répertoires à l'aide de barres obliques (par exemple,). `/path/to/directory`
6. Pour Sous-réseau, choisissez un sous-réseau dans lequel vous souhaitez DataSync créer les interfaces réseau pour gérer votre trafic de transfert de données.

   Le sous-réseau doit être situé :

   - Dans le même VPC que votre système de fichiers.
   - Dans la même zone de disponibilité qu'au moins une cible de montage du système de fichiers.

   > **Note**
   >
   > Vous n'avez pas besoin de spécifier un sous-réseau incluant une cible de montage de système de fichiers.

7. Pour les groupes de sécurité, choisissez le groupe de sécurité associé à la cible de montage de votre système de fichiers Amazon EFS. Vous pouvez choisir plusieurs groupes de sécurité.

   > **Note**
   >
   > Les groupes de sécurité que vous spécifiez doivent autoriser le trafic entrant sur le port NFS 2049. Pour de plus amples informations, veuillez consulter Déterminer le sous-réseau et les groupes de sécurité pour votre cible de montage.

8. Pour le chiffrement en transit, indiquez si vous DataSync souhaitez utiliser le chiffrement TLS (Transport Layer Security) lors du transfert de données vers ou depuis votre système de fichiers.

> **Note**
>
> Vous devez activer ce paramètre pour configurer un point d'accès, un rôle IAM ou les deux avec votre emplacement Amazon EFS.

9. (Facultatif) Pour le point d'accès EFS, choisissez un point d'accès qui DataSync peut être utilisé pour monter votre système de fichiers.

   Pour de plus amples informations, veuillez consulter Accès aux systèmes de fichiers restreints.

10. (Facultatif) Pour le rôle IAM, spécifiez un rôle qui permet d'accéder DataSync à votre système de fichiers.

    Pour plus d'informations sur la création de ce rôle, consultez Création d'un rôle DataSync IAM pour l'accès au système de fichiers.

11. (Facultatif) Sélectionnez Ajouter une balise pour étiqueter votre système de fichiers.

    Une balise est une paire clé-valeur qui vous aide à gérer, filtrer et rechercher vos emplacements.

12. Choisissez Créer un emplacement.

En utilisant le AWS CLI

1. Copiez la `create-location-efs` commande suivante :

```
aws datasync create-location-efs \
    --efs-filesystem-arn 'arn:aws:elasticfilesystem:region:account-id:file-
system/file-system-id' \
    --subdirectory /path/to/your/subdirectory \
    --ec2-config SecurityGroupArns='arn:aws:ec2:region:account-id:security-
group/security-group-id',SubnetArn='arn:aws:ec2:region:account-id:subnet/subnet-id'
 \
    --in-transit-encryption TLS1_2 \
    --access-point-arn 'arn:aws:elasticfilesystem:region:account-id:access-
point/access-point-id' \
    --file-system-access-role-arn 'arn:aws:iam::account-id:role/datasync-efs-
access-role
```

2. Pour`--efs-filesystem-arn`, spécifiez le nom de ressource Amazon (ARN) du système de fichiers Amazon EFS vers ou depuis lequel vous effectuez le transfert.
3. Pour`--subdirectory`, spécifiez un chemin de montage pour votre système de fichiers.

   C'est là que les données sont DataSync lues ou écrites (selon qu'il s'agit d'un emplacement source ou de destination) sur votre système de fichiers.

   Par défaut, DataSync utilise le répertoire racine (ou le point d'accès si vous en fournissez un`--access-point-arn`). Vous pouvez également spécifier des sous-répertoires à l'aide de barres obliques (par exemple,). `/path/to/directory`
4. Pour `--ec2-config`, procédez comme suit :

   - Pour`SecurityGroupArns`, spécifiez l'ARN du groupe de sécurité associé à la cible de montage de votre système de fichiers. Vous pouvez spécifier plusieurs groupes de sécurité.

     > **Note**
     >
     > Les groupes de sécurité que vous spécifiez doivent autoriser le trafic entrant sur le port NFS 2049. Pour de plus amples informations, veuillez consulter Déterminer le sous-réseau et les groupes de sécurité pour votre cible de montage.

   - Pour`SubnetArn`, spécifiez l'ARN du sous-réseau dans lequel vous souhaitez DataSync créer les interfaces réseau pour gérer votre trafic de transfert de données.

     Le sous-réseau doit être situé :

     - Dans le même VPC que votre système de fichiers.
     - Dans la même zone de disponibilité qu'au moins une cible de montage du système de fichiers.

     > **Note**
     >
     > Vous n'avez pas besoin de spécifier un sous-réseau incluant une cible de montage de système de fichiers.
5. Pour`--in-transit-encryption`, indiquez si vous DataSync souhaitez utiliser le chiffrement TLS (Transport Layer Security) lors du transfert de données vers ou depuis votre système de fichiers.

> **Note**
>
> Vous devez le définir `TLS1_2` pour configurer un point d'accès, un rôle IAM ou les deux avec votre emplacement Amazon EFS.

6. (Facultatif) Pour `--access-point-arn`, spécifiez l'ARN d'un point d'accès qui DataSync peut être utilisé pour monter votre système de fichiers.

   Pour de plus amples informations, veuillez consulter Accès aux systèmes de fichiers restreints.

7. (Facultatif) Pour `--file-system-access-role-arn`, spécifiez l'ARN d'un rôle IAM qui permet d'accéder DataSync à votre système de fichiers.

   Pour plus d'informations sur la création de ce rôle, consultez Création d'un rôle DataSync IAM pour l'accès au système de fichiers.

8. Exécutez la commande `create-location-efs`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de l'emplacement que vous avez créé. Par exemple :

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Configuration des transferts avec FSx pour Windows File Server

Pour transférer des données vers ou depuis votre système de fichiers Amazon FSx pour Windows File Server, vous devez créer un emplacement de AWS DataSync transfert. DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Fournir DataSync un accès FSx aux systèmes de fichiers Windows File Server

DataSync se connecte à votre système FSx de fichiers Windows File Server via le protocole SMB (Server Message Block) et le monte depuis votre cloud privé virtuel (VPC) à l'aide d'interfaces réseau.

> **Note**
>
> VPCs que vous utilisez avec DataSync doit avoir une location par défaut. VPCs avec location dédiée ne sont pas pris en charge.

Rubriques

- Autorisations requises
- Protocoles d'authentification requis
- Espaces de noms DFS

Autorisations requises

Vous devez fournir à DataSync un utilisateur les droits nécessaires pour monter et accéder à vos fichiers, dossiers et métadonnées de fichiers FSx pour Windows File Server.

Nous recommandons à cet utilisateur d'appartenir à un groupe Microsoft Active Directory pour administrer votre système de fichiers. Les spécificités de ce groupe dépendent de votre configuration Active Directory :

- Si vous utilisez AWS Directory Service for Microsoft Active Directory with FSx for Windows File Server, l'utilisateur doit être membre du groupe des FSx administrateurs AWS délégués.
- Si vous utilisez Active Directory autogéré avec FSx pour Windows File Server, l'utilisateur doit être membre de l'un des deux groupes suivants :
  - Le groupe des administrateurs du domaine, qui est le groupe d'administrateurs délégués par défaut.
  - Un groupe d'administrateurs délégués personnalisé doté de droits d'utilisateur permettant de DataSync copier les autorisations de propriété des objets et les listes de contrôle d'accès Windows (ACLs).

> **Important**
>
> Vous ne pouvez pas modifier le groupe d'administrateurs délégués une fois le système de fichiers déployé. Vous devez soit redéployer le système de fichiers, soit le restaurer à partir d'une sauvegarde pour utiliser le groupe d'administrateurs délégués personnalisé doté des droits d'utilisateur suivants qui DataSync doit copier les métadonnées.

Droit de l'utilisateur	Description
Restaurer des fichiers et des répertoires (`SE_RESTORE_NAME`)	Permet DataSync de copier la propriété des objets, les autorisations, les métadonnées des fichiers et les listes d'accès discrétio nnaires NTFS ()DACLs. Ce droit d'utilisateur est généralement accordé aux membres des groupes Domain Admins et Backup Operators (qui sont tous deux des groupes Active Directory par défaut).
Gérer le journal d'audit et de sécurité (`SE_SECURITY_NAME`)	Permet DataSync de copier les listes de contrôle d'accès au système NTFS (SACLs). Ce droit d'utilisateur est généralement accordé aux membres du groupe des administrateurs de domaine.

- Si vous souhaitez copier Windows ACLs et effectuez un transfert entre un serveur de fichiers SMB et FSx un système de fichiers Windows File Server ou entre FSx des systèmes de fichiers Windows File Server, les utilisateurs que vous indiquez DataSync doivent appartenir au même domaine Active Directory ou avoir une relation d'approbation Active Directory entre leurs domaines.

> **Warning**
>
> L'utilisateur SYSTEM de votre FSx système de fichiers Windows File Server doit disposer d'autorisations de contrôle total sur tous les dossiers de votre système de fichiers. Ne modifiez pas les autorisations ACL NTFS pour cet utilisateur sur vos dossiers. Si vous le faites, vous DataSync pouvez modifier les autorisations de votre système de fichiers de manière à rendre votre partage de fichiers inaccessible et à empêcher les sauvegardes du système de fichiers d'être utilisables. Pour plus d'informations sur l'accès au niveau des fichiers et des dossiers, consultez le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

Protocoles d'authentification requis

Votre serveur de fichiers FSx pour Windows doit utiliser l'authentification NTLM pour y DataSync accéder. DataSyncImpossible d'accéder à un serveur de fichiers qui utilise l'authentification Kerberos.

Espaces de noms DFS

DataSync ne prend pas en charge les espaces de noms Microsoft Distributed File System (DFS). Nous vous recommandons de spécifier un serveur de fichiers ou un partage sous-jacent lors de la création de votre DataSync emplacement.

Pour plus d'informations, consultez la section Regroupement de plusieurs systèmes de fichiers avec des espaces de noms DFS dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

Création de votre emplacement de transfert FSx pour Windows File Server

Avant de commencer, assurez-vous que vous disposez d'un serveur de fichiers FSx pour Windows existant dans votre Région AWS. Pour plus d'informations, consultez Getting started with Amazon FSx dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour le type de localisation, choisissez Amazon FSx.
4. Pour FSx le système de fichiers, choisissez le système de fichiers FSx pour le serveur de fichiers Windows que vous souhaitez utiliser comme emplacement.
5. Pour Nom du partage, entrez un chemin de montage FSx pour votre serveur de fichiers Windows à l'aide de barres obliques.

   Ceci indique le chemin où les données sont DataSync lues ou écrites (selon qu'il s'agit d'un emplacement source ou de destination).

   Vous pouvez également inclure des sous-répertoires (par exemple,`/path/to/directory`).
6. Pour les groupes de sécurité, choisissez jusqu'à cinq groupes EC2 de sécurité Amazon qui fournissent un accès au sous-réseau préféré de votre système de fichiers.

Les groupes de sécurité que vous choisissez doivent pouvoir communiquer avec les groupes de sécurité de votre système de fichiers. Pour plus d'informations sur la configuration des groupes de sécurité pour l'accès au système de fichiers, consultez le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

> **Note**
>
> Si vous choisissez un groupe de sécurité qui n'autorise pas les connexions internes, effectuez l'une des opérations suivantes :
>
> - Configurez le groupe de sécurité pour lui permettre de communiquer au sein de lui-même.
> - Choisissez un autre groupe de sécurité capable de communiquer avec le groupe de sécurité de la cible de montage.

7. Dans Utilisateur, entrez le nom d'un utilisateur qui peut accéder à votre serveur de fichiers FSx pour Windows.

   Pour de plus amples informations, veuillez consulter Autorisations requises.
8. Dans Mot de passe, entrez le mot de passe du nom d'utilisateur.
9. (Facultatif) Dans le champ Domaine, entrez le nom du domaine Windows auquel appartient votre FSx système de fichiers Windows File Server.

   Si votre environnement comporte plusieurs domaines Active Directory, la configuration de ce paramètre garantit la DataSync connexion au bon système de fichiers.
10. (Facultatif) Entrez des valeurs dans les champs Clé et Valeur FSx pour étiqueter le serveur de fichiers Windows.

    Les balises vous aident à gérer, à filtrer et à rechercher vos AWS ressources. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.
11. Choisissez Créer un emplacement.

En utilisant le AWS CLI

Pour créer un emplacement de serveur de fichiers FSx pour Windows à l'aide du AWS CLI

- Utilisez la commande suivante pour créer un FSx site Amazon.

```
aws datasync create-location-fsx-windows \
    --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system/filesystem-id \
    --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
    --user smb-user --password password
```

Dans la `create-location-fsx-windows` commande, procédez comme suit :

- `fsx-filesystem-arn`— Spécifiez le nom de ressource Amazon (ARN) du système de fichiers vers ou depuis lequel vous souhaitez effectuer le transfert.
- `security-group-arns`— Spécifiez un maximum ARNs de cinq groupes de EC2 sécurité Amazon qui fournissent l'accès au sous-réseau préféré de votre système de fichiers.

  Les groupes de sécurité que vous spécifiez doivent pouvoir communiquer avec les groupes de sécurité de votre système de fichiers. Pour plus d'informations sur la configuration des groupes de sécurité pour l'accès au système de fichiers, consultez le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

  > **Note**
  >
  > Si vous choisissez un groupe de sécurité qui n'autorise pas les connexions internes, effectuez l'une des opérations suivantes :
  >
  > - Configurez le groupe de sécurité pour lui permettre de communiquer au sein de lui-même.
  > - Choisissez un autre groupe de sécurité capable de communiquer avec le groupe de sécurité de la cible de montage.

- La Région AWS — La région que vous spécifiez est celle où se trouve votre système de FSx fichiers Amazon cible.

La commande renvoie un ARN d'emplacement similaire à celui indiqué ci-après.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07db7abfc326c50fb"
}
```

Configuration des DataSync transferts avec FSx for Lustre

Pour transférer des données vers ou depuis votre système de fichiers Amazon FSx for Lustre, vous devez créer un emplacement AWS DataSync de transfert. DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Fournir un DataSync accès FSx aux systèmes de fichiers Lustre

DataSync accède à votre système de fichiers FSx for Lustre à l'aide du client Lustre. DataSyncnécessite l'accès à toutes les données de votre système de fichiers FSx for Lustre. Pour bénéficier de ce niveau d'accès, DataSync monte votre système de fichiers en tant qu'utilisateur root à l'aide d'un ID utilisateur (UID) et d'un ID de groupe (GID) de. `0`

DataSync monte votre système de fichiers à partir de votre cloud privé virtuel (VPC) à l'aide d'interfaces réseau. DataSync gère entièrement la création, l'utilisation et la suppression de ces interfaces réseau en votre nom.

> **Note**
>
> VPCs que vous utilisez avec DataSync doit avoir une location par défaut. VPCs avec location dédiée ne sont pas pris en charge.

Création de votre lieu de transfert FSx pour Lustre

Pour créer l'emplacement de transfert, vous avez besoin d'un système de fichiers existant FSx pour Lustre. Pour plus d'informations, consultez Getting started with Amazon FSx for Lustre dans le guide de l'utilisateur d'Amazon FSx for Lustre.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour le type de localisation, choisissez Amazon FSx.

   Vous configurerez cet emplacement comme source ou destination plus tard.
4. Pour FSx le système de fichiers, choisissez le FSx système de fichiers Lustre que vous souhaitez utiliser comme emplacement.

5. Pour Chemin de montage, entrez le chemin de montage de votre système de fichiers FSx for Lustre.

   Le chemin peut inclure un sous-répertoire. Lorsque l'emplacement est utilisé comme source, DataSync lit les données depuis le chemin de montage. Lorsque l'emplacement est utilisé comme destination, DataSync écrit toutes les données sur le chemin de montage. Si aucun sous-répertoire n'est fourni, DataSync utilise le répertoire racine (`/`).

6. Pour les groupes de sécurité, choisissez jusqu'à cinq groupes de sécurité qui donnent accès à votre système de fichiers FSx for Lustre.

   Les groupes de sécurité doivent pouvoir accéder aux ports du système de fichiers. Le système de fichiers doit également autoriser l'accès depuis les groupes de sécurité.

   Pour plus d'informations sur les groupes de sécurité, consultez la section Contrôle d'accès au système de fichiers avec Amazon VPC dans le guide de l'utilisateur d'Amazon FSx for Lustre.

7. (Facultatif) Entrez des valeurs dans les champs Clé et Valeur FSx pour étiqueter le système de fichiers Lustre.

   Les balises vous aident à gérer, à filtrer et à rechercher vos AWS ressources. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

8. Choisissez Créer un emplacement.

En utilisant le AWS CLI

Pour créer un emplacement FSx pour Lustre à l'aide du AWS CLI

- Utilisez la commande suivante pour créer un emplacement FSx pour Lustre.

```
aws datasync create-location-fsx-lustre \
    --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system:filesystem-id \
    --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id
```

  Les paramètres suivants sont obligatoires dans la `create-location-fsx-lustre` commande.

  - `fsx-filesystem-arn`— Le nom de ressource Amazon (ARN) complet du système de fichiers dans lequel vous souhaitez lire ou écrire.

- `security-group-arns`— L'ARN d'un groupe de EC2 sécurité Amazon à appliquer aux interfaces réseau du sous-réseau préféré du système de fichiers.

La commande précédente renvoie un ARN de localisation similaire au suivant.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07sb7abfc326c50fb"
}
```

Configuration des DataSync transferts avec Amazon FSx pour OpenZFS

Pour transférer des données vers ou depuis votre système de fichiers Amazon FSx pour OpenZFS, vous devez créer un emplacement de AWS DataSync transfert. DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Fournir un DataSync accès aux FSx systèmes de fichiers OpenZFS

DataSync monte votre système de fichiers FSx pour OpenZFS à partir de votre cloud privé virtuel (VPC) à l'aide d'interfaces réseau. DataSyncgère entièrement la création, l'utilisation et la suppression de ces interfaces réseau en votre nom.

> **Note**
>
> VPCs que vous utilisez avec DataSync doit avoir une location par défaut. VPCs avec location dédiée ne sont pas pris en charge.

Configuration de FSx l'autorisation du système de fichiers OpenZFS

DataSync accède à votre système FSx de fichiers OpenZFS en tant que client NFS, en le montant en tant qu'utilisateur root avec un ID utilisateur (UID) et un ID de groupe (GID) de. `0`

DataSync Pour copier toutes les métadonnées de vos fichiers, vous devez configurer les paramètres d'exportation NFS sur les volumes de votre système de fichiers à l'aide `no_root_squash` de. Toutefois, vous pouvez limiter ce niveau d'accès à une DataSync tâche spécifique uniquement.

Pour plus d'informations, consultez la section Propriétés du volume dans le guide de l'utilisateur FSx d'Amazon pour OpenZFS.

Configuration des exportations NFS spécifiques à DataSync (recommandé)

Vous pouvez configurer une exportation NFS spécifique à chaque volume accessible uniquement par votre DataSync tâche. Procédez ainsi pour le volume ancêtre le plus récent du chemin de montage que vous avez spécifié lors de la création de votre emplacement FSx pour OpenZFS.

Pour configurer une exportation NFS spécifique à DataSync

1. Créez votre DataSynctâche.

   Cela crée les interfaces réseau de la tâche que vous spécifiez dans vos paramètres d'exportation NFS.
2. Localisez les adresses IP privées des interfaces réseau de la tâche à l'aide de la EC2 console Amazon ou AWS CLI.
3. FSx Pour votre volume de système de fichiers OpenZFS, configurez les paramètres d'exportation NFS suivants pour chacune des interfaces réseau de la tâche :
   - Adresse du client : entrez l'adresse IP privée de l'interface réseau (par exemple,`10.24.34.0`).
   - Options NFS : Entrez`rw,no_root_squash`.

Configuration des exportations NFS pour tous les clients

Vous pouvez spécifier une exportation NFS qui autorise l'accès root à tous les clients.

Pour configurer une exportation NFS pour tous les clients

- FSx Pour votre volume de système de fichiers OpenZFS, configurez les paramètres d'exportation NFS suivants :
  - Adresse du client : Entrez`*`.
  - Options NFS : Entrez`rw,no_root_squash`.

Création de votre lieu FSx de transfert pour OpenZFS

Pour créer l'emplacement, vous avez besoin d'un système de fichiers existant FSx pour OpenZFS. Si vous n'en avez pas, consultez Getting started with Amazon FSx for OpenZFS dans le guide de l'utilisateur d'Amazon FSx pour OpenZFS.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Locations, puis Create location.
3. Pour le type de localisation, choisissez Amazon FSx.

   Vous configurerez cet emplacement comme source ou destination plus tard.
4. Pour FSx le système de fichiers, choisissez le FSx système de fichiers OpenZFS que vous souhaitez utiliser comme emplacement.
5. Dans le champ Chemin de montage, entrez le chemin de montage de votre FSx système de fichiers OpenZFS.

   Le chemin doit commencer par `/fsx` et peut être n'importe quel chemin de répertoire existant dans le système de fichiers. Lorsque l'emplacement est utilisé comme source, DataSync lit les données depuis le chemin de montage. Lorsque l'emplacement est utilisé comme destination, DataSync écrit toutes les données sur le chemin de montage. Si aucun sous-répertoire n'est fourni, DataSync utilise le répertoire du volume racine (par exemple,`/fsx`).
6. Pour les groupes de sécurité, choisissez jusqu'à cinq groupes de sécurité qui fournissent un accès réseau à votre système FSx de fichiers OpenZFS.

   Les groupes de sécurité doivent fournir un accès aux ports réseau utilisés par le système de fichiers FSx for OpenZFS. Le système de fichiers doit autoriser l'accès au réseau à partir des groupes de sécurité.

   Pour plus d'informations sur les groupes de sécurité, consultez la section Contrôle d'accès au système de fichiers avec Amazon VPC dans le guide de l'utilisateur Amazon FSx pour OpenZFS.
7. (Facultatif) Développez les paramètres supplémentaires et pour la version NFS, choisissez la version NFS DataSync utilisée pour accéder à votre système de fichiers.

   Par défaut, DataSync utilise la version 4.1 de NFS.
8. (Facultatif) Entrez des valeurs dans les champs Clé et Valeur FSx pour étiqueter le système de fichiers OpenZFS.

   Les tags vous aident à gérer, filtrer et rechercher votre position. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.
9. Choisissez Créer un emplacement.

En utilisant le AWS CLI

Pour créer un emplacement FSx pour OpenZFS à l'aide du AWS CLI

1. Copiez la `create-location-fsx-open-zfs` commande suivante :

```
aws datasync create-location-fsx-open-zfs \
   --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system/filesystem-id \
   --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
   --protocol NFS={}
```

2. Spécifiez les options requises suivantes dans la commande :

   - Pour`fsx-filesystem-arn`, spécifiez le nom de ressource Amazon (ARN) complet du système de fichiers de localisation. Cela inclut l' Région AWS emplacement de votre système de fichiers Compte AWS, votre identifiant et l'identifiant du système de fichiers.
   - Pour`security-group-arns`, spécifiez l'ARN du groupe de EC2 sécurité Amazon qui fournit l'accès aux interfaces réseau du sous-réseau préféré FSx de votre système de fichiers OpenZFS. Cela inclut l' Région AWS emplacement de votre EC2 instance Amazon, le vôtre Compte AWS et l'ID du groupe de sécurité.

     Pour plus d'informations sur les groupes de sécurité, consultez la section Contrôle d'accès au système de fichiers avec Amazon VPC dans le guide de l'utilisateur d'Amazon FSx pour OpenZFS.
   - Pour`protocol`, spécifiez le protocole DataSync utilisé pour accéder à votre système de fichiers. (ne prend DataSync actuellement en charge que NFS.)

3. Exécutez la commande . Vous obtenez une réponse indiquant l'emplacement que vous venez de créer.

```
{
    "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890"
}
```

Configuration des transferts avec Amazon FSx pour NetApp ONTAP

Pour transférer des données depuis ou vers votre système de fichiers Amazon FSx for NetApp ONTAP, vous devez créer un lieu de AWS DataSync transfert. DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Fournir un DataSync accès aux FSx systèmes de fichiers ONTAP

Pour accéder à un système de fichiers FSx pour ONTAP, DataSync installez une machine virtuelle de stockage (SVM) sur votre système de fichiers à l'aide des interfaces réseau de votre cloud privé virtuel (VPC). DataSync crée ces interfaces réseau dans le sous-réseau préféré de votre système de fichiers uniquement lorsque vous créez une tâche qui inclut votre emplacement FSx pour ONTAP.

> **Note**
>
> VPCs que vous utilisez avec DataSync doit avoir une location par défaut. VPCs avec location dédiée ne sont pas pris en charge.

DataSync peut se connecter à la SVM FSx d'un système de fichiers ONTAP et copier des données en utilisant le protocole NFS (Network File System) ou SMB (Server Message Block).

Rubriques

- Utilisation du protocole NFS
- Utilisation du protocole SMB
- Protocoles non pris en charge
- Choisir le bon protocole
- Accès aux SnapLock volumes

Utilisation du protocole NFS

Avec le protocole NFS, DataSync utilise le mécanisme de `AUTH_SYS` sécurité avec un ID utilisateur (UID) et un ID de groupe (GID) `0` pour s'authentifier auprès de votre SVM.

> **Note**
>
> DataSync ne prend actuellement en charge que la version 3 de NFS FSx pour les emplacements ONTAP.

Utilisation du protocole SMB

Avec le protocole SMB, DataSync utilise les informations d'identification que vous fournissez pour vous authentifier auprès de votre SVM.

Versions SMB prises en charge

Par défaut, choisit DataSync automatiquement une version du protocole SMB en fonction de la négociation avec votre serveur de fichiers SMB. Vous pouvez également configurer DataSync pour utiliser une version spécifique, mais nous vous recommandons de le faire uniquement si DataSync vous rencontrez des difficultés pour négocier automatiquement avec le serveur de fichiers SMB. Pour des raisons de sécurité, nous recommandons d'utiliser SMB version 3.0.2 ou ultérieure.

Consultez le tableau suivant pour obtenir la liste des options de la DataSync console et de l'API permettant de configurer une version SMB avec votre emplacement FSx for ONTAP :

Option console	Option d'API	Description
Automatique	`AUTOMATIC`	DataSync et le serveur de fichiers SMB négocient la version la plus élevée de SMB qu'ils supportent mutuellement entre 2.1 et 3.1.1. Il s'agit de l'option recommandée par défaut. Si vous optez pour une version spécifique que votre serveur de fichiers ne prend pas en charge, vous risquez de recevoir une erreur `Operation Not Supported` .
SMB 3.0.2	`SMB3`	Limite la négociation du protocole à la version SMB 3.0.2 uniquement.
SMB 2.1	`SMB2`	Limite la négociation du protocole à la version 2.1 de SMB uniquement.

Option console	Option d'API	Description
SMB 2.0	`SMB2_0`	Limite la négociation du protocole à la version 2.0 de SMB uniquement.

Autorisations requises

Vous devez fournir à DataSync un utilisateur local de votre SVM ou à un utilisateur de domaine de votre Microsoft Active Directory les droits nécessaires pour monter et accéder à vos fichiers, dossiers et métadonnées de fichiers.

Si vous indiquez un utilisateur dans votre Active Directory, notez les points suivants :

- Si vous utilisez AWS Directory Service for Microsoft Active Directory, l'utilisateur doit être membre du groupe des FSxadministrateurs AWS délégués.
- Si vous utilisez un Active Directory autogéré, l'utilisateur doit être membre de l'un des deux groupes suivants :
  - Le groupe des administrateurs du domaine, qui est le groupe d'administrateurs délégués par défaut.
  - Un groupe d'administrateurs délégués personnalisé doté de droits d'utilisateur permettant de DataSync copier les autorisations de propriété des objets et les listes de contrôle d'accès Windows (ACLs).

> **Important**
>
> Vous ne pouvez pas modifier le groupe d'administrateurs délégués une fois le système de fichiers déployé. Vous devez soit redéployer le système de fichiers, soit le restaurer à partir d'une sauvegarde pour utiliser le groupe d'administrateurs délégués personnalisé doté des droits d'utilisateur suivants qui DataSync doit copier les métadonnées.

Droit de l'utilisateur	Description
Agir en tant que partie intégrante du système d'exploitation (`SE_TCB_NAME`)	Permet DataSync de copier la propriété des objets, les autorisations, les métadonnées

Droit de l'utilisateur	Description
	des fichiers et les listes d'accès discrétio nnaires NTFS ()DACLs. Ce droit d'utilisateur est généralement accordé aux membres des groupes Domain Admins et Backup Operators (qui sont tous deux des groupes Active Directory par défaut).
Gérer le journal d'audit et de sécurité (`SE_SECURITY_NAME`)	Permet DataSync de copier les listes de contrôle d'accès au système NTFS (SACLs). Ce droit d'utilisateur est généralement accordé aux membres du groupe des administrateurs de domaine.

- Si vous souhaitez copier Windows ACLs et effectuer un transfert entre FSx des systèmes de fichiers ONTAP utilisant SMB (ou d'autres types de systèmes de fichiers utilisant SMB), les utilisateurs que vous indiquez DataSync doivent appartenir au même domaine Active Directory ou avoir une relation d'approbation Active Directory entre leurs domaines.

Protocoles d'authentification requis

Pour accéder DataSync à votre partage SMB, votre système de fichiers FSx for ONTAP doit utiliser l'authentification NTLM. DataSync Impossible d'accéder aux systèmes FSx de fichiers ONTAP qui utilisent l'authentification Kerberos.

Espaces de noms DFS

DataSync ne prend pas en charge les espaces de noms Microsoft Distributed File System (DFS). Nous vous recommandons de spécifier un serveur de fichiers ou un partage sous-jacent lors de la création de votre DataSync emplacement.

Protocoles non pris en charge

DataSync Impossible d'accéder FSx aux systèmes de fichiers ONTAP à l'aide du protocole iSCSI (Internet Small Computer Systems Interface).

Choisir le bon protocole

Pour conserver les métadonnées des fichiers FSx pour les migrations ONTAP, configurez vos emplacements DataSync source et de destination pour utiliser le même protocole. Parmi les protocoles pris en charge, SMB préserve les métadonnées avec la plus grande fidélité (voir Comprendre le mode de DataSync gestion des métadonnées des fichiers et des objets pour plus de détails).

Lors de la migration depuis un serveur Unix (Linux) ou un partage de stockage rattaché au réseau (NAS) qui dessert les utilisateurs via NFS, procédez comme suit :

1. Créez un emplacement NFS pour le serveur Unix (Linux) ou le partage NAS. (Ce sera votre emplacement source.)
2. Configurez FSx le volume ONTAP vers lequel vous transférez les données avec le style de sécurité Unix.
3. Créez un emplacement pour votre système de fichiers FSx for ONTAP configuré pour NFS. (Ce sera votre destination.)

Lors de la migration depuis un serveur Windows ou un partage NAS qui dessert les utilisateurs via SMB, procédez comme suit :

1. Créez un emplacement SMB pour le serveur Windows ou le partage NAS. (Ce sera votre emplacement source.)
2. Configurez FSx le volume ONTAP vers lequel vous transférez les données avec le style de sécurité NTFS.
3. Créez un emplacement pour votre système de fichiers FSx for ONTAP configuré pour SMB. (Ce sera votre destination.)

Si votre environnement FSx for ONTAP utilise plusieurs protocoles, nous vous recommandons de faire appel à un spécialiste du AWS stockage. Pour en savoir plus sur les meilleures pratiques en matière d'accès multiprotocole, consultez la section Activation des charges de travail multiprotocoles avec Amazon FSx pour ONTAP. NetApp

Accès aux SnapLock volumes

Si vous transférez des données vers un SnapLock volume sur un système de fichiers FSx pour ONTAP, assurez-vous que les SnapLock paramètres Autocommit et Mode d'ajout de volume sont

désactivés sur le volume pendant le transfert. Vous pouvez réactiver ces paramètres lorsque vous avez terminé de transférer les données.

Création de votre lieu FSx de transfert pour ONTAP

Pour créer l'emplacement, vous avez besoin d'un système FSx de fichiers ONTAP existant. Si vous n'en avez pas, consultez Getting started with Amazon FSx for NetApp ONTAP dans le guide de l'utilisateur d'Amazon FSx for NetApp ONTAP.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour le type de localisation, choisissez Amazon FSx.

   Vous configurerez cet emplacement comme source ou destination plus tard.
4. Pour FSx le système de fichiers, choisissez le FSx système de fichiers ONTAP que vous souhaitez utiliser comme emplacement.
5. Pour Machine virtuelle de stockage, choisissez une machine virtuelle de stockage (SVM) dans votre système de fichiers vers laquelle vous souhaitez copier des données.
6. Pour le chemin de montage, spécifiez le chemin du partage de fichiers dans cette SVM où vous allez copier vos données.

   Vous pouvez spécifier un chemin de jonction (également appelé point de montage), un chemin qtree (pour les partages de fichiers NFS) ou un nom de partage (pour les partages de fichiers SMB). Par exemple, votre chemin de montage peut être `/vol1`, `/vol1/tree1` ou `/share1`.

   > **Tip**
   >
   > Ne spécifiez pas de chemin dans le volume racine de la SVM. Pour plus d'informations, consultez la section Gestion FSx des machines virtuelles de stockage ONTAP dans le guide de l'utilisateur Amazon FSx pour NetApp ONTAP.
7. Pour les groupes de sécurité, choisissez jusqu'à cinq groupes EC2 de sécurité Amazon qui fournissent un accès au sous-réseau préféré de votre système de fichiers.

Les groupes de sécurité doivent autoriser le trafic sortant sur les ports suivants (selon le protocole que vous utilisez) :

- NFS : ports TCP 111, 635 et 2049
- SMB — Port TCP 445

Les groupes de sécurité de votre système de fichiers doivent également autoriser le trafic entrant sur les mêmes ports.

8. Dans le champ Protocole, choisissez le protocole de transfert de données à DataSync utiliser pour accéder à la SVM de votre système de fichiers.

   Pour de plus amples informations, veuillez consulter Choisir le bon protocole.

   NFS

   DataSync utilise la version 3 de NFS.

   SMB

   Configurez une version SMB, un utilisateur, un mot de passe et un nom de domaine Active Directory (si nécessaire) pour accéder à la SVM.

   - (Facultatif) Développez les paramètres supplémentaires et choisissez une version SMB DataSync à utiliser lors de l'accès à votre SVM.

     Par défaut, choisit DataSync automatiquement une version en fonction de la négociation avec le serveur de fichiers SMB. Pour de plus amples informations, veuillez consulter Utilisation du protocole SMB.
   - Dans le champ Utilisateur, entrez un nom d'utilisateur qui peut monter et accéder aux fichiers, dossiers et métadonnées que vous souhaitez transférer dans la SVM.

     Pour de plus amples informations, veuillez consulter Utilisation du protocole SMB.
   - Dans le champ Mot de passe, entrez le mot de passe de l'utilisateur que vous avez indiqué qui peut accéder à la SVM.
   - (Facultatif) Pour le nom de domaine Active Directory, entrez le nom de domaine complet (FQDN) de l'Active Directory auquel appartient votre SVM.

Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion à la SVM appropriée.

9. (Facultatif) Entrez des valeurs pour les champs Clé et Valeur afin de baliser le système FSx de fichiers ONTAP.

   Les balises vous aident à gérer, à filtrer et à rechercher vos AWS ressources. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

10. Choisissez Créer un emplacement.

En utilisant le AWS CLI

Pour créer un emplacement FSx pour ONTAP à l'aide du AWS CLI

1. Copiez la `create-location-fsx-ontap` commande suivante :

```
aws datasync create-location-fsx-ontap \
   --storage-virtual-machine-arn arn:aws:fsx:region:account-id:storage-virtual-
machine/fs-file-system-id \
   --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
   --protocol data-transfer-protocol={}
```

2. Spécifiez les options requises suivantes dans la commande :

   - Pour`storage-virtual-machine-arn`, spécifiez le nom Amazon Resource Name (ARN) complet d'une machine virtuelle de stockage (SVM) de votre système de fichiers vers ou depuis laquelle vous souhaitez copier des données.

     Cet ARN inclut l' Région AWS emplacement de votre système de fichiers, le vôtre Compte AWS, le système de fichiers et la SVM IDs.

   - Pour`security-group-arns`, spécifiez les groupes ARNs de EC2 sécurité Amazon qui fournissent l'accès aux interfaces réseau du sous-réseau préféré de votre système de fichiers.

     Cela inclut l' Région AWS endroit où réside votre EC2 instance Amazon, le Compte AWS vôtre et votre groupe de sécurité IDs. Vous pouvez spécifier jusqu'à cinq groupes de sécurité ARNs.

     Pour plus d'informations sur les groupes de sécurité, consultez la section Contrôle d'accès au système de fichiers avec Amazon VPC dans le guide de l'utilisateur Amazon FSx for NetApp ONTAP.

- Pour`protocol`, configurez le protocole DataSync utilisé pour accéder à la SVM de votre système de fichiers.
  - Pour NFS, vous pouvez utiliser la configuration par défaut :

    ```
    --protocol NFS={}
    ```

  - Pour les PME, vous devez indiquer un nom d'utilisateur et un mot de passe permettant d'accéder à la SVM :

    ```
    --protocol SMB={User=smb-user,Password=smb-password}
    ```

3. Exécutez la commande .

   Vous obtenez une réponse qui indique l'emplacement que vous venez de créer.

   ```
   {
       "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
   abcdef01234567890"
   }
   ```

Transfert vers ou depuis un autre stockage dans le cloud avec AWS DataSync

Avec AWS DataSync, vous pouvez transférer des données entre d'autres fournisseurs de cloud et services AWS de stockage. Pour plus d'informations, consultez Où puis-je transférer mes données DataSync ?

Rubriques

- Planification des transferts vers ou depuis des systèmes de stockage cloud tiers
- Configuration des AWS DataSync transferts avec Google Cloud Storage
- Configuration des transferts avec Microsoft Azure Blob Storage
- Configuration des AWS DataSync transferts avec Microsoft Azure Files Actions de PME
- Configuration des transferts avec d'autres solutions de stockage d'objets dans le cloud

Planification des transferts vers ou depuis des systèmes de stockage cloud tiers

Lorsque vous planifiez des transferts de données entre clouds, tenez compte des points suivants :

- Utilisation d'un agent : un agent est uniquement requis pour accéder au stockage dans d'autres clouds lors de l'utilisation de tâches en mode de base. Les tâches en mode amélioré ne nécessitent pas d'agent. Si vous décidez d'utiliser un agent, vous pouvez le déployer en tant qu' EC2instance Amazon lors du transfert depuis le stockage d'objets compatible S3 d'un fournisseur de cloud, ou en tant que moteur de calcul Google ou machine virtuelle Azure pour les transferts depuis ces services de stockage spécifiques, respectivement. Lors du transfert depuis des systèmes de fichiers dans Google et Azure, nous recommandons de déployer l'agent en tant que machine virtuelle Google ou Azure afin qu'il soit le plus proche possible du système de fichiers. En outre, DataSync compresse les données de l'agent vers le serveur AWS, ce qui peut contribuer à réduire les coûts de sortie. DataSync fournit une liste d'emplacements cloud validés qui fournissent la compatibilité requise avec les API Amazon S3.
- Point de terminaison de stockage d'objets de l'autre cloud : le point de terminaison de stockage d'un fournisseur de cloud tiers est généralement spécifique à une région ou à un compte. Le point de terminaison régional est utilisé comme serveur dans l'emplacement de stockage d' DataSync objets, avec un nom de compartiment spécifié.
- Classes de stockage des objets sources : comme Amazon S3, certains fournisseurs de cloud proposent un niveau d'archivage qui nécessite une restauration avant de pouvoir accéder aux objets archivés. Par exemple, les objets du niveau d'archive Azure Blob doivent être récupérés pour un accès standard avant le transfert de données. Les objets du niveau d'archivage de Google Cloud Storage sont accessibles immédiatement et ne nécessitent pas de restauration, mais l'accès direct au niveau d'archivage entraîne des coûts de récupération. Consultez la documentation de votre classe de stockage cross-cloud pour déterminer les exigences d'accès et les frais de récupération avant de commencer votre transfert de données. Pour plus d'informations sur la restauration d'objets archivés dans Amazon S3, consultez la section Restauration d'un objet archivé dans le guide de l'utilisateur d'Amazon Simple Storage Service.
- Accès au stockage d'objets : le transfert de données entre fournisseurs de cloud tiers nécessite l'accès au stockage d'objets de l'autre cloud sous forme de clés d'authentification. Par exemple, pour fournir un accès à Google Cloud Storage, vous configurez un emplacement de stockage d' DataSync objets qui se connecte à l'API XML de Google Cloud Storage et s'authentifie à l'aide d'une clé HMAC (Hash Based Message Authentication Code) pour votre compte de service. Pour le stockage Azure Blob, vous configurez un DataSync emplacement Azure Blob dédié qui

s'authentifie à l'aide de jetons SAS. DataSync utilise AWS Secrets Manager pour stocker en toute sécurité vos informations d'identification de stockage d'objets. Pour plus d'informations, consultez la section Sécurisation des informations d'identification de l'emplacement de stockage.

- Support des balises d'objet :
  - Contrairement à Amazon S3, tous les fournisseurs de cloud ne prennent pas en charge les balises d'objet. DataSync les tâches peuvent échouer lors de la tentative de lecture de balises depuis l'emplacement source si le fournisseur de cloud ne prend pas en charge les balises d'objet via l'API Amazon S3 ou si les informations d'identification que vous fournissez sont insuffisantes pour récupérer les balises. DataSyncfournit une option de tâche pour désactiver la lecture et la copie des balises d'objet lors d'un transfert si les balises d'objet ne sont pas prises en charge ou si vous ne souhaitez pas conserver les balises. Consultez la documentation de votre fournisseur de cloud pour déterminer si les balises d'objet sont prises en charge, et vérifiez les paramètres des balises d'objet de votre tâche de transfert avant de lancer le transfert.
  - Vous pouvez utiliser l'API Amazon S3 pour vérifier si un fournisseur de cloud renverra une `get-object-tagging` demande. Pour plus d'informations, consultez get-object-tagging dans la Référence des commandes de l'AWS CLI .

    Un fournisseur de cloud qui prend en charge les balises d'objet renverra une réponse similaire à l'exemple suivant :

    ```
    aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint- url=https://
    BUCKET_ENDPOINT --key prefix/file1

    {

        "TagSet": []

    }
    ```

    Un fournisseur de cloud qui ne prend pas en charge `get-object-tagging` renverra le message suivant :

    ```
    aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint- url=https://
    BUCKET_ENDPOINT --key prefix/file1

    An error occurred (OperationNotSupported) when calling the GetObjectTagging
     operation: The operation is not supported for this resource
    ```

- Coûts associés aux demandes et à la sortie de données : le transfert de données depuis le stockage d'objets dans le cloud entraîne des coûts de demande et de sortie associés à la lecture des données et au transfert de données sortantes. Les frais de demande varient selon les fournisseurs de cloud et entre les classes de stockage, le cas échéant. Consultez la documentation de votre fournisseur de cloud concernant les coûts spécifiques des demandes relatifs à la classe de stockage que vous prévoyez de lire. Pour un aperçu des frais de demande liés aux transferts DataSync de données, consultez la section Évaluation des coûts des demandes S3 lors de l'utilisation DataSync et de la AWS DataSync tarification. Le transfert de données depuis des fournisseurs de cloud spécifiques entraîne des frais de sortie. Les coûts de transfert de données varient selon les fournisseurs de cloud et dépendent également de la région dans laquelle les données sont stockées.
- Taux de demandes de stockage d'objets : les fournisseurs de cloud présentent diverses caractéristiques de performance et de taux de demandes pour leurs plateformes de stockage d'objets. Passez en revue les taux de demandes de votre autre fournisseur de cloud et déterminez où les limites de demandes sont appliquées. Planifiez à l'avance les transferts hautement parallélisés composés de plusieurs agents, où un partitionnement spécifique ou une augmentation des performances peuvent être nécessaires.

  Amazon S3 dispose de taux de demandes documentés sur lesquels vous pouvez élaborer votre solution. Les taux de requêtes Amazon S3 sont calculés par préfixe partitionné et sont évolutifs sur plusieurs préfixes. Pour plus d'informations, consultez la section Modèles de conception des meilleures pratiques : optimisation des performances d'Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Configuration des AWS DataSync transferts avec Google Cloud Storage

Le didacticiel suivant montre comment AWS DataSync migrer des objets d'un bucket Google Cloud Storage (GCS) vers un bucket Amazon S3.

Présentation

DataSync utilise l'API XML de Google Cloud Storage pour les transferts de données. Cette API fournit une interface compatible avec Amazon S3 pour lire et écrire des données avec des buckets GCS.

DataSync prend en charge les transferts entre GCS et les services AWS de stockage. Lorsque vous copiez entre GCS et Amazon EFS ou Amazon FSx, un agent est requis et votre tâche doit utiliser le

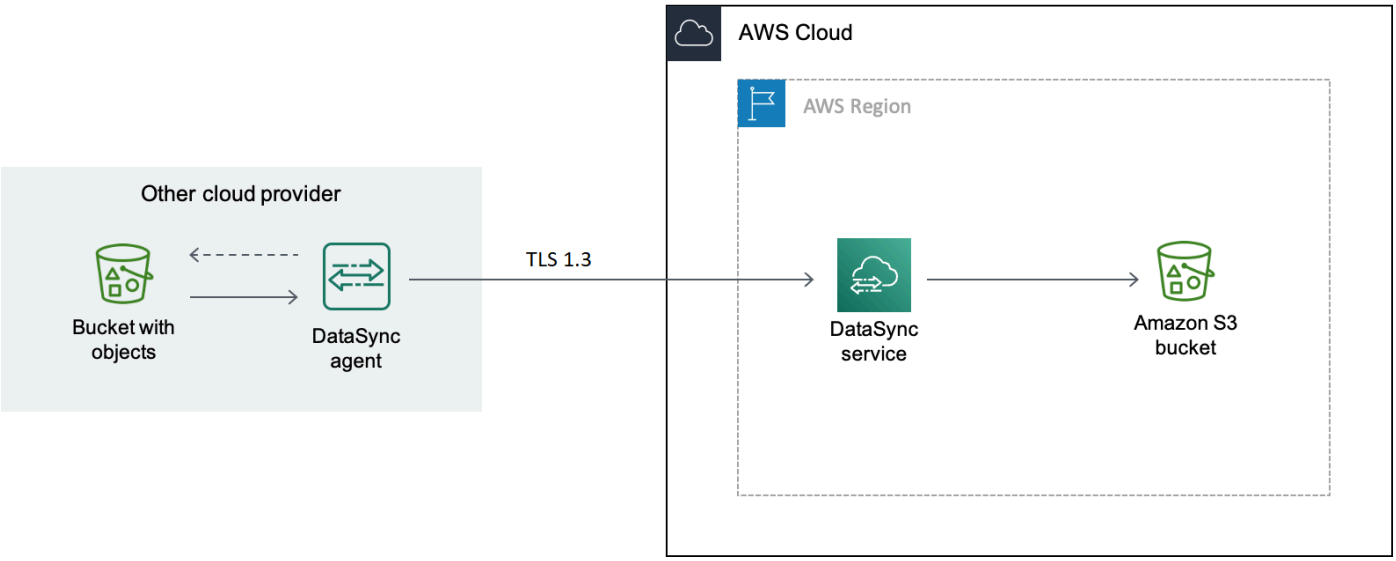
mode Basic. Lors de la copie entre GCS et Amazon S3, un agent n'est requis que si vous utilisez le mode Basic.

Si vous utilisez un agent pour votre transfert, vous pouvez le déployer dans Google Cloud ou dans votre Amazon VPC.

Agent in Google Cloud

1. Vous déployez un DataSync agent dans votre environnement Google Cloud.
2. L'agent lit votre bucket Google Cloud Storage à l'aide d'une clé HMAC (Hash Based Message Authentication Code).
3. Les objets de votre bucket Google Cloud Storage sont transférés en toute sécurité via TLS 1.3 vers le en AWS Cloud utilisant un point de terminaison public.
4. Le DataSync service écrit les données dans votre compartiment S3.

Le schéma suivant illustre le transfert.

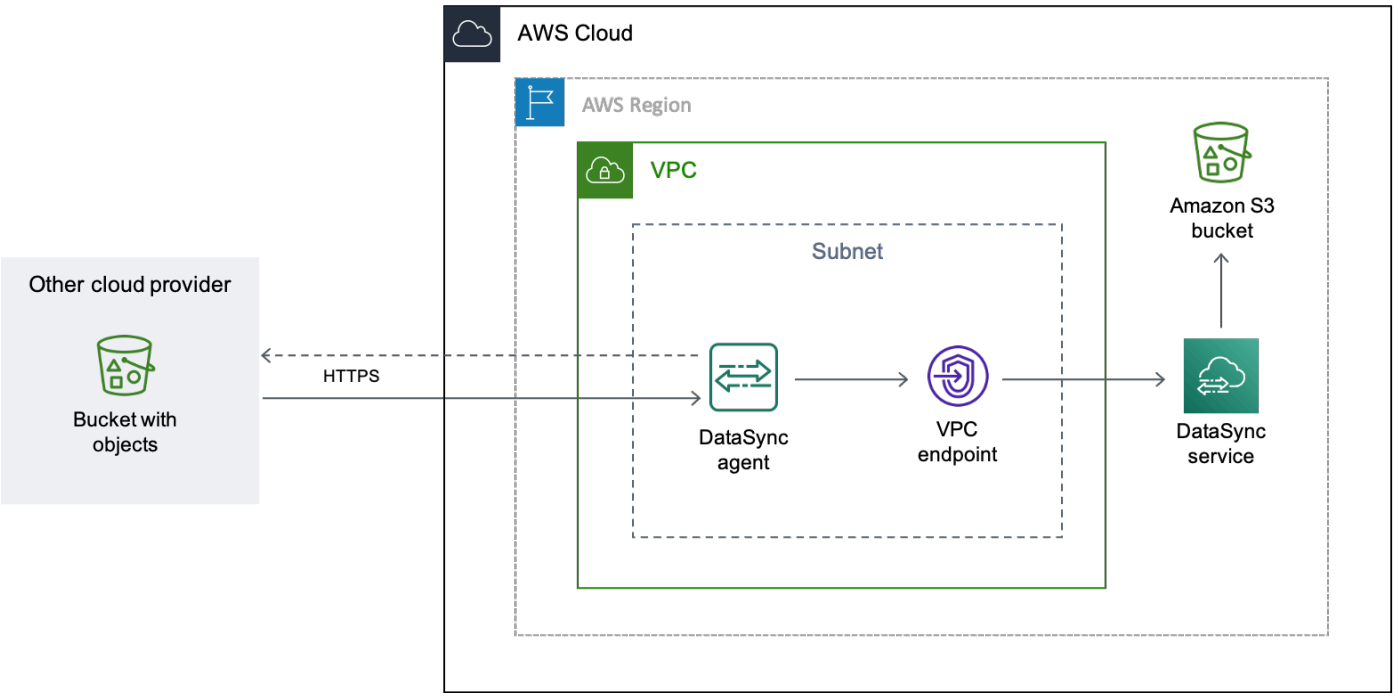


Agent in your VPC

1. Vous déployez un DataSync agent dans un cloud privé virtuel (VPC) de votre AWS environnement.
2. L'agent lit votre bucket Google Cloud Storage à l'aide d'une clé HMAC (Hash Based Message Authentication Code).
3. Les objets de votre bucket Google Cloud Storage sont transférés en toute sécurité via TLS 1.3 vers le en AWS Cloud utilisant un point de terminaison VPC privé.

4. Le DataSync service écrit les données dans votre compartiment S3.

Le schéma suivant illustre le transfert.



Coûts

Les frais associés à cette migration peuvent inclure :

- Exécution d'une instance de machine virtuelle (VM) Google Compute Engine (si vous déployez votre DataSync agent dans Google Cloud)
- Exécution d'une EC2 instance Amazon (si vous déployez votre DataSync agent dans un VPC intégré) AWS
- Transférer les données en utilisant DataSync, y compris les frais de demande liés à Google Cloud Storage et Amazon S3 (si S3 est l'un de vos sites de transfert)
- Transférer des données depuis Google Cloud Storage
- Stockage de données dans Amazon S3

Prérequis

Avant de commencer, procédez comme suit si ce n'est pas déjà fait :

- Créez un bucket Google Cloud Storage contenant les objets vers lesquels vous souhaitez effectuer le transfert AWS.
- Inscrivez-vous pour un Compte AWS.
- Créez un compartiment Amazon S3 pour stocker vos objets une fois qu'ils y sont entrés AWS.

Création d'une clé HMAC pour votre bucket Google Cloud Storage

DataSync utilise une clé HMAC associée à votre compte de service Google pour vous authentifier et lire le compartiment à partir duquel vous transférez les données. (Pour obtenir des instructions détaillées sur la création de clés HMAC, consultez la documentation de Google Cloud Storage.)

Pour créer une clé HMAC

1. Créez une clé HMAC pour votre compte de service Google.
2. Assurez-vous que votre compte de service Google dispose au moins `Storage Object Viewer` d'autorisations.
3. Enregistrez l'identifiant d'accès et le secret de votre clé HMAC dans un endroit sûr.

   Vous aurez besoin de ces éléments ultérieurement pour configurer votre emplacement DataSync source.

Étape 2 : Configuration de votre réseau

La configuration réseau n'est requise que si vous utilisez un DataSync agent lors de votre transfert. La configuration réseau requise pour cette migration dépend de l'endroit où vous choisissez de déployer votre agent.

Pour un DataSync agent dans Google Cloud

Si vous souhaitez héberger votre DataSync agent dans Google Cloud, configurez votre réseau pour autoriser les DataSync transferts via un point de terminaison public.

Pour un DataSync agent de votre VPC

Si vous souhaitez héberger votre agent AWS, vous avez besoin d'un VPC doté d'un point de terminaison d'interface. DataSync utilise le point de terminaison VPC pour faciliter le transfert.

Pour configurer votre réseau pour un point de terminaison VPC

1. Si vous n'en avez pas, créez un VPC dans le même emplacement Région AWS que votre compartiment S3.
2. Créez un sous-réseau privé pour votre VPC.
3. Créez un point de terminaison de service VPC pour. DataSync
4. Configurez votre réseau pour autoriser les DataSync transferts via un point de terminaison de service VPC.

   Pour ce faire, modifiez le groupe de sécurité associé à votre point de terminaison de service VPC.

Étape 3 : créer un DataSync agent (facultatif)

Un DataSync agent n'est requis que lors de l'utilisation des tâches en mode de base. Si vous utilisez le mode amélioré pour effectuer un transfert entre Google Cloud Storage (GCS) et Amazon S3, aucun agent n'est requis. Si vous souhaitez utiliser le mode Basic, vous avez besoin d'un DataSync agent capable d'accéder à votre bucket GCS.

Pour Google Cloud

Dans ce scénario, l' DataSync agent s'exécute dans votre environnement Google Cloud.

Avant de commencer : installez la CLI Google Cloud.

Pour créer l'agent pour Google Cloud

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Agents, puis Create agent.
3. Pour Hypervisor, choisissez VMware ESXi, puis choisissez Télécharger l'image pour télécharger un `.zip` fichier contenant l'agent.
4. Ouvrez un terminal . Décompressez l'image en exécutant la commande suivante :

   ```
   unzip AWS-DataSync-Agent-VMWare.zip
   ```

5. Extrayez le contenu du `.ova` fichier de l'agent `aws-datasync` en commençant par exécuter la commande suivante :

```
tar -xvf aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt.ova
```

6. Importez le `.vmdk` fichier de l'agent dans Google Cloud en exécutant la commande Google Cloud CLI suivante :

```
gcloud compute images import aws-datasync-2-test \
   --source-file INCOMPLETE-aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt-disk1.vmdk
 \
   --os centos-7
```

> **Note**
>
> L'importation du `.vmdk` fichier peut prendre jusqu'à deux heures.

7. Créez et démarrez une instance de machine virtuelle pour l'image d'agent que vous venez d'importer.

   L'instance a besoin des configurations suivantes pour votre agent. (Pour obtenir des instructions détaillées sur la création d'une instance, consultez la documentation de Google Cloud Compute Engine.)

   - Pour le type de machine, sélectionnez l'une des options suivantes :
     - e2-standard-8 — Pour les exécutions de DataSync tâches impliquant jusqu'à 20 millions d'objets.
     - e2-standard-16 — Pour les exécutions de DataSync tâches impliquant plus de 20 millions d'objets.
   - Pour les paramètres du disque de démarrage, rendez-vous dans la section des images personnalisées. Choisissez ensuite l'image de l' DataSync agent que vous venez d'importer.
   - Pour les paramètres du compte de service, choisissez votre compte de service Google (le même compte que celui que vous avez utilisé à l'étape 1).
   - Pour le paramétrage du pare-feu, choisissez l'option permettant d'autoriser le trafic HTTP (port 80).

     Pour activer votre DataSync agent, le port 80 doit être ouvert sur l'agent. Le port n'a pas besoin d'être accessible au public. Une fois activé, DataSync ferme le port.

8. Une fois que l'instance de machine virtuelle est en cours d'exécution, prenez note de son adresse IP publique.

   Vous aurez besoin de cette adresse IP pour activer l'agent.

9. Retournez à la DataSync console. Sur l'écran Créer un agent où vous avez téléchargé l'image de l'agent, procédez comme suit pour activer votre agent :

   - Pour le type de point de terminaison, choisissez l'option points de terminaison de service public (par exemple, points de terminaison de service public dans l'est de l'Ohio aux États-Unis).
   - Pour Clé d'activation, choisissez Obtenir automatiquement la clé d'activation auprès de votre agent.
   - Pour l'adresse de l'agent, entrez l'adresse IP publique de l'instance de machine virtuelle de l'agent que vous venez de créer.
   - Choisissez Obtenir la clé.

10. Donnez un nom à votre agent, puis choisissez Create agent.

Votre agent est en ligne et prêt à transférer des données.

Pour votre VPC

Dans ce scénario, l'agent s'exécute en tant qu' EC2 instance Amazon dans un VPC associé à votre. Compte AWS

Avant de commencer : Configurez le AWS Command Line Interface (AWS CLI).

Pour créer l'agent de votre VPC

1. Ouvrez un terminal . Assurez-vous de configurer votre AWS CLI profil pour utiliser le compte associé à votre compartiment S3.
2. Copiez la commande ci-après. *`vpc-region`*Remplacez-le par l' Région AWS endroit où réside votre VPC (par exemple,`us-east-1`).

   ```
   aws ssm get-parameter --name /aws/service/datasync/ami --region vpc-region
   ```

3. Exécutez la commande . Dans le résultat, prenez note de la `"Value"` propriété.

Cette valeur est l'ID DataSync Amazon Machine Image (AMI) de la région que vous avez spécifiée. Par exemple, un ID d'AMI pourrait ressembler à`ami-1234567890abcdef0`.

4. Copiez l'URL suivante. Encore une fois, *`vpc-region`* remplacez-le par l' Région AWS endroit où réside votre VPC. Remplacez-le ensuite *`ami-id`* par l'ID d'AMI que vous avez noté à l'étape précédente.

```
https://console.aws.amazon.com/ec2/v2/home?region=vpc-
region#LaunchInstanceWizard:ami=ami-id
```

5. Collez l'URL dans un navigateur.

   La page de lancement de l' EC2 instance Amazon s' AWS Management Console affiche.

6. Pour Type d'instance, choisissez l'une des EC2 instances Amazon recommandées pour les DataSync agents.
7. Pour Key pair, choisissez une paire de clés existante ou créez-en une nouvelle.
8. Pour les paramètres réseau, choisissez le VPC et le sous-réseau sur lesquels vous souhaitez déployer l'agent.
9. Choisissez Launch instance (Lancer une instance).
10. Une fois que l' EC2 instance Amazon est en cours d'exécution, choisissez votre point de terminaison VPC.
11. Activez votre agent.

Étape 4 : créer un emplacement DataSync source pour votre bucket Google Cloud Storage

Pour configurer l' DataSync emplacement de votre bucket Google Cloud Storage, vous avez besoin de l'ID d'accès et du secret de la clé HMAC que vous avez créée à l'étape 1.

Pour créer l'emplacement de la DataSync source

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour Type d'emplacement, choisissez Stockage d'objets.
4. Pour Serveur, entrez**`storage.googleapis.com`**.

5. Dans le champ Nom du bucket, saisissez le nom de votre bucket Google Cloud Storage.
6. Pour Dossier, entrez un préfixe d'objet.

   DataSync copie uniquement les objets portant ce préfixe.
7. Si votre transfert nécessite un agent, choisissez Utiliser des agents, puis choisissez l'agent que vous avez créé à l'étape 3.
8. Développer Additional settings (Paramètres supplémentaires). Pour le protocole du serveur, choisissez HTTPS. Pour le port du serveur, choisissez 443.
9. Faites défiler la page jusqu'à la section Authentification. Assurez-vous que la case Requiert des informations d'identification est cochée, puis effectuez les opérations suivantes :
   - Pour Clé d'accès, entrez l'ID d'accès de votre clé HMAC.
   - Pour la clé secrète, entrez directement la clé secrète de votre clé HMAC ou spécifiez un AWS Secrets Manager secret contenant la clé. Pour plus d'informations, consultez la section Fourniture d'informations d'identification pour les emplacements de stockage.
10. Choisissez Créer un emplacement.

Étape 5 : créer un emplacement de DataSync destination pour votre compartiment S3

Vous avez besoin d'un DataSync emplacement où vous souhaitez que vos données aboutissent.

Pour créer le lieu DataSync de destination

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Créez un DataSync emplacement pour le compartiment S3.

   Si vous avez déployé l' DataSync agent dans votre VPC, ce didacticiel part du principe que le compartiment S3 se trouve dans le même emplacement Région AWS que votre VPC et votre agent. DataSync

Étape 6 : créer et démarrer une DataSync tâche

Une fois vos emplacements source et de destination configurés, vous pouvez commencer à transférer vos données vers AWS.

Pour créer et démarrer la DataSync tâche

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Sur la page Configurer l'emplacement de la source, procédez comme suit :
   a. Choisissez Choisir un emplacement existant.
   b. Choisissez l'emplacement source que vous avez créé à l'étape 4, puis cliquez sur Suivant.
4. Sur la page Configurer l'emplacement de destination, procédez comme suit :
   a. Choisissez Choisir un emplacement existant.
   b. Choisissez l'emplacement de destination que vous avez créé à l'étape 5, puis cliquez sur Suivant.
5. Sur la page Configurer les paramètres, procédez comme suit :
   a. Sous Configuration du transfert de données, développez Paramètres supplémentaires et désactivez la case à cocher Copier les balises d'objet.

      > **Important**
      > Étant donné que l'API XML de Google Cloud Storage ne prend pas en charge la lecture ou l'écriture de balises d'objet, votre DataSync tâche risque d'échouer si vous essayez de copier des balises d'objet.

   b. Configurez les autres paramètres de tâche de votre choix, puis choisissez Next.
6. Sur la page Révision, passez en revue vos paramètres, puis choisissez Créer une tâche.
7. Sur la page de détails de la tâche, choisissez Démarrer, puis choisissez l'une des options suivantes :
   - Pour exécuter la tâche sans modification, choisissez Démarrer avec les valeurs par défaut.
   - Pour modifier la tâche avant de l'exécuter, choisissez Démarrer avec des options de remplacement.

Lorsque votre tâche sera terminée, vous verrez les objets de votre compartiment Google Cloud Storage dans votre compartiment S3.

Configuration des transferts avec Microsoft Azure Blob Storage

Avec AWS DataSync, vous pouvez transférer des données entre Microsoft Azure Blob Storage (y compris le stockage Azure Data Lake Storage Gen2 blob) et les services AWS de stockage suivants :

- Amazon S3
- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Pour configurer ce type de transfert, vous devez créer un emplacement pour votreAzure Blob Storage. Vous pouvez utiliser cet emplacement comme source ou destination de transfert. Un DataSync agent n'est requis que lors du transfert de données entre Azure Blob et Amazon EFS ou Amazon FSx, ou lors de l'utilisation de tâches en mode Basic. Vous n'avez pas besoin d'un agent pour transférer des données entre Azure Blob et Amazon S3 à l'aide du mode amélioré.

Fournir un DataSync accès à votre Azure Blob Storage

La manière dont vous DataSync accédez Azure Blob Storage dépend de plusieurs facteurs, notamment du fait que vous effectuez un transfert vers ou depuis le stockage blob et du type de jeton de signature d'accès partagé (SAS) que vous utilisez. Vos objets doivent également se trouver dans un niveau d' DataSync accès compatible avec.

Rubriques

- Jetons SAS
- Niveaux d'accès

Jetons SAS

Un jeton SAS spécifie les autorisations d'accès à votre stockage blob. (Pour plus d'informations sur SAS, consultez la Azure Blob Storagedocumentation.)

Vous pouvez générer des jetons SAS pour fournir différents niveaux d'accès. DataSync prend en charge les jetons avec les niveaux d'accès suivants :

- Compte
- Conteneur

Les autorisations d'accès DataSync nécessaires dépendent de l'étendue de votre jeton. Le fait de ne pas disposer des autorisations appropriées peut entraîner l'échec de votre transfert. Par exemple, votre transfert échouera si vous déplacez des objets dotés de balises Azure Blob Storage mais que votre jeton SAS n'est pas autorisé à utiliser les balises.

Rubriques

- Autorisations liées aux jetons SAS pour un accès au niveau du compte
- Autorisations liées aux jetons SAS pour l'accès au niveau du conteneur
- Politiques d'expiration SAS

Autorisations liées aux jetons SAS pour un accès au niveau du compte

DataSync nécessite un jeton d'accès au niveau du compte avec les autorisations suivantes (selon que vous effectuez un transfert vers ou depuisAzure Blob Storage).

Transfers from blob storage

- Services autorisés — Blob
- Types de ressources autorisés : conteneur, objet

  Si vous n'incluez pas ces autorisations, vous ne DataSync pourrez pas transférer les métadonnées de votre objet, y compris les balises d'objet.
- Autorisations autorisées : lecture, liste
- Autorisations d'indexation blob autorisées : lecture/écriture (si vous souhaitez copier des balises DataSync d'objets)

Transfers to blob storage

- Services autorisés — Blob
- Types de ressources autorisés : conteneur, objet

  Si vous n'incluez pas ces autorisations, vous ne DataSync pourrez pas transférer les métadonnées de votre objet, y compris les balises d'objet.

- Autorisations autorisées : lecture, écriture, liste, suppression (si vous DataSync souhaitez supprimer des fichiers qui ne figurent pas dans votre source de transfert)
- Autorisations d'indexation blob autorisées : lecture/écriture (si vous souhaitez copier des balises DataSync d'objets)

Autorisations liées aux jetons SAS pour l'accès au niveau du conteneur

DataSync nécessite un jeton d'accès au niveau du conteneur avec les autorisations suivantes (selon que vous effectuez un transfert vers ou depuisAzure Blob Storage).

Transfers from blob storage

- Lecture
- Liste
- Tag (si vous DataSync souhaitez copier les balises d'objets)

> **Note**
>
> Vous ne pouvez pas ajouter l'autorisation de balise lorsque vous générez un jeton SAS sur le Azure portail. Pour ajouter l'autorisation du tag, générez plutôt le jeton à l'aide de l'Azure Storage Explorerapplication ou générez un jeton SAS qui fournit un accès au niveau du compte.

Transfers to blob storage

- Lecture
- Écrire
- Liste
- Supprimer (si vous souhaitez DataSync supprimer des fichiers qui ne figurent pas dans votre source de transfert)
- Tag (si vous DataSync souhaitez copier les balises d'objets)

> **Note**
>
> Vous ne pouvez pas ajouter l'autorisation de balise lorsque vous générez un jeton SAS sur le Azure portail. Pour ajouter l'autorisation du tag, générez plutôt le jeton à l'aide de

l'Azure Storage Explorerapplication ou générez un jeton SAS qui fournit un accès au niveau du compte.

Politiques d'expiration SAS

Assurez-vous que votre SAS n'expire pas avant de terminer votre transfert. Pour plus d'informations sur la configuration d'une politique d'expiration SAS, consultez la Azure Blob Storagedocumentation.

Si le SAS expire pendant le transfert, DataSync vous ne pouvez plus accéder à votre Azure Blob Storage position. (Le message d'erreur « Impossible d'ouvrir le répertoire » peut s'afficher.) Dans ce cas, mettez à jour votre position avec un nouveau jeton SAS et redémarrez votre DataSync tâche.

Niveaux d'accès

Lors du transfert depuisAzure Blob Storage, DataSync vous pouvez copier des objets dans les niveaux chaud et froid. Pour les objets du niveau d'accès aux archives, vous devez les réhydrater vers le niveau chaud ou froid avant de pouvoir les copier.

Lors du transfert versAzure Blob Storage, DataSync vous pouvez copier des objets dans les niveaux d'accès à chaud, à froid et aux archives. Si vous copiez des objets dans le niveau d'accès aux archives, vous ne DataSync pouvez pas vérifier le transfert si vous essayez de vérifier toutes les données de la destination.

DataSync ne prend pas en charge le niveau d'accès à froid. Pour plus d'informations sur les niveaux d'accès, consultez la Azure Blob Storagedocumentation.

Considérations relatives aux Azure Blob Storage transferts

Lorsque vous planifiez de transférer des données vers ou depuis Azure Blob Storage avec DataSync, il y a certaines choses à garder à l'esprit.

Rubriques

- Coûts
- Types de blob
- DisponibilitéRégion AWS
- Copier des balises d'objets
- Transfert vers Amazon S3
- Supprimer des répertoires dans une destination de transfert

- Limites

Coûts

Les frais associés à l'entrée ou à la sortie de données Azure Blob Storage peuvent inclure :

- Exécution d'une machine Azure virtuelle (VM) (si vous déployez un DataSync agent dansAzure)
- Exécution d'une EC2 instance Amazon (si vous déployez un DataSync agent dans un VPC intégré) AWS
- Transférer les données en utilisant DataSync, y compris les frais de demande liés à Azure Blob StorageAmazon S3 (si S3 est l'un de vos sites de transfert)
- Transfert de données vers ou depuis Azure Blob Storage
- Stockage des données dans un service AWS de stockage pris en charge par DataSync

Types de blob

Le DataSync fonctionnement des types de blob varie selon que vous effectuez un transfert vers ou depuisAzure Blob Storage. Lorsque vous déplacez des données vers un espace de stockage blob, les objets ou fichiers DataSync transférés ne peuvent être que des blobs. Lorsque vous déplacez des données hors du stockage blob, vous DataSync pouvez transférer des blobs, des pages et ajouter des blobs.

Pour plus d'informations sur les types de blob, consultez la Azure Blob Storagedocumentation.

DisponibilitéRégion AWS

Vous pouvez créer un lieu Azure Blob Storage de transfert dans n'importe quel Région AWS lieu pris en charge par DataSync.

Copier des balises d'objets

La capacité DataSync de conserver les balises d'objet lors du transfert vers ou depuis un objet Azure Blob Storage dépend des facteurs suivants :

- Taille des balises d'un objet : DataSync impossible de transférer un objet dont les balises dépassent 2 Ko.
- DataSync Configuré ou non pour copier les balises d'objet : DataSync copie les balises d'objet par défaut.

- L'espace de noms utilisé par votre compte Azure de stockage : vous DataSync pouvez copier des balises d'objets si votre compte de Azure stockage utilise un espace de noms plat, mais pas s'il utilise un espace de noms hiérarchique (une fonctionnalité de). Azure Data Lake Storage Gen2 Votre DataSync tâche échouera si vous essayez de copier des balises d'objets et si votre compte de stockage utilise un espace de noms hiérarchique.
- Si votre jeton SAS autorise le balisage : les autorisations dont vous avez besoin pour copier les balises d'objets varient en fonction du niveau d'accès fourni par votre jeton. Votre tâche échouera si vous essayez de copier des balises d'objets et si votre jeton ne dispose pas des autorisations nécessaires pour le balisage. Pour plus d'informations, consultez les exigences d'autorisation pour les jetons d'accès au niveau du compte ou les jetons d'accès au niveau du conteneur.

Transfert vers Amazon S3

Lors du transfert vers Amazon S3, les Azure Blob Storage objets DataSync dont la taille est supérieure à 5 To ou les objets dont les métadonnées sont supérieures à 2 Ko ne sont pas transférés.

Supprimer des répertoires dans une destination de transfert

Lors du transfert versAzure Blob Storage, DataSync vous pouvez supprimer des objets de votre stockage blob qui ne sont pas présents dans votre source de transfert. (Vous pouvez configurer cette option en désactivant le paramètre Conserver les fichiers supprimés dans la DataSync console. Votre jeton SAS doit également disposer d'autorisations de suppression.)

Lorsque vous configurez votre transfert de cette façon, les répertoires de votre stockage blob DataSync ne seront pas supprimés si votre compte Azure de stockage utilise un espace de noms hiérarchique. Dans ce cas, vous devez supprimer manuellement les répertoires (par exemple, en utilisant Azure Storage Explorer).

Limites

N'oubliez pas les limites suivantes lorsque vous transférez des données vers ou depuis Azure Blob Storage :

- DataSync crée des répertoires dans un emplacement pour faciliter votre transfert. S'il s'Azure Blob Storageagit d'un emplacement de destination et que votre compte de stockage utilise un espace de noms hiérarchique, vous remarquerez peut-être des sous-répertoires spécifiques aux tâches (tels que`task-000011112222abcde`) dans le dossier. `/.aws-datasync` DataSync supprime généralement ces sous-répertoires après un transfert. Si ce n'est pas le cas, vous

pouvez supprimer vous-même ces répertoires spécifiques à une tâche tant qu'aucune tâche n'est en cours d'exécution.

- DataSync ne prend pas en charge l'utilisation d'un jeton SAS pour accéder uniquement à un dossier spécifique de votre Azure Blob Storage conteneur.
- Vous ne pouvez pas fournir DataSync de jeton SAS de délégation utilisateur pour accéder à votre stockage blob.

Création de votre DataSync agent (facultatif)

Un DataSync agent n'est requis que lors du transfert de données entre Azure Blob et Amazon EFS ou Amazon FSx, ou lors de l'utilisation de tâches en mode Basic. Vous n'avez pas besoin d'un agent pour transférer des données entre Azure Blob et Amazon S3 à l'aide du mode amélioré. Cette section décrit comment déployer et activer un agent.

> **Tip**
>
> Bien que vous puissiez déployer votre agent sur une EC2 instance Amazon, l'utilisation d'un Microsoft Hyper-V agent peut réduire la latence du réseau et augmenter la compression des données.

Agents Microsoft Hyper-V

Vous pouvez déployer votre DataSync agent directement Azure avec une Microsoft Hyper-V image.

> **Tip**
>
> Avant de continuer, pensez à utiliser un script shell qui pourrait vous aider à déployer votre agent Hyper-V Azure plus rapidement. Vous pouvez obtenir plus d'informations et télécharger le code sur GitHub.
> Si vous utilisez le script, vous pouvez passer directement à la section à propos deObtenir la clé d'activation de votre agent.

Rubriques

- Prérequis
- Téléchargement et préparation de votre agent

- Déploiement de votre agent dans Azure
- Obtenir la clé d'activation de votre agent
- Activation de votre agent

Prérequis

Pour préparer votre DataSync agent et le déployerAzure, vous devez effectuer les opérations suivantes :

- Activez Hyper-V sur votre machine locale.
- Installez PowerShell(y compris leHyper-V Module).
- Installez la AzureCLI.
- Installer AzCopy.

Téléchargement et préparation de votre agent

Téléchargez un agent depuis la DataSync console. Avant de pouvoir déployer l'agentAzure, vous devez le convertir en disque dur virtuel (VHD) de taille fixe. Pour plus d'informations, consultez la documentation Azure.

Pour télécharger et préparer votre agent

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Agents, puis Create agent.
3. Pour Hypervisor, choisissez Microsoft Hyper-V, puis choisissez Télécharger l'image.

   L'agent télécharge dans un `.zip` fichier contenant un `.vhdx` fichier.
4. Extrayez le `.vhdx` fichier sur votre machine locale.
5. Ouvrez l'PowerShell et procédez comme suit :

   a. Copiez l'`Convert-VHD`applet de commande suivante :

```
Convert-VHD -Path .\local-path-to-vhdx-file\aws-datasync-2.0.1686143940.1-
x86_64.xfs.gpt.vhdx `
-DestinationPath .\local-path-to-vhdx-file\aws-datasync-2016861439401-
x86_64.vhd -VHDType Fixed
```

b. Remplacez chaque instance *local-path-to-vhdx-file* de par l'emplacement du `.vhdx` fichier sur votre ordinateur local.

c. Exécutez la commande .

Votre agent est désormais un VHD de taille fixe (avec un format de `.vhd` fichier) prêt à être déployé. Azure

Déploiement de votre agent dans Azure

Le déploiement de votre DataSync agent dans Azure implique :

- Création d'un disque géré dans Azure
- Téléchargement de votre agent sur ce disque géré
- Connexion du disque géré à une machine Linux virtuelle

Pour déployer votre agent dans Azure

1. DansPowerShell, accédez au répertoire qui contient le `.vhd` fichier de votre agent.
2. Exécutez la `ls` commande et enregistrez la `Length` valeur (par exemple,`85899346432`).

   Il s'agit de la taille de l'image de votre agent en octets, dont vous avez besoin pour créer un disque géré pouvant contenir l'image.
3. Procédez comme suit pour créer un disque géré :

   a. Copiez la commande Azure CLI suivante :

   ```
   az disk create -n your-managed-disk `
   -g your-resource-group `
   -l your-azure-region `
   --upload-type Upload `
   --upload-size-bytes agent-size-bytes `
   --sku standard_lrs
   ```

   b. *your-managed-disk*Remplacez-le par le nom de votre disque géré.

   c. *your-resource-group*Remplacez-le par le nom du groupe de Azure ressources auquel appartient votre compte de stockage.

d. Remplacez *your-azure-region* par la Azure région où se trouve votre groupe de ressources.

e. Remplacez *agent-size-bytes* par la taille de l'image de votre agent.

f. Exécutez la commande .

Cette commande crée un disque géré vide avec un SKU standard sur lequel vous pouvez télécharger votre DataSync agent.

4. Pour générer une signature d'accès partagé (SAS) qui autorise l'accès en écriture au disque géré, procédez comme suit :

   a. Copiez la commande Azure CLI suivante :

```
az disk grant-access -n your-managed-disk `
-g your-resource-group `
--access-level Write `
--duration-in-seconds 86400
```

   b. *your-managed-disk*Remplacez-le par le nom du disque géré que vous avez créé.

   c. *your-resource-group*Remplacez-le par le nom du groupe de Azure ressources auquel appartient votre compte de stockage.

   d. Exécutez la commande .

      Dans le résultat, prenez note de l'URI SAS. Vous avez besoin de cette URI pour télécharger l'agent versAzure.

Le SAS vous permet d'écrire sur le disque pendant une heure maximum. Cela signifie que vous avez une heure pour télécharger votre agent sur le disque géré.

5. Pour télécharger votre agent sur votre disque géréAzure, procédez comme suit :

   a. Copiez la `AzCopy` commande suivante :

```
.\azcopy copy local-path-to-vhd-file sas-uri --blob-type PageBlob
```

   b. Remplacez *local-path-to-vhd-file* par l'emplacement du `.vhd` fichier de l'agent sur votre ordinateur local.

   c. *sas-uri*Remplacez-le par l'URI SAS que vous avez obtenu lorsque vous avez exécuté la `az disk grant-access` commande.

   d. Exécutez la commande .

6. Lorsque le téléchargement de l'agent est terminé, révoquez l'accès à votre disque géré. Pour ce faire, copiez la commande Azure CLI suivante :

```
az disk revoke-access -n your-managed-disk -g your-resource-group
```

   a. *your-resource-group*Remplacez-le par le nom du groupe de Azure ressources auquel appartient votre compte de stockage.
   b. *your-managed-disk*Remplacez-le par le nom du disque géré que vous avez créé.
   c. Exécutez la commande .

7. Procédez comme suit pour associer votre disque géré à une nouvelle Linux machine virtuelle :

   a. Copiez la commande Azure CLI suivante :

```
az vm create --resource-group your-resource-group `
--location eastus `
--name your-agent-vm `
--size Standard_E4as_v4 `
--os-type linux `
--attach-os-disk your-managed-disk
```

   b. *your-resource-group*Remplacez-le par le nom du groupe de Azure ressources auquel appartient votre compte de stockage.
   c. *your-agent-vm*Remplacez-le par un nom de machine virtuelle dont vous vous souviendrez.
   d. *your-managed-disk*Remplacez-le par le nom du disque géré que vous connectez à la machine virtuelle.
   e. Exécutez la commande .

Vous avez déployé votre agent. Avant de commencer à configurer votre transfert de données, vous devez activer l'agent.

Obtenir la clé d'activation de votre agent

Pour obtenir manuellement la clé d'activation de votre DataSync agent, procédez comme suit.

Vous DataSync pouvez également obtenir automatiquement la clé d'activation pour vous, mais cette approche nécessite une certaine configuration réseau.

Pour obtenir la clé d'activation de votre agent

1. Sur le Azure portail, activez les diagnostics de démarrage de la machine virtuelle pour votre agent en choisissant le paramètre Activer avec un compte de stockage personnalisé et en spécifiant votre compte Azure de stockage.

   Après avoir activé les diagnostics de démarrage pour la machine virtuelle de votre agent, vous pouvez accéder à la console locale de votre agent pour obtenir la clé d'activation.
2. Pendant que vous êtes toujours sur le Azure portail, accédez à votre machine virtuelle et choisissez Serial console.
3. Dans la console locale de l'agent, connectez-vous à l'aide des informations d'identification par défaut suivantes :

   - Nom d'utilisateur – **`admin`**
   - Mot de passe — **`password`**

   Nous vous recommandons de modifier au moins le mot de passe de l'agent à un moment donné. Dans la console locale de l'agent, entrez dans **`5`** le menu principal, puis utilisez la `passwd` commande pour modifier le mot de passe.
4. Entrez **`0`** pour obtenir la clé d'activation de l'agent.
5. Entrez l' Région AWS endroit où vous utilisez DataSync (par exemple,**`us-east-1`**).
6. Choisissez le point de terminaison de service que l'agent utilisera pour se connecter AWS.
7. Enregistrez la valeur de la `Activation key` sortie.

Activation de votre agent

Une fois que vous avez obtenu la clé d'activation, vous pouvez terminer la création de votre DataSync agent.

Pour activer votre agent

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Agents, puis Create agent.
3. Pour Hypervisor, choisissez Microsoft Hyper-V.

4. Pour le type de point de terminaison, choisissez le même type de point de terminaison de service que celui que vous avez spécifié lorsque vous avez obtenu la clé d'activation de votre agent (par exemple, choisissez Points de terminaison de service public dans ***Region name***).
5. Configurez votre réseau pour qu'il fonctionne avec le type de point de terminaison de service utilisé par votre agent. Pour connaître les exigences du réseau des points de terminaison de service, consultez les rubriques suivantes :
   - Points de terminaison d'un VPC
   - Points de terminaison publics
   - Points de terminaison FIPS (Federal Information Processing Standard)
6. Pour la clé d'activation, procédez comme suit :
   a. Choisissez Entrez manuellement la clé d'activation de votre agent.
   b. Entrez la clé d'activation que vous avez reçue de la console locale de l'agent.
7. Choisissez Create agent (Créer un agent).

Votre agent est prêt à communiquer avec vousAzure Blob Storage. Pour de plus amples informations, veuillez consulter Création de votre lieu Azure Blob Storage de transfert.

EC2 Agents Amazon

Vous pouvez déployer votre DataSync agent sur une EC2 instance Amazon.

Pour créer un EC2 agent Amazon

1. Déployez un EC2 agent Amazon.
2. Choisissez un point de terminaison de service avec lequel l'agent communique AWS.

   Dans ce cas, nous vous recommandons d'utiliser un point de terminaison de service de cloud privé virtuel (VPC).
3. Configurez votre réseau pour qu'il fonctionne avec les points de terminaison du service VPC.
4. Activez l'agent.

Création de votre lieu Azure Blob Storage de transfert

Vous pouvez le configurer DataSync pour l'utiliser Azure Blob Storage comme source ou destination de transfert.

Avant de commencer

Assurez-vous de savoir comment DataSync accéder et utiliser les niveaux d'accès Azure Blob Storage et les types de blob. Vous avez également besoin d'un DataSync agent capable de se connecter à votre Azure Blob Storage conteneur.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour Location type (Type d'emplacement), choisissez Microsoft Azure Blob Storage.
4. Pour URL du conteneur, entrez l'URL du conteneur impliqué dans votre transfert.
5. (Facultatif) Pour le niveau d'accès lorsqu'il est utilisé comme destination, choisissez le niveau d'accès vers lequel vous souhaitez transférer vos objets ou fichiers.
6. Pour Dossier, entrez des segments de chemin si vous souhaitez limiter votre transfert vers un répertoire virtuel de votre conteneur (par exemple,`/my/images`).
7. Si votre transfert nécessite un agent, choisissez Utiliser des agents, puis choisissez l' DataSync agent qui peut se connecter à votre Azure Blob Storage conteneur.
8. Pour le jeton SAS, fournissez les informations d'identification nécessaires DataSync pour accéder à votre stockage blob. Certains ensembles de données publics sur le stockage Azure Blob ne nécessitent pas d'informations d'identification. Vous pouvez saisir directement un jeton SAS ou spécifier un AWS Secrets Manager secret contenant le jeton. Pour plus d'informations, consultez la section Fourniture d'informations d'identification pour les emplacements de stockage.

   Votre jeton SAS fait partie de la chaîne d'URI SAS qui suit l'URI de votre ressource de stockage et un point d'interrogation (?). Un jeton ressemble à ceci :

   ```
   sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=aBBKD
   %2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
   ```

9. (Facultatif) Entrez des valeurs pour les champs Clé et Valeur afin de baliser l'emplacement.

   Les balises vous aident à gérer, filtrer et rechercher vos AWS ressources. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

10. Choisissez Créer un emplacement.

En utilisant le AWS CLI

1. Copiez la `create-location-azure-blob` commande suivante :

```
aws datasync create-location-azure-blob \
  --container-url "https://path/to/container" \
  --authentication-type "SAS" \
  --sas-configuration '{
      "Token": "your-sas-token"
    }' \
  --agent-arns my-datasync-agent-arn \
  --subdirectory "/path/to/my/data" \
  --access-tier "access-tier-for-destination" \
  --tags [{"Key": "key1","Value": "value1"}]
```

2. Pour le `--container-url` paramètre, spécifiez l'URL du Azure Blob Storage conteneur impliqué dans votre transfert.
3. Pour le paramètre `--authentication-type`, spécifiez `SAS`. Si vous accédez à un ensemble de données public qui ne nécessite pas d'authentification, spécifiez`NONE`.
4. Pour l'`Token`option du `--sas-configuration` paramètre, spécifiez le jeton SAS qui permet d'accéder DataSync à votre stockage blob.

   Vous pouvez également fournir des paramètres supplémentaires pour sécuriser vos clés à l'aide de AWS Secrets Manager. Pour plus d'informations, consultez la section Fourniture d'informations d'identification pour les emplacements de stockage.

   Votre jeton SAS fait partie de la chaîne d'URI SAS qui suit l'URI de votre ressource de stockage et un point d'interrogation (?). Un jeton ressemble à ceci :

```
sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=aBBKD
%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

5. (Facultatif) Pour le `--agent-arns` paramètre, spécifiez le nom de ressource Amazon (ARN) de l' DataSync agent qui peut se connecter à votre conteneur.

   Voici un exemple d'ARN d'agent : `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

   Vous pouvez spécifier plusieurs agents. Pour de plus amples informations, veuillez consulter Utilisation de plusieurs DataSync agents.

6. Pour le `--subdirectory` paramètre, spécifiez les segments de chemin si vous souhaitez limiter votre transfert vers un répertoire virtuel de votre conteneur (par exemple,`/my/images`).
7. (Facultatif) Pour le `--access-tier` paramètre, spécifiez le niveau d'accès (`HOTCOOL`, ou`ARCHIVE`) vers lequel vous souhaitez transférer vos objets ou fichiers.

   Ce paramètre s'applique uniquement lorsque vous utilisez cet emplacement comme destination de transfert.
8. (Facultatif) Pour le `--tags` paramètre, spécifiez des paires clé-valeur qui peuvent vous aider à gérer, filtrer et rechercher votre position.

   Nous vous recommandons de créer une balise de nom pour votre emplacement.
9. Exécutez la commande `create-location-azure-blob`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de l'emplacement que vous avez créé. Par exemple :

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh"
}
```

Afficher le lieu Azure Blob Storage de votre transfert

Vous pouvez obtenir des informations sur le lieu DataSync de transfert existant pour votreAzure Blob Storage.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.
3. Choisissez votre Azure Blob Storage emplacement.

   Vous pouvez consulter les informations relatives à votre position, y compris les tâches de DataSync transfert qui l'utilisent.

En utilisant le AWS CLI

1. Copiez la `describe-location-azure-blob` commande suivante :

```
aws datasync describe-location-azure-blob \
  --location-arn "your-azure-blob-location-arn"
```

2. Pour le `--location-arn` paramètre, spécifiez l'ARN de l'Azure Blob Storageemplacement que vous avez créé (par exemple,`arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Exécutez la commande `describe-location-azure-blob`.

   Vous recevez une réponse qui vous indique les détails de votre position. Par exemple :

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh",
    "LocationUri": "azure-blob://my-user.blob.core.windows.net/container-1",
    "AuthenticationType": "SAS",
    "Subdirectory": "/my/images",
    "AgentArns": ["arn:aws:datasync:us-east-1:123456789012:agent/
agent-01234567890deadfb"],
}
```

Mettre à jour le lieu Azure Blob Storage de votre transfert

Si nécessaire, vous pouvez modifier la configuration de votre emplacement dans la console ou en utilisant le AWS CLI.

En utilisant le AWS CLI

1. Copiez la `update-location-azure-blob` commande suivante :

```
aws datasync update-location-azure-blob \
  --location-arn "your-azure-blob-location-arn" \
  --authentication-type "SAS" \
  --sas-configuration '{
      "Token": "your-sas-token"
    }' \
  --agent-arns my-datasync-agent-arn \
  --subdirectory "/path/to/my/data" \
```

```
  --access-tier "access-tier-for-destination"
```

2. Pour le `--location-arn` paramètre, spécifiez l'ARN de l'Azure Blob Storageemplacement que vous mettez à jour (par exemple,`arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Pour le paramètre `--authentication-type`, spécifiez `SAS`.
4. Pour l'`Tokenoption` du `--sas-configuration` paramètre, spécifiez le jeton SAS qui permet d'accéder DataSync à votre stockage blob.

   Le jeton fait partie de la chaîne d'URI SAS qui suit l'URI de la ressource de stockage et un point d'interrogation (`?`). Un jeton ressemble à ceci :

   ```
   sp=r&st=2022-12-20T14:54:52Z&se=2022-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=qCBKD
   %2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
   ```

5. Pour le `--agent-arns` paramètre, spécifiez l'Amazon Resource Name (ARN) de l' DataSync agent que vous souhaitez connecter à votre conteneur.

   Voici un exemple d'ARN d'agent : `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

   Vous pouvez spécifier plusieurs agents. Pour de plus amples informations, veuillez consulter Utilisation de plusieurs DataSync agents.
6. Pour le `--subdirectory` paramètre, spécifiez les segments de chemin si vous souhaitez limiter votre transfert vers un répertoire virtuel de votre conteneur (par exemple,`/my/images`).
7. (Facultatif) Pour le `--access-tier` paramètre, spécifiez le niveau d'accès (`HOTCOOL`, ou`ARCHIVE`) vers lequel vous souhaitez transférer vos objets.

   Ce paramètre s'applique uniquement lorsque vous utilisez cet emplacement comme destination de transfert.

Étapes suivantes

Une fois que vous avez créé un DataSync lieu pour votreAzure Blob Storage, vous pouvez continuer à configurer votre transfert. Voici les prochaines étapes à prendre en compte :

1. Si ce n'est pas déjà fait, créez un autre emplacement où vous prévoyez de transférer vos données vers ou depuis votreAzure Blob Storage.

2. Découvrez comment DataSync gère les métadonnées et les fichiers spéciaux, en particulier si vos lieux de transfert ne disposent pas d'une structure de métadonnées similaire.
3. Configurez le mode de transfert de vos données. Par exemple, vous pouvez uniquement transférer un sous-ensemble de vos données ou supprimer des fichiers de votre stockage blob qui ne se trouvent pas dans votre emplacement source (à condition que votre jeton SAS dispose des autorisations de suppression).
4. Commencez votre transfert.

Configuration des AWS DataSync transferts avec Microsoft Azure Files Actions de PME

Vous pouvez configurer AWS DataSync pour transférer des données vers ou depuis un Microsoft Azure Files Partage SMB (Server Message Block).

> **Tip**
>
> Pour une présentation complète du transfert de données depuis des partages Azure Files SMB vers AWS, consultez le blog sur le AWS stockage.

Fournir un DataSync accès aux partages des PME

DataSync se connecte à votre partage SMB à l'aide du protocole SMB et s'authentifie à l'aide des informations d'identification que vous lui fournissez.

Rubriques

- Versions de protocole SMB prises en charge
- Autorisations requises

Versions de protocole SMB prises en charge

Par défaut, choisit DataSync automatiquement une version du protocole SMB en fonction de la négociation avec votre serveur de fichiers SMB.

Vous pouvez également configurer DataSync pour utiliser une version SMB spécifique, mais nous vous recommandons de le faire uniquement si DataSync vous rencontrez des difficultés pour négocier automatiquement avec le serveur de fichiers SMB. DataSync prend en charge les versions

SMB 1.0 et ultérieures. Pour des raisons de sécurité, nous recommandons d'utiliser SMB version 3.0.2 ou ultérieure. Les versions antérieures, telles que SMB 1.0, contiennent des failles de sécurité connues que les attaquants peuvent exploiter pour compromettre vos données.

Consultez le tableau suivant pour obtenir la liste des options de la DataSync console et de l'API :

Option console	Option d'API	Description
Automatique	`AUTOMATIC`	DataSync et le serveur de fichiers SMB négocient la version la plus élevée de SMB qu'ils supportent mutuellement entre 2.1 et 3.1.1. Il s'agit de l'option recommandée par défaut. Si vous optez pour une version spécifique que votre serveur de fichiers ne prend pas en charge, vous risquez de recevoir une erreur `Operation Not Supported` .
SMB 3.0.2	`SMB3`	Limite la négociation du protocole à la version SMB 3.0.2 uniquement.
SMB 2.1	`SMB2`	Limite la négociation du protocole à la version 2.1 de SMB uniquement.
SMB 2.0	`SMB2_0`	Limite la négociation du protocole à la version 2.0 de SMB uniquement.
SMB 1.0	`SMB1`	Limite la négociation du protocole à la version 1.0 de SMB uniquement.

Autorisations requises

DataSync a besoin d'un utilisateur autorisé à monter et à accéder à votre site SMB. Il peut s'agir d'un utilisateur local sur votre serveur de fichiers Windows ou d'un utilisateur de domaine défini dans votre Microsoft Active Directory.

Pour définir la propriété des objets, DataSync il faut le `SE_RESTORE_NAME` privilège, qui est généralement accordé aux membres des groupes Active Directory intégrés Backup Operators et Domain Admins. L'attribution de ce privilège DataSync à un utilisateur permet également de

garantir des autorisations suffisantes pour les fichiers, les dossiers et les métadonnées des fichiers, à l'exception des listes de contrôle d'accès au système NTFS (SACLs).

Des privilèges supplémentaires sont nécessaires pour copier SACLs. Plus précisément, cela nécessite le `SE_SECURITY_NAME` privilège Windows, qui est accordé aux membres du groupe des administrateurs de domaine. Si vous configurez votre tâche pour qu'elle soit copiée SACLs, assurez-vous que l'utilisateur dispose des privilèges requis. Pour en savoir plus sur la configuration d'une tâche à copier SACLs, consultezConfiguration du mode de gestion des fichiers, des objets et des métadonnées.

Lorsque vous copiez des données entre un serveur de fichiers SMB et le système de fichiers Amazon FSx pour Windows File Server, les emplacements source et de destination doivent appartenir au même domaine Microsoft Active Directory ou avoir une relation de confiance Active Directory entre leurs domaines.

Création de votre emplacement de transfert Azure Files à l'aide de la console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour Location type (Type d'emplacement), choisissez Server Message Block (SMB).

   Vous configurerez cet emplacement comme source ou destination plus tard.
4. Pour les agents, choisissez un ou plusieurs DataSync agents que vous souhaitez connecter à votre partage SMB.

   Si vous choisissez plusieurs agents, assurez-vous de bien comprendre l'utilisation de plusieurs agents pour un même point de vente.
5. Pour le serveur SMB, entrez le nom du système de noms de domaine (DNS) ou l'adresse IP du partage SMB que votre DataSync agent va monter.

   > **Note**
   >
   > Vous ne pouvez pas spécifier d'adresse IP version 6 (IPv6).
6. Dans Nom du partage, entrez le nom du partage exporté par votre partage SMB où les données DataSync seront lues ou écrites.

Vous pouvez inclure un sous-répertoire dans le chemin de partage (par exemple,`/path/to/subdirectory`). Assurez-vous que les autres clients SMB de votre réseau peuvent également monter ce chemin.

Pour copier toutes les données du sous-répertoire, vous DataSync devez être en mesure de monter le partage SMB et d'accéder à toutes ses données. Pour de plus amples informations, veuillez consulter Autorisations requises.

7. (Facultatif) Développez les paramètres supplémentaires et choisissez une version SMB DataSync à utiliser lors de l'accès à votre partage SMB.

   Par défaut, choisit DataSync automatiquement une version en fonction de la négociation avec le partage SMB. Pour plus d'informations, veuillez consulter Versions SMB prises en charge.

8. Dans Utilisateur, entrez un nom d'utilisateur capable de monter votre partage SMB et autorisé à accéder aux fichiers et dossiers concernés par votre transfert.

   Pour de plus amples informations, veuillez consulter Autorisations requises.

9. Dans Mot de passe, entrez le mot de passe de l'utilisateur qui peut monter votre partage SMB et qui est autorisé à accéder aux fichiers et dossiers concernés par votre transfert.

10. (Facultatif) Dans le champ Domaine, entrez le nom de domaine Windows auquel appartient votre partage SMB.

    Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre permet de s'assurer qu' DataSync ils sont connectés au partage approprié.

11. (Facultatif) Choisissez Ajouter un tag pour marquer votre position.

    Les tags sont des paires clé-valeur qui vous permettent de gérer, de filtrer et de rechercher vos emplacements. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

12. Choisissez Créer un emplacement.

Configuration des transferts avec d'autres solutions de stockage d'objets dans le cloud

Vous pouvez ainsi transférer des données entre les services AWS de stockage et les fournisseurs de stockage d'objets cloud suivants : AWS DataSync

- Wasabi Cloud Storage
- DigitalOcean Spaces
- Oracle Cloud Infrastructure Object Storage
- Cloudflare R2 Storage
- Backblaze B2 Cloud Storage
- NAVER Cloud Object Storage
- Alibaba Cloud Object Storage Service
- IBM Cloud Object Storage
- Seagate Lyve Cloud

Un DataSync agent n'est requis que lors du transfert de données entre des systèmes de stockage situés dans d'autres clouds et Amazon EFS ou Amazon FSx, ou lors de l'utilisation de tâches en mode Basic. Vous n'avez pas besoin d'un agent pour transférer des données entre des systèmes de stockage situés dans d'autres clouds et Amazon S3 à l'aide du mode amélioré.

Que vous utilisiez ou non un agent, vous devez également créer un emplacement de transfert pour votre stockage d'objets dans le cloud (en particulier un emplacement de stockage d'objets). DataSync peut utiliser cet emplacement comme source ou destination pour votre transfert.

Fournir un DataSync accès à votre autre espace de stockage d'objets dans le cloud

La manière dont DataSync vous accédez à votre stockage d'objets dans le cloud dépend de plusieurs facteurs, notamment de la compatibilité de votre stockage avec l'API Amazon S3 et des autorisations et informations d'identification DataSync nécessaires pour accéder à votre stockage.

Rubriques

- Compatibilité avec les API Amazon S3
- Autorisations de stockage et points de terminaison
- Informations d'identification de stockage

Compatibilité avec les API Amazon S3

Votre stockage d'objets dans le cloud doit être compatible avec les opérations d'API Amazon S3 suivantes DataSync pour pouvoir vous y connecter :

- `AbortMultipartUpload`

- `CompleteMultipartUpload`
- `CopyObject`
- `CreateMultipartUpload`
- `DeleteObject`
- `DeleteObjects`
- `DeleteObjectTagging`
- `GetBucketLocation`
- `GetObject`
- `GetObjectTagging`
- `HeadBucket`
- `HeadObject`
- `ListObjectsV2`
- `PutObject`
- `PutObjectTagging`
- `UploadPart`

Autorisations de stockage et points de terminaison

Vous devez configurer les autorisations permettant d'accéder DataSync à votre espace de stockage d'objets dans le cloud. Si votre stockage d'objets est un emplacement source, DataSync des autorisations de lecture et de liste sont nécessaires pour le compartiment à partir duquel vous transférez les données. Si votre stockage d'objets est un emplacement de destination, il DataSync nécessite des autorisations de lecture, de liste, d'écriture et de suppression pour le compartiment.

DataSync a également besoin d'un point de terminaison (ou serveur) pour se connecter à votre système de stockage. Le tableau suivant décrit les points de terminaison qui DataSync peuvent être utilisés pour accéder à d'autres solutions de stockage d'objets dans le cloud :

Autre fournisseur de cloud	Point de terminaison
Wasabi Cloud Storage	`S3.`*`region`*`.wasabisys.com`
DigitalOcean Spaces	*`region`*`.digitaloceanspaces.com`

Autre fournisseur de cloud	Point de terminaison
Oracle Cloud Infrastructure Object Storage	`namespace .compat.objectstorage. region.oraclecloud.com`
Cloudflare R2 Storage	`account-id .r2.cloudflarestorage.com`
Backblaze B2 Cloud Storage	`S3.region.backblazeb2.com`
NAVER Cloud Object Storage	`region.object.ncloudstorage.com` (dans la plupart des régions)
Alibaba Cloud Object Storage Service	`region.aliyuncs.com`
IBM Cloud Object Storage	`s3.region.cloud-object-storage.appdomain.cloud`
Seagate Lyve Cloud	`s3.region.lyvecloud.seagate.com`

> **Important**
>
> Pour plus d'informations sur la configuration des autorisations de bucket et pour obtenir des informations actualisées sur les points de terminaison de stockage, consultez la documentation de votre fournisseur de cloud.

Informations d'identification de stockage

DataSync a également besoin des informations d'identification pour accéder au bucket de stockage d'objets impliqué dans votre transfert. Il peut s'agir d'une clé d'accès et d'une clé secrète ou de quelque chose de similaire, selon la façon dont votre fournisseur de stockage cloud fait référence à ces informations d'identification.

Pour plus d'informations, consultez la documentation de votre fournisseur de cloud.

Considérations relatives au transfert depuis un autre stockage d'objets dans le cloud

Lorsque vous envisagez de transférer des objets vers ou depuis un autre fournisseur de stockage dans le cloud en utilisant DataSync, vous devez garder certains points à l'esprit.

Rubriques

- Coûts
- Classes de stockage
- Balises d'objet
- Transfert vers Amazon S3

Coûts

Les frais associés au transfert de données vers et depuis un autre fournisseur de stockage cloud peuvent inclure :

- Exécution d'une EC2 instance Amazon pour votre DataSync agent
- Transférer les données en utilisant DataSync, y compris les frais de demande liés à votre stockage d'objets dans le cloud et à Amazon S3 (si S3 est votre destination de transfert)
- Transfert de données vers ou depuis votre espace de stockage cloud (consultez les tarifs de votre fournisseur de cloud)
- Stockage des données dans un service AWS de stockage pris en charge par DataSync
- Stockage des données chez un autre fournisseur de cloud (vérifiez les tarifs de votre fournisseur de cloud)

Classes de stockage

Certains fournisseurs de stockage dans le cloud proposent des classes de stockage (similaires à Amazon S3) qui ne DataSync peuvent pas être lues sans avoir été restaurées au préalable. Oracle Cloud Infrastructure Object StoragePossède, par exemple, une classe de stockage d'archives. Vous devez restaurer les objets de cette classe de stockage avant de DataSync pouvoir les transférer. Pour plus d'informations, consultez la documentation de votre fournisseur de cloud.

Balises d'objet

Les fournisseurs de cloud ne prennent pas tous en charge les balises d'objet. Ceux qui le font peuvent ne pas autoriser l'interrogation de balises via l'API Amazon S3. Dans les deux cas, votre tâche de DataSync transfert peut échouer si vous essayez de copier des balises d'objets.

Vous pouvez éviter cela en décochant la case Copier les balises d'objets dans la DataSync console lors de la création, du démarrage ou de la mise à jour de votre tâche.

Transfert vers Amazon S3

Lors du transfert vers Amazon S3, DataSync impossible de transférer des objets de plus de 5 To. DataSyncne peut également copier que des métadonnées d'objets d'une taille maximale de 2 Ko.

Création de votre DataSync agent

Un DataSync agent n'est requis que lors du transfert de données entre des systèmes de stockage situés dans d'autres clouds et Amazon EFS ou Amazon FSx, ou lors de l'utilisation de tâches en mode Basic. Vous n'avez pas besoin d'un agent pour transférer des données entre des systèmes de stockage situés dans d'autres clouds et Amazon S3 à l'aide du mode amélioré. Cette section explique comment déployer et activer un agent sur une EC2 instance Amazon dans votre cloud privé virtuel (VPC) dans. AWS

Pour créer un EC2 agent Amazon

1. Déployez un EC2 agent Amazon.
2. Choisissez un point de terminaison de service avec lequel l'agent communique AWS.

   Dans ce cas, nous vous recommandons d'utiliser un point de terminaison de service VPC.
3. Configurez votre réseau pour qu'il fonctionne avec les points de terminaison du service VPC.
4. Activez l'agent.

Création d'un lieu de transfert pour votre autre espace de stockage d'objets dans le cloud

Vous pouvez configurer DataSync pour utiliser votre stockage d'objets dans le cloud comme emplacement source ou de destination.

Avant de commencer

Assurez-vous de savoir comment DataSync accéder à votre espace de stockage d'objets dans le cloud. Vous avez également besoin d'un DataSync agent capable de se connecter à votre espace de stockage d'objets dans le cloud.

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations et Create location.
3. Pour Type d'emplacement, choisissez Stockage d'objets.
4. Dans Serveur, entrez le point de terminaison qui DataSync peut être utilisé pour accéder à votre stockage d'objets dans le cloud :
   - Wasabi Cloud Storage – `S3.`*`region`*`.wasabisys.com`
   - DigitalOcean Spaces – *`region`*`.digitaloceanspaces.com`
   - Oracle Cloud Infrastructure Object Storage – *`namespace`*`.compat.objectstorage.`*`region`*`.oraclecloud.com`
   - Cloudflare R2 Storage – *`account-id`*`.r2.cloudflarestorage.com`
   - Backblaze B2 Cloud Storage – `S3.`*`region`*`.backblazeb2.com`
   - NAVER Cloud Object Storage— *`region`*`.object.ncloudstorage.com` (dans la plupart des régions)
   - Alibaba Cloud Object Storage Service – *`region`*`.aliyuncs.com`
   - IBM Cloud Object Storage – `s3.`*`region`*`.cloud-object-storage.appdomain.cloud`
   - Seagate Lyve Cloud – `s3.`*`region`*`.lyvecloud.seagate.com`
5. Dans le champ Nom du compartiment, entrez le nom du compartiment de stockage d'objets vers ou depuis lequel vous transférez des données.
6. Pour Dossier, entrez un préfixe d'objet. DataSync transfère uniquement les objets portant ce préfixe.
7. Si votre transfert nécessite un agent, choisissez Utiliser des agents, puis choisissez l' DataSync agent capable de se connecter à votre espace de stockage d'objets dans le cloud.
8. Développer Additional settings (Paramètres supplémentaires). Pour le protocole serveur, choisissez HTTPS. Pour le port du serveur, choisissez 443.
9. Faites défiler la page jusqu'à la section Authentification. Assurez-vous que la case Requiert des informations d'identification est cochée, puis fournissez DataSync vos informations d'identification de stockage.

- Dans le champ Clé d'accès, entrez l'ID pour accéder à votre espace de stockage d'objets dans le cloud.
- Pour Clé secrète, fournissez la clé secrète pour accéder à votre stockage d'objets dans le cloud. Vous pouvez soit saisir la clé directement, soit spécifier un AWS Secrets Manager secret contenant la clé. Pour plus d'informations, consultez la section Fourniture d'informations d'identification pour les emplacements de stockage.

10. (Facultatif) Entrez des valeurs pour les champs Clé et Valeur afin de baliser l'emplacement.

    Les balises vous aident à gérer, filtrer et rechercher vos AWS ressources. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

11. Choisissez Créer un emplacement.

Étapes suivantes

Une fois que vous avez créé un DataSync emplacement pour votre stockage d'objets dans le cloud, vous pouvez continuer à configurer votre transfert. Voici les prochaines étapes à prendre en compte :

1. Si ce n'est pas déjà fait, créez un autre emplacement vers ou depuis lequel vous prévoyez de transférer vos données AWS.
2. Découvrez comment DataSync gère les métadonnées et les fichiers spéciaux pour les emplacements de stockage d'objets.
3. Configurez le mode de transfert de vos données. Par exemple, vous souhaitez peut-être uniquement transférer un sous-ensemble de vos données.

   > **Important**
   >
   > Assurez-vous de configurer correctement le mode de DataSync copie des balises d'objets. Pour plus d'informations, consultez les considérations relatives aux balises d'objet.

4. Commencez votre transfert.

Transfert vers ou depuis un stockage compatible S3 sur Snowball Edge

Vous pouvez ainsi transférer des objets entre le stockage compatible Amazon S3 sur un AWS Snowball Edge appareil ou un cluster et l'un des services de AWS stockage suivants : AWS DataSync

- Amazon S3
- Amazon Elastic File System (Amazon EFS)
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Prérequis

Avant de commencer, assurez-vous d'avoir effectué les opérations suivantes :

- Vous avez créé une ressource de AWS stockage vers ou depuis Région AWS laquelle vous prévoyez de transférer des données. Par exemple, il peut s'agir d'un compartiment S3 ou d'un système de fichiers Amazon EFS dans l'est des États-Unis (Virginie du Nord).
- Mise en place d'une connexion réseau étendu (WAN) pour le trafic entrant et sortant de votre environnement de stockage sur site. Par exemple, vous pouvez établir ce type de connexion avec AWS Direct Connect.

  Lorsque vous créerez votre DataSync agent, vous configurerez cette connexion WAN afin de DataSync pouvoir transférer des données entre votre espace de stockage compatible Amazon S3 sur site et votre ressource de stockage dans AWS.
- Vous avez téléchargé et installé le client Snowball Edge.

Fournir DataSync un accès au stockage compatible S3

Pour accéder à votre compartiment de stockage compatible Amazon S3, vous devez DataSync disposer des éléments suivants :

- Informations d'identification utilisateur sur votre appareil ou cluster Snowball Edge qui peuvent accéder au compartiment vers ou depuis lequel vous transférez des données.
- Un certificat HTTPS qui permet DataSync de vérifier l'authenticité de la connexion entre l' DataSync agent et le `s3api` point de terminaison sur votre appareil ou votre cluster.

Rubriques

- Obtenir les informations d'identification utilisateur pour accéder à votre compartiment S3
- Obtenir un certificat pour la connexion du s3api point de terminaison

Obtenir les informations d'identification utilisateur pour accéder à votre compartiment S3

DataSync a besoin de la clé d'accès et de la clé secrète pour un utilisateur qui peut accéder au compartiment avec lequel vous travaillez sur votre appareil ou cluster Snowball Edge.

Pour obtenir les informations d'identification utilisateur permettant d'accéder à votre bucket

1. Ouvrez un terminal et exécutez le client Snowball Edge.

   Pour plus d'informations sur l'exécution du client Snowball Edge, consultez la section Utilisation du client Snowball Edge dans le manuel du développeur.AWS Snowball Edge

2. Pour obtenir les clés d'accès associées à votre appareil ou à votre cluster, exécutez la `snowballEdge` commande suivante :

   ```
   snowballEdge list-access-keys
   ```

3. Dans la sortie, recherchez la clé d'accès au compartiment qui DataSync fonctionnera avec (par exemple,`AKIAIOSFODNN7EXAMPLE`).

4. Pour obtenir la clé d'accès secrète, exécutez la `snowballEdge` commande suivante. *`access-key-for-datasync`*Remplacez-la par la clé d'accès que vous avez trouvée à l'étape précédente.

   ```
   snowballEdge get-secret-access-key --access-key-id access-key-for-datasync
   ```

   La sortie inclut la clé secrète correspondante à la clé d'accès (par exemple,`wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`).

5. Enregistrez la clé d'accès et la clé secrète dans un endroit dont vous vous souviendrez.

   Vous aurez besoin de ces clés pour configurer l'emplacement de la DataSync source pour votre transfert.

Obtenir un certificat pour la connexion du **`s3api`** point de terminaison

Vous avez besoin d'un certificat HTTPS capable de vérifier l'authenticité de la connexion entre votre DataSync agent et un `s3api` point de terminaison sur votre appareil ou cluster Snowball Edge.

Pour obtenir un certificat pour la connexion du **`s3api`** point de terminaison

1. Dans le client Snowball Edge, exécutez la commande suivante : `list-certificates`

   ```
   snowballEdge list-certificates
   ```

   Dans le résultat, prenez note de la `CertificateArn` valeur. Il s'agit du nom de ressource Amazon (ARN) du certificat. Vous avez besoin de l'ARN pour obtenir le contenu du certificat.

2. Exécutez la `get-certificate` commande suivante qui spécifie l'ARN du certificat que vous venez de récupérer :

   ```
   snowballEdge get-certificate --certificate-arn arn:aws:snowball-
   device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
   ```

3. Copiez la sortie, y compris les `END CERTIFICATE` lignes `BEGIN CERTIFICATE` et, et enregistrez-la sous forme de `.pem` fichier.

   Exemple de **`get-certificate`** sortie :

   ```
   -----BEGIN CERTIFICATE-----
   Certificate
   -----END CERTIFICATE-----
   ```

Vous spécifiez ce `.pem` fichier lors de la création de l'emplacement DataSync source de votre transfert.

Création d'un DataSync agent dans votre environnement de stockage sur site

Au cours d'un transfert, DataSync utilise un agent pour lire ou écrire sur le stockage compatible Amazon S3 sur votre appareil ou cluster Snowball Edge.

Cet agent doit être déployé dans votre environnement de stockage sur site où il peut se connecter à votre appareil ou à votre cluster via votre réseau. Par exemple, vous pouvez exécuter l'agent sur un VMware ESXi hyperviseur disposant d'un accès réseau local à votre cluster.

Pour créer un DataSync agent dans votre environnement de stockage sur site

1. Assurez-vous que l'DataSync agent peut s'exécuter sur votre hyperviseur et que vous lui allouez suffisamment de ressources de machine virtuelle (VM).
2. Déployez l'agent dans votre environnement sur site.

   Pour obtenir des instructions, consultez l'une des rubriques suivantes, en fonction du type d'hyperviseur sur lequel vous déployez l'agent :

   - Déployez votre agent sur VMware
   - Déployez votre agent sur une machine basée sur le noyau Linux (KVM)
   - Déployez votre agent sur Microsoft Hyper-V
   - Déployez votre agent sur Amazon EC2

   > **Warning**
   >
   > Nous ne recommandons pas de déployer un agent sur un EC2 agent Amazon pour accéder au stockage sur site en raison de l'augmentation de la latence du réseau.

3. Configurez votre réseau pour autoriser le trafic suivant entre l'agent et votre espace de stockage compatible Amazon S3 :

De	Pour	Protocole et port
DataSync agent	Interface réseau virtuelle (VNI) pour un `s3api` point de terminaison sur votre appareil ou votre cluster.	TCP 443 (HTTPS)

De	Pour	Protocole et port
	Si vous avez un cluster, il peut s'agir de n'importe quel `s3api` point de terminaison VNI.	

Si vous avez besoin de trouver un VNI sur votre appareil ou votre cluster, reportez-vous à la section Description de vos interfaces réseau virtuelles sur Snowball Edge.

4. Choisissez un point de terminaison de service que l'agent utilise pour communiquer avec le DataSync service.
5. Activez votre agent.

Configuration de l'emplacement de la source pour votre transfert

Après avoir créé votre agent, vous pouvez configurer l'emplacement source de votre DataSync transfert.

> **Note**
>
> Les instructions suivantes supposent que vous effectuez un transfert depuis un stockage compatible avec Amazon S3, mais vous pouvez également utiliser cet emplacement comme destination de transfert.

Pour configurer l'emplacement de la source à l'aide de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données. Choisissez Tâches, puis choisissez Créer une tâche.
3. Sur la page Configure source location (Configurer l'emplacement source), choisissez Create a new location (Créer un nouvel emplacement).
4. Pour Type d'emplacement, choisissez Stockage d'objets.
5. Pour les agents, choisissez l' DataSync agent que vous avez créé dans votre environnement de stockage sur site.

6. Pour Server, entrez le VNI du `s3api` point de terminaison utilisé par votre système de stockage compatible Amazon S3.

   Si vous disposez d'un cluster Snowball Edge au lieu d'un seul appareil, vous pouvez spécifier n'importe quel point de terminaison du `s3api` cluster. VNIs
7. Dans le champ Nom du compartiment, entrez le nom du compartiment de stockage compatible Amazon S3 à partir duquel vous transférez des objets.
8. Pour Dossier, entrez un préfixe d'objet.

   DataSync transfère uniquement les objets portant ce préfixe.
9. Pour configurer la DataSync connexion au périphérique ou au cluster Snowball Edge, développez les paramètres supplémentaires et procédez comme suit :

   a. Pour le protocole du serveur, choisissez HTTPS.

   b. Pour Port du serveur, entrez**443**.

   c. Pour Certificat, choisissez le fichier de certificat pour la connexion du `s3api` point de terminaison.
10. Sélectionnez Requiert des informations d'identification, puis entrez la clé d'accès et la clé secrète pour accéder au compartiment de stockage compatible Amazon S3 sur votre appareil ou cluster Snowball Edge.
11. Choisissez Suivant.

Configuration de l'emplacement de destination pour votre transfert

Le lieu de destination de votre transfert doit être le même que celui Région AWS Compte AWS où vous avez créé votre agent.

Avant de commencer : assurez-vous d'avoir configuré l'emplacement source pour votre transfert.

Pour configurer l'emplacement de destination de votre transfert à l'aide de la DataSync console

1. Sur la page Configurer l'emplacement de destination, choisissez Créer un nouvel emplacement ou Choisissez un emplacement existant pour la ressource AWS de stockage vers laquelle vous transférez des objets.

   Si vous créez un nouveau point de vente, consultez l'une des rubriques suivantes :

   - Amazon S3

- Amazon EFS
- FSx pour le serveur de fichiers Windows
- FSx pour Lustre
- FSx pour OpenZFS
- FSx pour ONTAP

2. Lorsque vous avez terminé de configurer l'emplacement de destination, choisissez Next.

Configuration de vos paramètres de transfert

Vous pouvez notamment définir un calendrier de transfert, personnaliser la manière dont l'intégrité de vos données est vérifiée et indiquer si vous souhaitez transférer uniquement un sous-ensemble d'objets. DataSync

Avant de commencer : assurez-vous d'avoir configuré le lieu de destination de votre transfert.

Pour configurer vos paramètres de transfert à l'aide de la DataSync console

1. Sur la page Configurer les paramètres, modifiez les paramètres de transfert ou utilisez les valeurs par défaut.

   Pour plus d'informations sur ces paramètres, consultez la page Choisir quels AWS DataSync transferts.
2. Choisissez Suivant.
3. Vérifiez les détails de votre transfert, puis choisissez Créer une tâche.

Commencer votre transfert

Une fois que vous avez créé votre tâche de transfert, vous êtes prêt à commencer à déplacer les données. Pour obtenir des instructions sur le démarrage d'une tâche à l'aide de la DataSync console ou AWS CLI consultez la section Démarrage de votre tâche.

Limites

- Si votre système de stockage source utilise le protocole NFS (tel qu'Amazon EFS), DataSync vous ne pouvez pas transférer de fichiers contenant des liens physiques vers un appareil Snowball Edge.

- DataSync Impossible de transférer des objets de plus de 1 024 octets d'un appareil Snowball Edge vers un compartiment S3. Pour plus d'informations, consultez le guide de l'utilisateur Amazon S3.

Création d'une tâche pour le transfert de vos données

Une tâche décrit où et comment les données sont AWS DataSync transférées. Une tâche comprend les éléments suivants :

- Emplacement de la source : système ou service de stockage à partir duquel DataSync les données sont transférées.
- Lieu de destination : système ou service de stockage DataSync vers lequel les données sont transférées.
- Options des tâches : paramètres tels que les fichiers à transférer, le mode de vérification des données, le moment d'exécution de la tâche, etc.
- Exécutions de tâches : lorsque vous exécutez une tâche, cela s'appelle une exécution de tâche.

Création de votre tâche

Lorsque vous créez une DataSync tâche, vous spécifiez vos emplacements source et de destination. Vous pouvez également personnaliser votre tâche en choisissant les fichiers à transférer, la manière dont les métadonnées sont traitées, en établissant un calendrier, etc.

Avant de créer votre tâche, assurez-vous de comprendre le fonctionnement des DataSync transferts et vérifiez les quotas de tâches.

> **Important**
>
> Si vous prévoyez de transférer des données depuis ou vers un site Amazon S3, examinez comment cela DataSync peut affecter les frais de votre demande S3 et la page de DataSync tarification avant de commencer.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Assurez-vous que vous vous trouvez dans l'un des Régions AWS endroits où vous prévoyez de transférer des données.

3. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
4. Sur la page Configurer l'emplacement de la source, créez ou choisissez un emplacement source, puis choisissez Suivant.
5. Sur la page Configurer l'emplacement de destination, créez ou choisissez un emplacement de destination, puis choisissez Suivant.
6. (Recommandé) Sur la page Configurer les paramètres, attribuez à votre tâche un nom dont vous vous souviendrez.
7. Tout en restant sur la page Configurer les paramètres, choisissez les options de vos tâches ou utilisez les paramètres par défaut.

   Certaines des options suivantes pourraient vous intéresser :

   - Spécifiez le mode de tâche que vous souhaitez utiliser.
   - Spécifiez les données à transférer à l'aide d'un manifeste ou de filtres.
   - Configurez le mode de gestion des métadonnées des fichiers et de vérification de l'intégrité des données.
   - Surveillez votre transfert à l'aide de rapports de tâches ou d'Amazon CloudWatch. Nous vous recommandons de configurer une sorte de surveillance pour votre tâche.

   Lorsque vous avez terminé, sélectionnez Next.
8. Vérifiez la configuration de vos tâches, puis choisissez Créer une tâche.

Vous êtes prêt à commencer votre tâche.

À l'aide du AWS CLI

Une fois que vous avez créé vos emplacements DataSync source et de destination, vous pouvez créer votre tâche.

1. Dans vos AWS CLI paramètres, assurez-vous que vous utilisez l'un des Régions AWS endroits où vous prévoyez de transférer des données.
2. Copiez la `create-task` commande suivante :

```
aws datasync create-task \
```

```
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-
id" \
  --destination-location-arn "arn:aws:datasync:us-east-1:account-
id:location/location-id" \
  --name "task-name"
```

3. Pour`--source-location-arn`, spécifiez l'Amazon Resource Name (ARN) de votre emplacement source.
4. Pour`--destination-location-arn`, spécifiez l'ARN de votre position de destination.

   Si vous transférez plusieurs Régions AWS comptes, assurez-vous que l'ARN inclut l'autre région ou l'autre identifiant de compte.
5. (Recommandé) Pour`--name`, spécifiez un nom mémorisable pour votre tâche.
6. Spécifiez les autres options de tâche selon vos besoins. Certaines des options suivantes pourraient vous intéresser :

   - Spécifiez les données à transférer à l'aide d'un manifeste ou de filtres.
   - Configurez le mode de gestion des métadonnées des fichiers et de vérification de l'intégrité des données.
   - Surveillez votre transfert à l'aide de rapports de tâches ou d'Amazon CloudWatch. Nous vous recommandons de configurer une sorte de surveillance pour votre tâche.

   Pour plus d'options, voir create-task. Voici un exemple de `create-task` commande qui spécifie plusieurs options :

```
aws datasync create-task \
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-
id" \
  --destination-location-arn "arn:aws:datasync:us-east-1:account-
id:location/location-id" \
  --cloud-watch-log-group-arn "arn:aws:logs:region:account-id" \
  --name "task-name" \
  --options
 VerifyMode=NONE,OverwriteMode=NEVER,Atime=BEST_EFFORT,Mtime=PRESERVE,Uid=INT_VALUE,Gid=INT
```

7. Exécutez la commande `create-task`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de la tâche que vous avez créée. Par exemple :

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Vous êtes prêt à commencer votre tâche.

Statuts des tâches

Lorsque vous créez une DataSync tâche, vous pouvez vérifier son statut pour voir si elle est prête à être exécutée.

État de la console	État de l'API	Description
Disponible	`AVAILABLE`	La tâche est prête à démarrer le transfert de données.
En cours d'exécution	`RUNNING`	L'exécution d'une tâche est en cours. Pour de plus amples informations, veuillez consulter Statuts d'exécution des tâches.
Unavailable	`UNAVAILABLE`	Un DataSync agent utilisé par la tâche est hors ligne. Pour de plus amples informations, consultez Que dois-je faire si mon agent est hors ligne ?.
Mis en file d'attente	`QUEUED`	Une autre exécution de tâche utilisant le même DataSync agent est en cours. Pour de plus amples informations, veuillez consulter Savoir quand votre tâche est en file d'attente.

Partitionnement de grands ensembles de données avec plusieurs tâches

Si vous transférez un ensemble de données volumineux, par exemple si vous migrez des millions de fichiers ou d'objets, nous vous recommandons de partitionner votre ensemble de données en plusieurs DataSync tâches. Le partitionnement de vos données sources entre plusieurs tâches

(et éventuellement des agents, en fonction de vos sites) permet de réduire le temps nécessaire DataSync à la préparation et au transfert de vos données.

Envisagez certaines des manières dont vous pouvez partitionner un ensemble de données volumineux entre plusieurs DataSync tâches :

- Créez des tâches qui transfèrent des dossiers distincts. Par exemple, vous pouvez créer deux tâches qui ciblent `/FolderA` et`/FolderB`, respectivement, dans votre stockage source.
- Créez des tâches qui transfèrent des sous-ensembles de fichiers, d'objets et de dossiers à l'aide d'un manifeste ou de filtres.

Sachez que cette approche peut augmenter les I/O opérations sur votre stockage et affecter la bande passante de votre réseau. Pour plus d'informations, consultez le blog Comment accélérer vos transferts de données grâce à des architectures DataSync évolutives.

Segmentation des données transférées à l'aide de plusieurs tâches

Si vous transférez différents ensembles de données vers la même destination, vous pouvez créer plusieurs tâches pour segmenter les données que vous transférez.

Par exemple, si vous effectuez un transfert vers le même compartiment S3 nommé`MyBucket`, vous pouvez créer différents préfixes dans le compartiment correspondant à chaque tâche. Cette approche évite les conflits de noms de fichiers entre les ensembles de données et vous permet de définir des autorisations différentes pour chaque préfixe. Voici comment vous pouvez le configurer :

1. Créez trois préfixes dans la destination `MyBucket` nommée `task1`task2, et `task3` :
   - `s3://MyBucket/task1`
   - `s3://MyBucket/task2`
   - `s3://MyBucket/task3`
2. Créez trois DataSync tâches nommées `task1`task2, et `task3` transférez-les vers le préfixe correspondant dans`MyBucket`.

Choix d'un mode de tâche pour le transfert de données

Votre AWS DataSync tâche peut être exécutée dans l'un des modes suivants :

- Mode amélioré : transférez un nombre pratiquement illimité d'objets avec des performances supérieures à celles du mode de base. Les tâches en mode amélioré optimisent le processus de transfert de données en listant, préparant, transférant et vérifiant les données en parallèle. Le mode amélioré est actuellement disponible pour les transferts entre les sites Amazon S3, les transferts entre Azure Blob et Amazon S3 sans agent, et les transferts entre d'autres clouds et Amazon S3 sans agent.
- Mode de base : transférez des fichiers ou des objets entre le AWS stockage et tous les autres DataSync emplacements pris en charge. Les tâches en mode de base sont soumises à des quotas sur le nombre de fichiers, d'objets et de répertoires dans un ensemble de données. Le mode de base prépare, transfère et vérifie les données de manière séquentielle, ce qui le rend plus lent que le mode amélioré pour la plupart des charges de travail.

Comprendre les différences entre les modes de tâche

Les informations suivantes peuvent vous aider à déterminer le mode de tâche à utiliser.

Capacité	Comportement en mode amélioré	Comportement du mode de base
Performances	DataSync répertorie, prépare, transfère et vérifie vos données en parallèle. Fournit des performances supérieur es à celles du mode de base pour la plupart des charges de travail (telles que le transfert d'objets volumineux)	DataSync prépare, transfère et vérifie vos données de manière séquentielle. Les performances sont plus lentes que le mode amélioré pour la plupart des charges de travail
Nombre d'éléments d'un ensemble de données qui DataSync peuvent être utilisés par exécution de tâche	Un nombre pratiquement illimité d'objets	Des quotas s'appliquent
Compteurs et métriques de transfert de données	Plus de compteurs et de métriques que le mode de base, tels que le nombre d'objets trouvés DataSync à	Moins de compteurs et de métriques que le mode amélioré

Capacité	Comportement en mode amélioré	Comportement du mode de base
	votre emplacement source et le nombre d'objets préparés lors de chaque exécution de tâche	
Journalisation	Journaux structurés (format JSON)	Journaux non structurés
Emplacements pris en charge	Actuellement pour les transfert s entre les sites Amazon S3, les transferts entre Azure Blob et Amazon S3 sans agent, et les transferts entre d'autres clouds et Amazon S3 sans agent.	Pour les transferts entre tous les sites DataSync compatibl es
Options de vérification des données	DataSync vérifie uniquement les données transférées	DataSync vérifie toutes les données par défaut
Limites de bande passante	Ne s'applique pas	Pris en charge
Coût	Pour plus d'informations, consultez la page de DataSync tarification	Pour plus d'informations, consultez la page de DataSync tarification

Capacité	Comportement en mode amélioré	Comportement du mode de base
Gestion des défaillances pour les balises d'objet non prises en charge	Pour les transferts de stockage dans le cloud vers ou depuis des emplaceme nts qui ne prennent pas en charge le balisage d'objets, l'exécution de la tâche échouera immédiatement si l'`ObjectTags` option n'est pas spécifiée ou si elle est définie sur. `PRESERVE`	Pour les transferts de stockage dans le cloud vers ou depuis des emplacements qui ne prennent pas en charge le balisage d'objets, l'exécuti on des tâches s'exécutera normalement, mais les échecs par objet seront signalés pour les objets balisés si l'`ObjectTags` option n'est pas spécifiée ou si elle est définie sur. `PRESERVE`

Choix d'un mode de tâche

Vous pouvez choisir le mode amélioré uniquement pour les transferts entre les sites Amazon S3, les transferts entre Azure Blob et Amazon S3 sans agent, et les transferts entre d'autres clouds et Amazon S3 sans agent. Dans le cas contraire, vous devez utiliser le mode de base. Par exemple, un transfert d'un emplacement NFS sur site vers un emplacement S3 nécessite le mode Basic.

Les options et les performances de vos tâches peuvent varier en fonction du mode de tâche que vous choisissez. Une fois que vous avez créé votre tâche, vous ne pouvez pas modifier le mode de tâche.

Autorisations requises

Pour créer une tâche en mode amélioré, le rôle IAM que vous utilisez doit disposer DataSync de l'`iam:CreateServiceLinkedRole`autorisation.

Pour vos autorisations DataSync d'utilisateur, pensez à utiliser AWSDataSyncFullAccess. Il s'agit d'une politique AWS gérée qui fournit à l'utilisateur un accès complet DataSync et un accès minimal à ses dépendances.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.

2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Pour le mode tâche, choisissez l'une des options suivantes :

   - Amélioré
   - Base

   Pour de plus amples informations, veuillez consulter Comprendre les différences entre les modes de tâche.
5. Tout en restant sur la page Configurer les paramètres, choisissez d'autres options de tâche ou utilisez les paramètres par défaut.

   Certaines des options suivantes pourraient vous intéresser :

   - Spécifiez les données à transférer à l'aide d'un manifeste ou de filtres.
   - Configurez le mode de gestion des métadonnées des fichiers et de vérification de l'intégrité des données.
   - Surveillez votre transfert à l'aide de rapports de tâches ou d'Amazon CloudWatch Logs.

   Lorsque vous avez terminé, sélectionnez Next.
6. Vérifiez la configuration de vos tâches, puis choisissez Créer une tâche.

À l'aide du AWS CLI

1. Dans vos AWS CLI paramètres, assurez-vous que vous utilisez l'un des emplacements Régions AWS où vous prévoyez de transférer des données.
2. Copiez la `create-task` commande suivante :

```
aws datasync create-task \
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
```

```
  --destination-location-arn "arn:aws:datasync:us-east-1:account-
id:location/location-id" \
  --task-mode "ENHANCED-or-BASIC"
```

3. Pour`--source-location-arn`, spécifiez l'Amazon Resource Name (ARN) de votre emplacement source.
4. Pour`--destination-location-arn`, spécifiez l'ARN de votre position de destination.

   Si vous transférez plusieurs Régions AWS comptes, assurez-vous que l'ARN inclut l'autre région ou l'autre identifiant de compte.
5. Pour`--task-mode`, spécifiez `ENHANCED` ou`BASIC`.

   Pour de plus amples informations, veuillez consulter Comprendre les différences entre les modes de tâche.
6. Spécifiez les autres options de tâche selon vos besoins. Certaines des options suivantes pourraient vous intéresser :

   - Spécifiez les données à transférer à l'aide d'un manifeste ou de filtres.
   - Configurez le mode de gestion des métadonnées des fichiers et de vérification de l'intégrité des données.
   - Surveillez votre transfert à l'aide de rapports de tâches ou d'Amazon CloudWatch Logs.

   Pour plus d'options, voir create-task. Voici un exemple de `create-task` commande qui spécifie le mode amélioré et plusieurs autres options :

```
aws datasync create-task \
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-
id" \
  --destination-location-arn "arn:aws:datasync:us-east-1:account-
id:location/location-id" \
  --name "task-name" \
  --task-mode "ENHANCED" \
  --options
 TransferMode=CHANGED,VerifyMode=ONLY_FILES_TRANSFERRED,ObjectTags=PRESERVE,LogLevel=TRANSF
```

7. Exécutez la commande `create-task`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de la tâche que vous avez créée. Par exemple :

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Utilisation de l' DataSync API

Vous pouvez définir le mode de DataSync tâche en configurant le `TaskMode` paramètre dans l'CreateTaskopération.

Choisir quels AWS DataSync transferts

AWS DataSync vous permet de choisir les éléments à transférer et la manière dont vous souhaitez que vos données soient traitées. Certaines options incluent :

- Transférer une liste exacte de fichiers ou d'objets à l'aide d'un manifeste.
- Inclure ou exclure certains types de données dans votre transfert à l'aide d'un filtre.
- Pour les transferts récurrents, déplacer uniquement les données modifiées depuis le dernier transfert
- Remplacer les données de l'emplacement de destination pour qu'elles correspondent à celles de l'emplacement source.
- Choix des métadonnées de fichier ou d'objet à conserver entre vos emplacements de stockage.

Rubriques

- Transfert de fichiers ou d'objets spécifiques à l'aide d'un manifeste
- Transfert de fichiers, d'objets et de dossiers spécifiques à l'aide de filtres
- Comprendre le mode de DataSync gestion des métadonnées des fichiers et des objets
- Liens et répertoires copiés par AWS DataSync
- Configuration du mode de gestion des fichiers, des objets et des métadonnées

Transfert de fichiers ou d'objets spécifiques à l'aide d'un manifeste

Un manifeste est une liste de fichiers ou d'objets que vous AWS DataSync souhaitez transférer. Par exemple, au lieu de tout transférer dans un compartiment S3 contenant potentiellement des millions d'objets, il ne DataSync transfère que les objets que vous listez dans votre manifeste.

Les manifestes sont similaires aux filtres, mais ils vous permettent d'identifier exactement les fichiers ou les objets à transférer plutôt que les données correspondant à un modèle de filtre.

Création de votre manifeste

Un manifeste est un fichier au format CSV (valeurs séparées par des virgules) qui répertorie les fichiers ou les objets que vous souhaitez transférer dans votre emplacement source. DataSync Si votre source est un compartiment S3, vous pouvez également indiquer la version d'un objet à transférer.

Rubriques

- Consignes
- Exemples de manifestes

Consignes

Utilisez ces directives pour vous aider à créer un manifeste compatible avec DataSync.

Do

- Spécifiez le chemin complet de chaque fichier ou objet que vous souhaitez transférer.

  Vous ne pouvez pas spécifier uniquement un répertoire ou un dossier dans le but de transférer tout son contenu. Dans ces situations, pensez à utiliser un filtre d'inclusion au lieu d'un manifeste.
- Assurez-vous que le chemin de chaque fichier ou objet est relatif au chemin de montage, au dossier, au répertoire ou au préfixe que vous avez spécifié lors de la configuration de votre emplacement DataSync source.

  Supposons, par exemple, que vous configurez un emplacement S3 avec un préfixe nomméphotos. Ce préfixe inclut un objet `my-picture.png` que vous souhaitez transférer. Dans le manifeste, il suffit alors de spécifier l'objet (`my-picture.png`) au lieu du préfixe et de l'objet (`photos/my-picture.png`).
- Pour spécifier la version de l'objet Amazon S3 IDs, séparez le chemin et l'ID de version de l'objet à l'aide d'une virgule.

  L'exemple suivant montre une entrée de manifeste comportant deux champs. Le premier champ inclut un objet nommé`picture1.png`. Le deuxième champ est séparé par une virgule et inclut un ID de version de `111111` :

```
picture1.png,111111
```

- Utilisez des guillemets dans les situations suivantes :
  - Lorsqu'un chemin contient des caractères spéciaux (virgules, guillemets et fins de ligne) :

    `"filename,with,commas.txt"`
  - Lorsqu'un chemin s'étend sur plusieurs lignes :

    ```
    "this
    is
    a
    filename.txt"
    ```
  - Lorsqu'un chemin inclut des guillemets :

    `filename""with""quotes.txt`

    Cela représente un chemin nommé`filename"with"quotes.txt`.

  Ces règles de devis s'appliquent également aux champs d'ID de version. En général, si un champ de manifeste contient un guillemet, vous devez y échapper par un autre guillemet.
- Séparez chaque entrée de fichier ou d'objet par une nouvelle ligne.

  Vous pouvez séparer les lignes en utilisant des sauts de ligne de style Linux (alimentation en ligne ou retour en chariot) ou Windows (retour en chariot suivi d'une alimentation en ligne).
- Enregistrez votre manifeste (par exemple, `my-manifest.csv` ou`my-manifest.txt`).
- Téléchargez le manifeste dans un compartiment S3 auquel il est DataSync possible d'accéder.

  Il n'est pas nécessaire que ce compartiment se trouve dans le même compte Région AWS ou dans le même compte que celui que vous utilisez DataSync.

Don't

- Spécifiez uniquement un répertoire ou un dossier dans le but de transférer tout son contenu.

  Un manifeste ne peut inclure que les chemins complets vers les fichiers ou les objets que vous souhaitez transférer. Si vous configurez votre emplacement source pour utiliser un chemin de

montage, un dossier, un répertoire ou un préfixe spécifique, vous n'êtes pas obligé de l'inclure dans votre manifeste.

- Spécifiez un chemin de fichier ou d'objet de plus de 4 096 caractères.
- Spécifiez un chemin de fichier, un chemin d'objet ou un ID de version d'objet Amazon S3 supérieur à 1 024 octets.
- Spécifiez les chemins de fichiers ou d'objets dupliqués.
- Incluez un ID de version d'objet si votre emplacement source n'est pas un compartiment S3.
- Incluez plus de deux champs dans une entrée de manifeste.

  Une entrée ne peut inclure qu'un chemin de fichier ou d'objet et (le cas échéant) un ID de version d'objet Amazon S3.
- Incluez des caractères non conformes au codage UTF-8.
- Incluez des espaces involontaires dans vos champs de saisie en dehors des guillemets.

Exemples de manifestes

Utilisez ces exemples pour vous aider à créer un manifeste qui fonctionne avec DataSync.

Manifeste avec chemins complets de fichiers ou d'objets

L'exemple suivant montre un manifeste avec les chemins complets des fichiers ou des objets à transférer.

```
photos/picture1.png
photos/picture2.png
photos/picture3.png
```

Manifeste avec uniquement des clés d'objet

L'exemple suivant montre un manifeste contenant des objets à transférer depuis un emplacement source Amazon S3. L'emplacement étant configuré avec le préfixe`photos`, seules les clés de l'objet sont spécifiées.

```
picture1.png
picture2.png
picture3.png
```

Manifeste avec chemins d'objets et version IDs

Les deux premières entrées de l'exemple de manifeste suivant incluent des versions d'objets Amazon S3 spécifiques à transférer.

```
photos/picture1.png,111111
photos/picture2.png,121212
photos/picture3.png
```

Manifeste avec caractères UTF-8

L'exemple suivant montre un manifeste contenant des fichiers contenant des caractères UTF-8.

```
documents/résumé1.pdf
documents/résumé2.pdf
documents/résumé3.pdf
```

Fournir DataSync l'accès à votre manifeste

Vous avez besoin d'un rôle AWS Identity and Access Management (IAM) qui donne DataSync accès à votre manifeste dans son compartiment S3. Ce rôle doit inclure les autorisations suivantes :

- `s3:GetObject`
- `s3:GetObjectVersion`

Vous pouvez générer ce rôle automatiquement dans la DataSync console ou le créer vous-même.

> **Note**
>
> Si votre manifeste se trouve dans un autre Compte AWS format, vous devez créer ce rôle manuellement.

Création automatique du rôle IAM

Lorsque vous créez ou lancez une tâche de transfert dans la console, vous DataSync pouvez créer un rôle IAM avec les `s3:GetObjectVersion` autorisations `s3:GetObject` et les autorisations dont vous avez besoin pour accéder à votre manifeste.

Autorisations requises pour créer automatiquement le rôle

Pour créer automatiquement le rôle, assurez-vous que le rôle que vous utilisez pour accéder à la DataSync console dispose des autorisations suivantes :

- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam:AttachRolePolicy`

Création du rôle IAM (même compte)

Vous pouvez créer manuellement le rôle IAM qui DataSync doit accéder à votre manifeste. Les instructions suivantes supposent que vous vous trouvez dans le même Compte AWS emplacement que celui que vous utilisez DataSync et que le compartiment S3 de votre manifeste se trouve.

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles, puis sélectionnez Créer un rôle.
3. Sur la page Sélectionner une entité de confiance, pour Type d'entité de confiance, sélectionnez Service AWS.
4. Pour Cas d'utilisation, choisissez DataSyncdans la liste déroulante et sélectionnez DataSync. Choisissez Suivant.
5. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant). Donnez un nom à votre rôle et choisissez Créer un rôle.
6. Sur la page Rôles, recherchez le rôle que vous venez de créer et choisissez son nom.
7. Sur la page de détails du rôle, choisissez l'onglet Autorisations. Choisissez Ajouter des autorisations, puis Créer une politique en ligne.
8. Choisissez l'onglet JSON et collez l'exemple de politique suivant dans l'éditeur de politiques :

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DataSyncAccessManifest",
        "Effect": "Allow",
        "Action": [
```

```
            "s3:GetObject",
            "s3:GetObjectVersion"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/my-manifest.csv"
    }]
}
```

9. Dans l'exemple de politique que vous venez de coller, remplacez les valeurs suivantes par les vôtres :

   a. `amzn-s3-demo-bucket`Remplacez-le par le nom du compartiment S3 qui héberge votre manifeste.

   b. `my-manifest.csv`Remplacez-le par le nom de fichier de votre manifeste.

10. Choisissez Suivant. Donnez un nom à votre politique et choisissez Create policy.

11. (Recommandé) Pour éviter le problème de confusion entre les services adjoints, procédez comme suit :

    a. Sur la page de détails du rôle, choisissez l'onglet Relations de confiance. Choisissez Edit trust policy (Modifier la politique d'approbation).

    b. Mettez à jour la politique de confiance en utilisant l'exemple suivant, qui inclut les clés de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale :

       JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
            "Service": "datasync.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
            "aws:SourceAccount": "555555555555"
            },
            "ArnLike": {
            "aws:SourceArn": "arn:aws:datasync:us-east-1:555555555555:*"
            }
```

```
            }
        }
    ]
}
```

- Remplacez chaque instance *account-id* par l' Compte AWS ID que vous utilisez DataSync.
- *region*Remplacez-le Région AWS par celui que vous utilisez DataSync.

c. Choisissez Mettre à jour une politique.

Vous avez créé un rôle IAM qui permet d'accéder DataSync à votre manifeste. Spécifiez ce rôle lors de la création ou du démarrage de votre tâche.

Création du rôle IAM (compte différent)

Si votre manifeste se trouve dans un compartiment S3 appartenant à un autre compartiment Compte AWS, vous devez créer manuellement le rôle IAM qui permet DataSync d'accéder au manifeste. Ensuite, dans l' Compte AWS endroit où se trouve votre manifeste, vous devez inclure le rôle dans la politique du compartiment S3.

Création du rôle

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles, puis sélectionnez Créer un rôle.
3. Sur la page Sélectionner une entité de confiance, pour Type d'entité de confiance, sélectionnez Service AWS.
4. Pour Cas d'utilisation, choisissez DataSyncdans la liste déroulante et sélectionnez DataSync. Choisissez Suivant.
5. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant). Donnez un nom à votre rôle et choisissez Créer un rôle.
6. Sur la page Rôles, recherchez le rôle que vous venez de créer et choisissez son nom.
7. Sur la page de détails du rôle, choisissez l'onglet Autorisations. Choisissez Ajouter des autorisations, puis Créer une politique en ligne.
8. Choisissez l'onglet JSON et collez l'exemple de politique suivant dans l'éditeur de politiques :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DataSyncAccessManifest",
        "Effect": "Allow",
        "Action": [
            "s3:GetObject",
            "s3:GetObjectVersion"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/my-manifest.csv"
    }]
}
```

9. Dans l'exemple de politique que vous venez de coller, remplacez les valeurs suivantes par les vôtres :

   a. *amzn-s3-demo-bucket*Remplacez-le par le nom du compartiment S3 qui héberge votre manifeste.

   b. *my-manifest.csv*Remplacez-le par le nom de fichier de votre manifeste.

10. Choisissez Suivant. Donnez un nom à votre politique et choisissez Create policy.

11. (Recommandé) Pour éviter le problème de confusion entre les services adjoints, procédez comme suit :

    a. Sur la page de détails du rôle, choisissez l'onglet Relations de confiance. Choisissez Edit trust policy (Modifier la politique d'approbation).

    b. Mettez à jour la politique de confiance en utilisant l'exemple suivant, qui inclut les clés de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale :

    JSON

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

```
            "Service": "datasync.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
            "aws:SourceAccount": "000000000000"
            },
            "ArnLike": {
            "aws:SourceArn": "arn:aws:datasync:us-east-1:000000000000:*"
            }
        }
    }
  ]
}
```

- Remplacez chaque instance *account-id* de par l' Compte AWS ID que vous utilisez DataSync.
- *region*Remplacez-le Région AWS par celui que vous utilisez DataSync.

c. Choisissez Mettre à jour une politique.

Vous avez créé le rôle IAM que vous pouvez inclure dans votre politique de compartiment S3.

Mettre à jour votre politique de compartiment S3 avec le rôle

Une fois que vous avez créé le rôle IAM, vous devez l'ajouter à la politique du compartiment S3 dans l'autre Compte AWS endroit où se trouve votre manifeste.

1. Dans le AWS Management Console, passez au compte contenant le compartiment S3 de votre manifeste.
2. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
3. Sur la page détaillée du bucket, choisissez l'onglet Permissions.
4. Sous Politique de compartiment, choisissez Modifier et procédez comme suit pour modifier votre politique de compartiment S3 :

   a. Mettez à jour le contenu de l'éditeur pour inclure les déclarations de politique suivantes :

```
{
  "Version": "2008-10-17",
  "Statement": [
```

```
    {
      "Sid": "DataSyncAccessManifestBucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:role/datasync-role"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

b. *account-id*Remplacez-le par l' Compte AWS identifiant du compte que vous utilisez DataSync .

c. *datasync-role*Remplacez-le par le rôle IAM que vous venez de créer et qui permet d'accéder DataSync à votre manifeste.

d. *amzn-s3-demo-bucket*Remplacez-le par le nom du compartiment S3 qui héberge votre manifeste dans l'autre Compte AWS.

5. Sélectionnez Enregistrer les modifications.

Vous avez créé un rôle IAM qui permet d'accéder DataSync à votre manifeste dans l'autre compte. Spécifiez ce rôle lors de la création ou du démarrage de votre tâche.

Spécification de votre manifeste lors de la création d'une tâche

Vous pouvez spécifier le manifeste que vous DataSync souhaitez utiliser lors de la création d'une tâche.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Tâches, puis sélectionnez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.

4. Pour le contenu à analyser, sélectionnez Fichiers, objets et dossiers spécifiques, puis sélectionnez Utiliser un manifeste.
5. Pour l'URI S3, choisissez votre manifeste hébergé sur un compartiment S3.

   Vous pouvez également saisir l'URI (par exemple,`s3://bucket/prefix/my-manifest.csv`).
6. Pour la version de l'objet, choisissez la version du manifeste que vous DataSync souhaitez utiliser.

   Par défaut, DataSync utilise la dernière version de l'objet.
7. Pour le rôle d'accès au manifeste, effectuez l'une des opérations suivantes :

   - Choisissez Autogenerate pour DataSync créer automatiquement un rôle IAM doté des autorisations requises pour accéder à votre manifeste dans son compartiment S3.
   - Choisissez un rôle IAM existant qui peut accéder à votre manifeste.

   Pour de plus amples informations, veuillez consulter Fournir DataSync l'accès à votre manifeste.
8. Configurez les autres paramètres de tâche dont vous avez besoin, puis choisissez Next.
9. Choisissez Créer tâche.

À l'aide du AWS CLI

1. Copiez la `create-task` commande suivante :

```
aws datasync create-task \
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh \
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/loc-
abcdefgh12345678 \
  --manifest-config {
      "Source": {
        "S3": {
            "ManifestObjectPath": "s3-object-key-of-manifest",
            "BucketAccessRoleArn": "bucket-iam-role",
            "S3BucketArn": "amzn-s3-demo-bucket-arn",
            "ManifestObjectVersionId": "manifest-version-to-use"
        }
      }
```

```
}
```

2. Pour le `--source-location-arn` paramètre, spécifiez l'Amazon Resource Name (ARN) de l'emplacement à partir duquel vous transférez les données.
3. Pour le `--destination-location-arn` paramètre, spécifiez l'ARN de l'emplacement vers lequel vous transférez les données.
4. Pour le `--manifest-config` paramètre, procédez comme suit :
   - `ManifestObjectPath`— Spécifiez la clé d'objet S3 de votre manifeste.
   - `BucketAccessRoleArn`— Spécifiez le rôle IAM qui permet d'accéder DataSync à votre manifeste dans son compartiment S3.

     Pour de plus amples informations, veuillez consulter Fournir DataSync l'accès à votre manifeste.

   - `S3BucketArn`— Spécifiez l'ARN du compartiment S3 qui héberge votre manifeste.
   - `ManifestObjectVersionId`— Spécifiez la version du manifeste que vous DataSync souhaitez utiliser.

     Par défaut, DataSync utilise la dernière version de l'objet.
5. Exécutez la `create-task` commande pour créer votre tâche.

Lorsque vous êtes prêt, vous pouvez commencer votre tâche de transfert.

Spécification de votre manifeste lors du démarrage d'une tâche

Vous pouvez spécifier le manifeste que vous DataSync souhaitez utiliser lors de l'exécution d'une tâche.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Tâches, puis choisissez la tâche que vous souhaitez démarrer.
3. Sur la page d'aperçu des tâches, choisissez Démarrer, puis sélectionnez Démarrer avec des options de remplacement.

4. Pour le contenu à analyser, sélectionnez Fichiers, objets et dossiers spécifiques, puis sélectionnez Utiliser un manifeste.
5. Pour l'URI S3, choisissez votre manifeste hébergé sur un compartiment S3.

   Vous pouvez également saisir l'URI (par exemple,`s3://bucket/prefix/my-manifest.csv`).
6. Pour la version de l'objet, choisissez la version du manifeste que vous DataSync souhaitez utiliser.

   Par défaut, DataSync utilise la dernière version de l'objet.
7. Pour le rôle d'accès au manifeste, effectuez l'une des opérations suivantes :

   - Choisissez Autogenerate pour DataSync créer automatiquement un rôle IAM afin d'accéder à votre manifeste dans son compartiment S3.
   - Choisissez un rôle IAM existant qui peut accéder à votre manifeste.

   Pour de plus amples informations, veuillez consulter Fournir DataSync l'accès à votre manifeste.
8. Choisissez Démarrer pour commencer votre transfert.

À l'aide du AWS CLI

1. Copiez la `start-task-execution` commande suivante :

```
aws datasync start-task-execution \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh \
  --manifest-config {
      "Source": {
        "S3": {
            "ManifestObjectPath": "s3-object-key-of-manifest",
            "BucketAccessRoleArn": "bucket-iam-role",
            "S3BucketArn": "amzn-s3-demo-bucket-arn",
            "ManifestObjectVersionId": "manifest-version-to-use"
        }
      }
  }
```

2. Pour le `--task-arn` paramètre, spécifiez l'Amazon Resource Name (ARN) de la tâche que vous lancez.

3. Pour le `--manifest-config` paramètre, procédez comme suit :

   - `ManifestObjectPath`— Spécifiez la clé d'objet S3 de votre manifeste.
   - `BucketAccessRoleArn`— Spécifiez le rôle IAM qui permet d'accéder DataSync à votre manifeste dans son compartiment S3.

     Pour de plus amples informations, veuillez consulter Fournir DataSync l'accès à votre manifeste.

   - `S3BucketArn`— Spécifiez l'ARN du compartiment S3 qui héberge votre manifeste.
   - `ManifestObjectVersionId`— Spécifiez la version du manifeste que vous DataSync souhaitez utiliser.

     Par défaut, DataSync utilise la dernière version de l'objet.

4. Exécutez la `start-task-execution` commande pour commencer le transfert.

Limites

- Vous ne pouvez pas utiliser un manifeste avec des filtres.
- Vous ne pouvez pas spécifier uniquement un répertoire ou un dossier dans le but de transférer tout son contenu. Dans ces situations, pensez à utiliser un filtre d'inclusion au lieu d'un manifeste.
- Vous ne pouvez pas utiliser l'option de tâche Conserver les fichiers supprimés (`PreserveDeletedFiles`dans l'API) pour conserver des fichiers ou des objets dans la destination qui ne figurent pas dans la source. DataSync transfère uniquement ce qui est répertorié dans votre manifeste et ne supprime rien dans la destination.

Résolution des problèmes

Si vous transférez des objets dotés d'une version spécifique IDs depuis un compartiment S3, il se peut qu'une erreur liée à `HeadObject` ou s'affiche`GetObjectTagging`. Par exemple, voici une erreur liée à `GetObjectTagging` :

```
[WARN] Failed to read metadata for file /picture1.png (versionId: 111111): S3 Get
 Object Tagging Failed
[ERROR] S3 Exception: op=GetObjectTagging photos/picture1.png, code=403, type=15,
 exception=AccessDenied,
```

```
msg=Access Denied req-hdrs: content-type=application/xml, x-amz-api-version=2006-03-01
 rsp-hdrs: content-type=application/xml,
date=Wed, 07 Feb 2024 20:16:14 GMT, server=AmazonS3, transfer-encoding=chunked,
x-amz-id-2=IOWQ4fDEXAMPLEQM+ey7N9WgVhSnQ6JEXAMPLEZb7hSQDASK+Jd1vEXAMPLEa3Km, x-amz-
request-id=79104EXAMPLEB723
```

Si l'une de ces erreurs s'affiche, vérifiez que le rôle IAM DataSync utilisé pour accéder à votre emplacement source S3 dispose des autorisations suivantes :

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

Si vous devez mettre à jour votre rôle avec ces autorisations, consultezCréation d'un rôle IAM pour accéder DataSync à votre position Amazon S3.

Étapes suivantes

Si ce n'est pas déjà fait, commencez votre tâche. Sinon, surveillez l'activité de votre tâche.

Transfert de fichiers, d'objets et de dossiers spécifiques à l'aide de filtres

AWS DataSync vous permet d'appliquer des filtres pour inclure ou exclure des données de votre emplacement source lors d'un transfert. Par exemple, si vous ne souhaitez pas transférer des fichiers temporaires se terminant par `.tmp`, vous pouvez créer un filtre d'exclusion afin que ces fichiers ne soient pas acheminés vers votre emplacement de destination.

Vous pouvez utiliser une combinaison de filtres d'exclusion et d'inclusion dans la même tâche de transfert. Si vous modifiez les filtres d'une tâche, ces modifications seront appliquées lors de la prochaine exécution de la tâche.

Termes, définitions et syntaxe de filtrage

Familiarisez-vous avec les concepts liés au DataSync filtrage :

Filtre

La chaîne complète qui constitue un filtre particulier (par exemple, `*.tmp | *.temp` ou `/folderA|/folderB`).

Les filtres sont constitués de motifs délimités à l'aide d'un tube (|). Vous n'avez pas besoin de délimiteur lorsque vous ajoutez des modèles dans la DataSync console, car vous ajoutez chaque modèle séparément.

> **Note**
>
> Les filtres font la distinction majuscules/minuscules. Par exemple, le filtre `/folderA` ne correspondra pas`/FolderA`.

Modèle

Modèle interne à un filtre. Par exemple, `*.tmp` il s'agit d'un motif qui fait partie du `*.tmp | *.temp` filtre. Si votre filtre comporte plusieurs modèles, vous délimitez chaque motif à l'aide d'un tube (|).

Dossiers

- Tous les filtres se rapportent au chemin de l'emplacement source. Supposons, par exemple, que vous spécifiez `/my_source/` comme chemin source lorsque vous créez votre emplacement source et votre tâche et que vous spécifiez le filtre d'inclusion`/transfer_this/`. Dans ce cas, DataSync transfère uniquement le répertoire `/my_source/transfer_this/` et son contenu.
- Pour spécifier un dossier directement sous l'emplacement source, insérez une barre oblique (/) devant le nom du dossier. Dans l'exemple précédent, le modèle utilise `/transfer_this` et non pas `transfer_this`.
- DataSync interprète les modèles suivants de la même manière et fait correspondre à la fois le dossier et son contenu.

  ```
  /dir
  ```

  ```
  /dir/
  ```
- Lorsque vous transférez des données depuis ou vers un compartiment Amazon S3, DataSync traitez le `/` caractère de la clé d'objet comme l'équivalent d'un dossier dans un système de fichiers.

Caractères spéciaux

Les caractères spéciaux à utiliser avec le filtrage sont les suivants.

Caractère spécial	Description
* (caractère générique)	Caractère correspondant à zéro, un ou plusieurs caractères. Par exemple, `/movies_folder*` correspond à la fois à `/movies_folder` et à `/movies_folder1` .
| (barre verticale de séparation)	Caractère utilisé comme délimiteur entre des modèles. Il permet de spécifier plusieurs modèles, dont chacun peut correspondre au filtre. Par exemple, `*.tmp|*.temp` correspond aux fichiers se terminant par `tmp` ou par `temp`. **Note** Ce délimiteur n'est pas nécessaire lorsque vous ajoutez des modèles sur la console, car vous ajoutez chaque modèle sur une ligne distincte.
\ (barre oblique inverse)	Caractère utilisé pour échapper aux caractères spéciaux (*, |, \) du nom d'un fichier ou d'un objet. Une double barre oblique inverse (\\) est requise lorsqu'un e barre oblique inverse figure dans un nom de fichier. De la même façon, \\\\ représente deux barres obliques inverses consécutives dans un nom de fichier. Une barre oblique inverse suivie d'une barre verticale (\\\|) est requise lorsqu'une barre verticale figure dans un nom de fichier. Une barre oblique inverse (\) suivie de tout autre caractère, ou à la fin d'un modèle, est ignorée.

Exemples de filtres

Les exemples suivants montrent les filtres courants que vous pouvez utiliser DataSync.

> **Note**
>
> Le nombre de caractères que vous pouvez utiliser dans un filtre est limité. Pour de plus amples informations, veuillez consulter DataSync quotas.

Exclusion de certains dossiers de votre emplacement source

Dans certains cas, vous souhaiterez peut-être exclure des dossiers de votre emplacement source afin de ne pas les copier vers votre emplacement de destination. Par exemple, si vous avez work-in-progress des dossiers temporaires, vous pouvez utiliser le filtre suivant :

`*/.temp`

Pour exclure des dossiers présentant un contenu similaire (tel que `/reports2021` et `/reports2022`), vous pouvez utiliser un filtre d'exclusion tel que le suivant :

`/reports*`

Pour exclure des dossiers à n'importe quel niveau de la hiérarchie des fichiers, vous pouvez utiliser un filtre d'exclusion comme celui-ci.

`*/folder-to-exclude-1|*/folder-to-exclude-2`

Pour exclure des dossiers situés au niveau supérieur de l'emplacement source, vous pouvez utiliser un filtre d'exclusion tel que le suivant.

`/top-level-folder-to-exclude-1|/top-level-folder-to-exclude-2`

Inclure un sous-ensemble de dossiers sur votre emplacement source

Dans certains cas, votre emplacement source peut être une part importante et vous devez transférer un sous-ensemble des dossiers sous la racine. Pour inclure des dossiers spécifiques, démarrez une exécution de tâche avec un filtre d'inclusion similaire au suivant.

`/folder-to-transfer/*`

Exclusion de types de fichiers spécifiques

Pour exclure du transfert certains types de fichiers, vous pouvez créer une exécution de tâche avec un filtre d'exclusion tel que `*.temp`.

Transférez les fichiers individuels que vous spécifiez

Pour transférer une liste de fichiers individuels, lancez l'exécution d'une tâche avec un filtre d'inclusion tel que celui-ci : « `/folder/subfolder/file1.txt` | `/folder/subfolder/file2.txt` | `/folder/subfolder/file2.txt` »

Création de filtres d'inclusion

Les filtres d'inclusion définissent les fichiers, les objets et les dossiers que vous DataSync souhaitez transférer. Vous pouvez configurer des filtres d'inclusion lorsque vous créez, modifiez ou démarrez une tâche.

DataSync analyse et transfère uniquement les fichiers et dossiers qui correspondent aux filtres d'inclusion. Par exemple, pour inclure un sous-ensemble de vos dossiers sources, vous pouvez spécifier `/important_folder_1` |`/important_folder_2`.

> **Note**
>
> Les filtres d'inclusion prennent en charge le caractère générique (*) uniquement en tant que caractère le plus à droite d'un modèle. Par exemple, `/documents*` | `/code*` est pris en charge, mais ne l'`*.txt`est pas.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Tâches, puis sélectionnez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour plus d'informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Pour le contenu à scanner, sélectionnez Fichiers, objets et dossiers spécifiques, puis sélectionnez Utiliser des filtres.
5. Pour Includes, entrez votre filtre (par exemple, `/important_folders` pour inclure un répertoire important), puis choisissez Ajouter un modèle.
6. Ajoutez d'autres filtres d'inclusion si nécessaire.

À l'aide du AWS CLI

Lorsque vous utilisez le AWS CLI, vous devez utiliser des guillemets simples (`'`) autour du filtre et un | (tube) comme séparateur si vous avez plusieurs filtres.

L'exemple suivant indique deux filtres d'inclusion `/important_folder1` et `/important_folder2` lors de l'exécution de la `create-task` commande.

```
aws datasync create-task
   --source-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \
   --destination-location-arn 'arn:aws:datasync:region:account-id:location/location-id'
 \
   --includes FilterType=SIMPLE_PATTERN,Value='/important_folder1|/important_folder2'
```

Création de filtres d'exclusion

Les filtres d'exclusion définissent les fichiers, les objets et les dossiers de votre emplacement source que vous ne DataSync souhaitez pas transférer. Vous pouvez configurer ces filtres lorsque vous créez, modifiez ou démarrez une tâche.

Rubriques

- Données exclues par défaut

Données exclues par défaut

DataSync exclut automatiquement le transfert de certaines données :

- `.snapshot`— DataSync ignore tout chemin se terminant par `.snapshot`, qui est généralement utilisé pour les point-in-time instantanés des fichiers ou des répertoires d'un système de stockage.
- `/.aws-datasync`et `/.awssync` — DataSync crée ces dossiers dans votre région pour faciliter votre transfert.
- `/.zfs`— Vous pouvez voir ce dossier avec Amazon FSx pour les emplacements OpenZFS.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, choisissez Tâches, puis sélectionnez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour plus d'informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Pour Exclusions, entrez votre filtre (par exemple, `*/temp` pour exclure des dossiers temporaires), puis choisissez Ajouter un modèle.

5. Ajoutez d'autres filtres d'exclusion selon vos besoins.
6. Si nécessaire, ajoutez des filtres d'inclusion.

À l'aide du AWS CLI

Lorsque vous utilisez le AWS CLI, vous devez utiliser des guillemets simples (`'`) autour du filtre et un | (tube) comme séparateur si vous avez plusieurs filtres.

L'exemple suivant indique deux filtres d'exclusion `*/temp` et `*/tmp` lors de l'exécution de la `create-task` commande.

```
aws datasync create-task \
   --source-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \
   --destination-location-arn 'arn:aws:datasync:region:account-id:location/location-id'
 \
   --excludes FilterType=SIMPLE_PATTERN,Value='*/temp|*/tmp'
```

Comprendre le mode de DataSync gestion des métadonnées des fichiers et des objets

AWS DataSync peut conserver les métadonnées de votre fichier ou de votre objet lors d'un transfert de données. La manière dont vos métadonnées sont copiées dépend des lieux de transfert et de l'utilisation de types de métadonnées similaires par ces emplacements.

Métadonnées au niveau du système

En général, DataSync ne copie pas les métadonnées au niveau du système. Par exemple, lors du transfert depuis un serveur de fichiers SMB, les autorisations que vous avez configurées au niveau du système de fichiers ne sont pas copiées vers le système de stockage de destination.

Il y a des exceptions. Lors du transfert entre Amazon S3 et un autre stockage d'objets, copie DataSync certaines métadonnées d'objets définies par le système.

Métadonnées copiées dans les transferts Amazon S3

Les tableaux suivants décrivent les métadonnées qui DataSync peuvent être copiées lorsqu'un transfert implique un emplacement Amazon S3.

Rubriques

- Vers Amazon S3

- Entre Amazon S3 et d'autres types de stockage d'objets
- Entre Amazon S3 et HDFS

Vers Amazon S3

Lorsque vous copiez depuis l'un de ces emplacements	Vers cet endroit	DataSync peut copier
• NFS • Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP (en utilisant NFS)	• Amazon S3	Ce qui suit en tant que métadonnées utilisateur Amazon S3 : • Horodatages de modification de fichiers et de dossiers • Horodatages d'accès aux fichiers et aux dossiers (DataSync vous ne pouvez le faire que dans la mesure du possible) • ID utilisateur et ID de groupe • Autorisations POSIX Les métadonnées des fichiers stockées dans les métadonnées utilisateur d'Amazon S3 sont interopérables avec les partages NFS sur les passerelles de fichiers utilisant . AWS Storage Gateway Une passerelle de fichiers permet un accès à faible latence depuis les réseaux locaux aux données copiées sur Amazon S3 par. DataSync

Lorsque vous copiez depuis l'un de ces emplacements	Vers cet endroit	DataSync peut copier
		Ces métadonnées sont également interopérables avec FSx for Lustre. Lorsque DataSync des objets contenant ces métadonnées sont copiés vers un serveur NFS, les métadonnées du fichier sont restaurées. La restauration des métadonné es nécessite l'octroi d'autoris ations élevées au serveur NFS. Pour de plus amples informations, veuillez consulter Configuration des AWS DataSync transferts avec un serveur de fichiers NFS.

Entre Amazon S3 et d'autres types de stockage d'objets

Lors de la copie entre ces emplacements	DataSync peut copier

• Stockage d'objets
• Amazon S3
	• Métadonnées d'objet définies par l'utilisateur
	• Balises d'objet
	• Les métadonnées d'objet définies par le système suivantes :
	  • Content-Disposition
	  • Encodage-Contenu
	  • Content-Language
	  • Content-Type
	
	Remarque : DataSync copie les métadonné es au niveau du système pour tous les objets

• Microsoft Azure Blob Storage • Amazon S3	

Lors de la copie entre ces emplacements	DataSync peut copier
	lors d'un transfert initial. Si vous configurez votre tâche pour transférer uniquement les données modifiées, vous ne DataSync copierez pas les métadonnées du système lors des transferts suivants, sauf si le contenu d'un objet ou les métadonnées utilisateur ont également été modifiés. DataSync ne copie pas les autres métadonnées des objets, telles que les listes de contrôle d'accès aux objets (ACLs), les versions antérieures des objets ou la clé Last-Modified.

Entre Amazon S3 et HDFS

Lors de la copie entre ces emplacements	DataSync peut copier
• Système de fichiers distribué Hadoop (HDFS) • Amazon S3	Ce qui suit en tant que métadonnées utilisateur Amazon S3 : • Horodatages de modification de fichiers et de dossiers • Horodatages d'accès aux fichiers et aux dossiers (DataSync vous ne pouvez le faire que dans la mesure du possible) • ID utilisateur et ID de groupe • Autorisations POSIX HDFS utilise des chaînes pour stocker la propriété des utilisateurs et des groupes de fichiers et de dossiers, plutôt que des identifiants numériques tels que et. UIDs GIDs

Métadonnées copiées lors de transferts NFS

Le tableau suivant décrit les métadonnées qui DataSync peuvent être copiées entre des emplacements utilisant le système de fichiers réseau (NFS).

Lors de la copie entre ces emplacements	DataSync peut copier
• NFS • Amazon EFS • Amazon FSx pour Lustre • Amazon FSx pour OpenZFS • Amazon FSx pour NetApp ONTAP (à l'aide de NFS)	• Horodatages de modification de fichiers et de dossiers • Horodatages d'accès aux fichiers et aux dossiers (DataSync vous ne pouvez le faire que dans la mesure du possible) • ID utilisateur (UID) et ID de groupe (GID) • Autorisations POSIX

Métadonnées copiées dans les transferts SMB

Le tableau suivant décrit les métadonnées qui DataSync peuvent être copiées entre des emplacements utilisant le module SMB (Server Message Block).

Lors de la copie entre ces emplacements	DataSync peut copier
• SMB • Serveur FSx de fichiers Amazon pour Windows • FSx pour ONTAP (via SMB)	• Horodatages des fichiers : heure d'accès, heure de modification et heure de création • Identifiant de sécurité (SID) du propriétaire du fichier • Attributs de fichier standard : lecture seule (R), archive (A), système (S), masqué (H), compressé (C), contenu non indexé (I), crypté (E), temporaire (T), hors ligne (O) et fragmenté (P) DataSync tente de copier au mieux les attributs archive (A), compressé (C), non indexé en contexte (I), clairsemé (P) et temporaire (T). Si ces attributs ne sont pas

Lors de la copie entre ces emplacements	DataSync peut copier
	appliqués à la destination, ils sont ignorés lors de la vérification des tâches. • Listes d'accès discrétionnaires NTFS (DACLs), qui déterminent s'il faut accorder l'accès à un objet. • Listes de contrôle d'accès au système NTFS (SACLs), utilisées par les administrateurs pour consigner les tentatives d'accès à un objet sécurisé. Remarque : ne SACLs sont pas copiés si vous utilisez la version 1.0 de SMB. Copier DACLs et SACLs nécessite l'octroi d'autorisations spécifiques à l'utilisateur Windows DataSync qui accède à votre position via SMB. Pour plus d'informa tions, consultez la section Création d'un emplacement pour SMB, FSx pour Windows File Server ou FSx pour ONTAP (selon le type d'emplacement de votre transfert).

Métadonnées copiées dans d'autres scénarios de transfert

DataSync gère les métadonnées de la manière suivante lors de la copie entre ces systèmes de stockage (dont la plupart ont des structures de métadonnées différentes).

Lorsque vous copiez depuis l'un de ces emplacements	Vers l'un de ces sites	DataSync peut copier
• SMB • FSx pour le serveur de fichiers Windows • FSx pour ONTAP (via SMB)	• Amazon EFS • FSx pour Lustre • FSx pour OpenZFS	Métadonnées POSIX par défaut pour tous les fichiers et dossiers du système de fichiers de destination ou pour les objets du compartim

Lorsque vous copiez depuis l'un de ces emplacements	Vers l'un de ces sites	DataSync peut copier
	• FSx pour ONTAP (en utilisant NFS) • Amazon S3 • Stockage d'objets • Azure Blob Storage • NFS	ent S3 de destination. Cette approche inclut l'utilisation des valeurs d'ID utilisateur et d'ID de groupe POSIX par défaut. Les métadonnées basées sur Windows (telles que ACLs) ne sont pas conservées.
• Stockage d'objets • Amazon S3 • Azure Blob Storage	• Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP (en utilisant NFS)	Métadonnées POSIX par défaut sur les fichiers et dossiers de destination. Cette approche inclut l'utilisation des valeurs d'ID utilisateur et d'ID de groupe POSIX par défaut.
• Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP (en utilisant NFS)	• Azure Blob Storage	Les métadonnées suivantes sont définies par l'utilisateur : • Horodatages de modification de fichiers et de dossiers • Horodatages d'accès aux fichiers et aux dossiers (DataSync vous ne pouvez le faire que dans la mesure du possible) • ID utilisateur et ID de groupe • Autorisations POSIX

Lorsque vous copiez depuis l'un de ces emplacements	Vers l'un de ces sites	DataSync peut copier
• HDFS	• Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP (en utilisant NFS)	• Horodatages de modification de fichiers et de dossiers • Horodatages d'accès aux fichiers et aux dossiers (DataSync vous ne pouvez le faire que dans la mesure du possible) • Autorisations POSIX HDFS enregistre la propriété des utilisateurs et des groupes de fichiers et de dossiers sous forme de chaînes plutôt que d'identifiants numériques (tels que UIDs et). GIDs Les valeurs par défaut pour UIDs et GIDs sont appliquées au système de fichiers de destination. Pour de plus amples informations, veuillez consulter Comprendre quand et comment DataSync applique les métadonnées POSIX par défaut.

Lorsque vous copiez depuis l'un de ces emplacements	Vers l'un de ces sites	DataSync peut copier
• Amazon S3 • Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour le serveur de fichiers Windows • FSx pour ONTAP	• HDFS	Horodatage des fichiers et des dossiers à partir de l'emplace ment source. Le propriétaire du fichier ou du dossier est défini en fonction de l'utilisa teur HDFS ou du principal Kerberos que vous avez spécifié lors de la création de l'emplacement de transfert HDFS. La configuration du mappage des groupes sur le cluster Hadoop détermine le groupe.
• Amazon S3 • Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP (en utilisant NFS) • Stockage d'objets • NFS • HDFS	• SMB • FSx pour le serveur de fichiers Windows • FSx pour ONTAP (via SMB)	Horodatage des fichiers et des dossiers à partir de l'emplace ment source. La propriété est définie en fonction de l'utilisateur Windows qui a été spécifié DataSync pour accéder au partage Amazon FSx ou SMB. Les autorisat ions sont héritées du répertoir e parent.
• Azure Blob Storage	• FSx pour le serveur de fichiers Windows • FSx pour ONTAP (via SMB)	

Comprendre quand et comment DataSync applique les métadonnées POSIX par défaut

DataSync applique les métadonnées POSIX par défaut dans les situations suivantes :

- Lorsque les emplacements source et de destination de votre transfert n'ont pas de structures de métadonnées similaires
- Lorsque les métadonnées sont absentes de l'emplacement source

Le tableau suivant décrit comment DataSync appliquer les métadonnées POSIX par défaut lors de ces types de transferts :

Source	Destination	Autorisations de fichiers	Autorisations relatives aux dossiers	UID	GID
• Amazon S3 [1] • Stockage d'objets [1] • Stockage Microsoft Azure Blob [1]	• Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP (en utilisant NFS) • NFS	0755	0755	65534	65534
• SMB	• Amazon S3 • Stockage d'objets • Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP (en utilisant NFS)	0644	0755	65534	65534

Source	Destination	Autorisations de fichiers	Autorisations relatives aux dossiers	UID	GID
	• NFS				
• HDFS	• Amazon EFS • FSx pour Lustre • FSx pour OpenZFS • FSx pour ONTAP (en utilisant NFS) • NFS	0644	0755	65534	65534

[1] Dans les cas où les objets ne possèdent pas de métadonnées précédemment appliquées par DataSync.

Liens et répertoires copiés par AWS DataSync

AWS DataSync gère les liens physiques, les liens symboliques et les répertoires différemment selon les emplacements de stockage concernés par votre transfert.

Liens physiques

Voici comment DataSync gérer les liens physiques dans certains scénarios de transfert courants :

- Lors du transfert entre un serveur de fichiers NFS, FSx pour Lustre, pour OpenZFS, FSx FSx pour ONTAP (à l'aide de NFS) et Amazon EFS, les liens physiques sont préservés.
- Lors du transfert vers Amazon S3, chaque fichier sous-jacent référencé par un lien physique n'est transféré qu'une seule fois. Lors des transferts incrémentiels, des objets distincts sont créés dans votre compartiment S3. Si un lien dur est inchangé dans Amazon S3, il est correctement restauré lorsqu'il est transféré vers un serveur de fichiers NFS, FSx pour Lustre, pour OpenZFS, FSx pour ONTAP (à l'aide de NFS) ou FSx pour le système de fichiers Amazon EFS.

- Lors du transfert vers Microsoft Azure Blob Storage, chaque fichier sous-jacent référencé par un lien physique n'est transféré qu'une seule fois. Lors des transferts incrémentiels, des objets distincts sont créés dans votre stockage de blob si la source contient de nouvelles références. Lors du transfert depuisAzure Blob Storage, DataSync transfère les liens physiques comme s'il s'agissait de fichiers individuels.
- Lors du transfert entre un serveur de fichiers SMB, FSx pour Windows File Server et FSx pour ONTAP (via SMB), les liens physiques ne sont pas pris en charge. Si DataSync vous rencontrez des liens durs dans ces situations, la tâche de transfert se termine avec une erreur. Pour en savoir plus, consultez vos CloudWatch journaux.
- Lors du transfert vers HDFS, les liens physiques ne sont pas pris en charge. CloudWatch les journaux indiquent que ces liens ont été ignorés.

Liens symboliques

Voici comment DataSync gérer les liens symboliques dans certains scénarios de transfert courants :

- Lors du transfert entre un serveur de fichiers NFS, FSx pour Lustre, pour OpenZFS, FSx FSx pour ONTAP (à l'aide de NFS) et Amazon EFS, les liens symboliques sont préservés.
- Lors du transfert vers Amazon S3, le chemin cible du lien est stocké dans l'objet Amazon S3. Le lien est correctement restauré lorsqu'il est transféré vers un serveur de fichiers NFS, FSx pour Lustre, pour OpenZFS, FSx pour ONTAP ou FSx pour le système de fichiers Amazon EFS.
- Lors du transfert versAzure Blob Storage, les liens symboliques ne sont pas pris en charge. CloudWatch les journaux indiquent que ces liens ont été ignorés.
- Lors du transfert entre un serveur de fichiers SMB, FSx pour Windows File Server et FSx pour ONTAP (via SMB), les liens symboliques ne sont pas pris en charge. DataSync ne transfère pas un lien symbolique lui-même mais un fichier référencé par le lien symbolique. Pour reconnaître les fichiers dupliqués et les dédupliquer à l'aide de liens symboliques, vous devez configurer la déduplication sur votre système de fichiers de destination.
- Lors du transfert vers HDFS, les liens symboliques ne sont pas pris en charge. CloudWatch les journaux indiquent que ces liens ont été ignorés.

Annuaires

En général, DataSync préserve les répertoires lors du transfert entre systèmes de stockage. Ce n'est pas le cas dans les situations suivantes :

- Lors du transfert vers Amazon S3, les répertoires sont représentés sous forme d'objets vides dotés de préfixes et se terminant par une barre oblique ()/.
- Lors du transfert vers un espace de noms Azure Blob Storage sans espace de noms hiérarchique, les répertoires n'existent pas. Ce qui ressemble à un répertoire n'est qu'une partie du nom d'un objet.

Configuration du mode de gestion des fichiers, des objets et des métadonnées

Vous pouvez configurer le mode de AWS DataSync gestion de vos fichiers, objets et de leurs métadonnées associées lors du transfert d'un emplacement à un autre.

Par exemple, dans le cas de transferts récurrents, vous souhaiterez peut-être remplacer les fichiers de votre destination par des modifications apportées à la source afin de synchroniser les emplacements. Vous pouvez copier des propriétés telles que les autorisations POSIX pour les fichiers et les dossiers, les balises associées aux objets et les listes de contrôle d'accès (ACLs).

Options du mode de transfert

Vous pouvez configurer si vous DataSync transférez uniquement les données (y compris les métadonnées) modifiées après une copie initiale ou toutes les données à chaque fois que vous exécutez la tâche. Si vous prévoyez des transferts récurrents, vous souhaiterez peut-être uniquement transférer les modifications apportées depuis l'exécution de votre tâche précédente.

Option dans la console	Option dans l'API	Description
Transférez uniquement les données modifiées	TransferModeréglé sur `CHANGED`	Après votre transfert complet initial, DataSync copie uniquement les données et les métadonnées qui diffèrent entre l'emplacement source et l'emplacement de destination.
Transférez toutes les données	TransferModeréglé sur `ALL`	DataSync copie tout le contenu de la source vers la destination sans comparer les différences entre les emplacements.

Options de gestion des fichiers et des objets

Vous pouvez contrôler certains aspects du DataSync traitement de vos fichiers ou objets dans l'emplacement de destination. Par exemple, DataSync vous pouvez supprimer des fichiers dans la destination qui ne figurent pas dans la source.

Option dans la console	Option dans l'API	Description
Conserver les fichiers supprimés	PreserveDeletedFiles	Spécifie si DataSync des fichiers ou des objets qui n'existent pas dans la source sont conservés dans l'emplacement de destination. Si vous configurez votre tâche pour supprimer des objets de votre compartiment Amazon S3, des frais de durée de stockage minimale peuvent vous être facturés pour certaines classes de stockage. Pour plus d'informations, consultez Considérations relatives à la classe de stockage lors des transferts Amazon S3. Warning Vous ne pouvez pas configurer votre tâche de manière à supprimer des données dans la destination et à transférer toutes les données. Lorsque vous transférez

Option dans la console	Option dans l'API	Description
		toutes les données, DataSync il ne scanne pas votre position de destination et ne sait pas quoi supprimer.
Remplacer des fichiers	OverwriteMode	Spécifie si DataSync les données sont modifiées dans l'emplacement de destination lorsque les données source ou les métadonnées ont changé. Si vous ne configurez pas votre tâche pour remplacer les données, les données de destination ne sont pas remplacées, même si les données source sont différent es. Si votre tâche remplace des objets, des frais supplémen taires peuvent vous être facturés pour certaines classes de stockage (par exemple, pour la récupération ou la suppression anticipée). Pour plus d'informations, consultez Considérations relatives à la classe de stockage lors des transferts Amazon S3.

Options de gestion des métadonnées

DataSync peut conserver les métadonnées des fichiers et des objets lors d'un transfert. Les métadonnées DataSync pouvant être conservées dépendent des systèmes de stockage concernés et de l'utilisation par ces systèmes d'une structure de métadonnées similaire.

Avant de configurer votre tâche, assurez-vous de comprendre comment DataSync gère les métadonnées et les fichiers spéciaux lors du transfert entre votre emplacement source et votre emplacement de destination.

> **Important**
>
> DataSync prend en charge les transferts vers et depuis certains systèmes de stockage cloud tiers, tels que Google Cloud Storage et IBM Cloud Object Storage, qui gèrent les métadonnées du système d'une manière qui n'est pas totalement compatible avec S3. Pour ces transferts, DataSync essaie de copier des attributs de métadonnées tels que `ContentTypeContentEncoding`,`ContentLanguage`, et dans `CacheControl` la mesure du possible. Si le système de stockage de destination n'applique pas ces attributs, ils seront ignorés lors de la vérification des tâches.

Option dans la console	Option dans l'API	Description
Propriété de copie	Gid et Uid	Spécifie si les DataSync copies sont propriétaires des fichiers et dossiers POSIX, par exemple l'ID de groupe des propriétaires du fichier et l'ID utilisateur du propriétaire du fichier.
Autorisations de copie	PosixPermissions	Spécifie si les autorisations POSIX pour les fichiers et les dossiers sont DataSync copiées de la source vers la destination.

Option dans la console	Option dans l'API	Description
Copier les horodatages	Atime et Mtime	Spécifie si les métadonnées d'horodatage sont DataSync copiées de la source vers la destination. Obligatoire lorsque vous devez exécuter une tâche plusieurs fois.
Copier les balises d'objets	ObjectTags	Spécifie si les balises associées à vos objets sont DataSync préservées lors du transfert entre systèmes de stockage d'objets.

Option dans la console	Option dans l'API	Description
Propriété de copie DACLs, et SACLs	SecurityDescriptorCopyFlags réglé sur `OWNER_DACL_SACL`	DataSync copie ce qui suit : • Le propriétaire de l'objet. • Listes d'accès discrétionnaires NTFS (DACLs), qui déterminent s'il faut accorder l'accès à un objet. • Listes de contrôle d'accès au système NTFS (SACLs), utilisées par les administrateurs pour consigner les tentatives d'accès à un objet sécurisé. Remarque : ne SACLs sont pas copiés si vous utilisez la version 1.0 de SMB. Copier DACLs et SACLs nécessite l'octroi d'autorisations spécifiques à l'utilisateur Windows DataSync qui accède à votre position via SMB. Pour plus d'informations, consultez la section Création d'un emplacement pour SMB, FSx pour Windows File Server ou FSx pour ONTAP (selon le type d'emplacement de votre transfert).

Option dans la console	Option dans l'API	Description
Propriété de copie et DACLs	SecurityDescriptorCopyFlags réglé sur `OWNER_DACL`	DataSync copie ce qui suit : • Le propriétaire de l'objet. • DACLs, qui déterminent s'il convient d'accorder l'accès à un objet. DataSync ne sera pas SACLs copié lorsque vous choisissez cette option.
Ne copiez pas la propriété ou ACLs	SecurityDescriptorCopyFlags réglé sur `NONE`	DataSync ne copie aucune donnée de propriété ou d'autorisation. Les objets qui DataSync écrivent sur votre emplacement de destinati on appartiennent à l'utilisa teur dont les informations d'identification sont fournies pour accéder DataSync à la destination. Les autorisations des objets de destination sont déterminées en fonction des autorisations configurées sur le serveur de destination.

Configuration des options de gestion des fichiers, des objets et des métadonnées

Vous pouvez configurer le mode de DataSync gestion des fichiers, des objets et des métadonnées lors de la création, de la modification ou du démarrage de votre tâche de transfert.

Utilisation de la console DataSync

Les instructions suivantes décrivent comment configurer les options de gestion des fichiers, des objets et des métadonnées lors de la création d'une tâche.

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Pour le mode de transfert, choisissez l'une des options suivantes :

   - Transférez uniquement les données modifiées
   - Transférez toutes les données

   Pour plus d'informations sur ces options, consultez Options du mode de transfert.
5. Sélectionnez Conserver les fichiers supprimés si vous DataSync souhaitez conserver des fichiers ou des objets dans l'emplacement de destination qui n'existent pas dans la source.

   Si vous ne choisissez pas cette option et que votre tâche supprime des objets de votre compartiment Amazon S3, des frais de durée de stockage minimale peuvent vous être facturés pour certaines classes de stockage. Pour plus d'informations, consultez Considérations relatives à la classe de stockage lors des transferts Amazon S3.

   > **Warning**
   >
   > Vous ne pouvez pas désélectionner cette option et activer Transférer toutes les données. Lorsque vous transférez toutes les données, DataSync il ne scanne pas votre position de destination et ne sait pas quoi supprimer.
6. Sélectionnez Remplacer les fichiers si vous DataSync souhaitez modifier les données dans l'emplacement de destination lorsque les données source ou les métadonnées ont changé.

   Si votre tâche remplace des objets, des frais supplémentaires peuvent vous être facturés pour certaines classes de stockage (par exemple, pour la récupération ou la suppression anticipée). Pour plus d'informations, consultez Considérations relatives à la classe de stockage lors des transferts Amazon S3.

   Si vous ne sélectionnez pas cette option, les données de destination ne sont pas remplacées même si les données source sont différentes.

7. Sous Options de transfert, sélectionnez la manière dont vous DataSync souhaitez gérer les métadonnées. Pour plus d'informations sur ces options, consultez Options de gestion des métadonnées.

> **Important**
>
> Les options affichées dans la console dépendent de l'emplacement source et de destination de votre tâche. Vous devrez peut-être développer les paramètres supplémentaires pour voir certaines de ces options.

- Propriété de copie
- Autorisations de copie
- Copier les horodatages
- Copier les balises d'objets
- Propriété de copie DACLs, et SACLs
- Propriété de copie et DACLs
- Ne copiez pas la propriété ou ACLs

Utilisation de l' DataSync API

Vous pouvez configurer les options de gestion des fichiers, des objets et des métadonnées en utilisant le `Options` paramètre avec l'une des opérations suivantes :

- CreateTask
- StartTaskExecution
- UpdateTask

Configuration du mode de AWS DataSync vérification de l'intégrité des données

Lors d'un transfert, AWS DataSync utilise la vérification par somme de contrôle pour vérifier l'intégrité des données que vous copiez entre les sites. Vous pouvez également configurer DataSync pour effectuer une vérification supplémentaire à la fin de votre transfert.

Options de vérification des données

Utilisez les informations suivantes pour vous aider à décider si et comment vous DataSync souhaitez effectuer ces vérifications supplémentaires.

Option console	Option d'API	Description
Vérifier uniquement les données transférées (recommandé)	VerifyModeréglé sur `ONLY_FILES_TRANSFERRED`	DataSync calcule la somme de contrôle des données transférées (y compris les métadonnées) à l'emplacement source. À la fin de votre transfert, DataSync comparez cette somme de contrôle à la somme de contrôle calculée sur ces mêmes données à destination. Nous recommandons cette option lors du transfert vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour de plus amples informations, veuillez consulter Considérations relatives à la classe de stockage lors des transferts Amazon S3.
Vérifiez toutes les données	VerifyModeréglé sur `POINT_IN_TIME_CONSISTENT`	À la fin de votre transfert, DataSync vérifie l'intégralité de la source et de la destination pour vérifier que les deux emplacements sont parfaitement synchronisés.

Option console	Option d'API	Description
		Note Non pris en charge lorsque votre tâche utilise le mode amélioré. Si vous utilisez un manifeste, il analyse et vérifie DataSync uniquement ce qui est répertorié dans le manifeste. Vous ne pouvez pas utiliser cette option lors du transfert vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour de plus amples informati ons, veuillez consulter Considérations relatives à la classe de stockage lors des transferts Amazon S3.
Ne pas vérifier les données après le transfert	VerifyModeréglé sur `NONE`	DataSync effectue des contrôles d'intégrité des données uniquement pendant votre transfert. Contrairement aux autres options, il n'y a aucune vérification supplémen taire à la fin de votre transfert.

Configuration de la vérification des données

Vous pouvez configurer les options de vérification des données lors de la création d'une tâche, de sa mise à jour ou du lancement de son exécution.

Utilisation de la console DataSync

Les instructions suivantes décrivent comment configurer les options de vérification des données lors de la création d'une tâche.

Pour configurer la vérification des données à l'aide de la console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Pour la vérification, choisissez l'une des options suivantes :

   - Vérifier uniquement les données transférées (recommandé)
   - Vérifiez toutes les données
   - Ne pas vérifier les données après le transfert

Utilisation de l'API DataSync

Vous pouvez configurer le mode de DataSync vérification des données en utilisant le `VerifyMode` paramètre avec l'une des opérations suivantes :

- CreateTask
- UpdateTask
- StartTaskExecution

Définition des limites de bande passante pour votre AWS DataSync tâche

Vous pouvez configurer les limites de bande passante réseau pour votre AWS DataSync tâche et chacune de ses exécutions.

> **Note**
>
> Non applicable aux tâches en mode amélioré.

Limiter la bande passante pour une tâche

Définissez une limite de bande passante lors de la création, de la modification ou du démarrage d'une tâche.

Utilisation de la console DataSync

Les instructions suivantes décrivent comment configurer une limite de bande passante pour votre tâche lorsque vous la créez.

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Pour Limite de bande passante, choisissez l'une des options suivantes :

   - Sélectionnez Utiliser disponible pour utiliser toute la bande passante réseau disponible pour chaque exécution de tâche.
   - Sélectionnez Définir la limite de bande passante (Mbits/s) et entrez la bande passante maximale que vous souhaitez utiliser DataSync pour chaque exécution de tâche.

Utilisation de l' DataSync API

Vous pouvez configurer la limite de bande passante d'une tâche en utilisant le `BytesPerSecond` paramètre avec l'une des opérations suivantes :

- CreateTask
- UpdateTask
- StartTaskExecution

Limitation de la bande passante pour l'exécution d'une tâche

Vous pouvez modifier la limite de bande passante pour l'exécution d'une tâche en cours ou en file d'attente.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation, développez Transfert de données, puis choisissez Tâches.
3. Choisissez la tâche, puis sélectionnez Historique pour afficher les exécutions de la tâche.
4. Choisissez l'exécution de la tâche que vous souhaitez modifier, puis sélectionnez Modifier.
5. Dans la boîte de dialogue, sélectionnez l'une des options suivantes :
   - Sélectionnez Utiliser disponible pour utiliser toute la bande passante réseau disponible pour l'exécution de la tâche.
   - Sélectionnez Définir la limite de bande passante (Mbits/s) et entrez la bande passante maximale que vous souhaitez utiliser DataSync pour l'exécution de la tâche.
6. Sélectionnez Enregistrer les modifications.

   La nouvelle limite de bande passante prend effet dans les 60 secondes.

Utilisation de l'API DataSync

Vous pouvez modifier la limite de bande passante pour l'exécution d'une tâche en cours ou en file d'attente en utilisant le `BytesPerSecond` paramètre avec l'UpdateTaskExecutionopération.

Planification de l'exécution de votre AWS DataSync tâche

Vous pouvez configurer un calendrier des AWS DataSync tâches pour transférer régulièrement des données entre les emplacements de stockage.

Comment fonctionne DataSync la planification des tâches

Une DataSync tâche planifiée s'exécute à la fréquence que vous spécifiez, avec un intervalle minimum d'une heure. Vous pouvez créer un planning de tâches à l'aide d'un cron ou d'expressions de taux.

> **Important**
>
> Vous ne pouvez pas planifier l'exécution d'une tâche à un intervalle inférieur à 1 heure.

Utilisation d'expressions cron

Utilisez des expressions cron pour les plannings de tâches exécutés à une heure et à un jour spécifiques. Par exemple, voici comment configurer un calendrier de tâches dans le AWS CLI qui s'exécute à 12 h 00 UTC tous les dimanches et mercredis.

```
cron(0 12 ? * SUN,WED *)
```

Utilisation d'expressions de taux

Utilisez des expressions de taux pour les planifications de tâches exécutées à intervalles réguliers, par exemple toutes les 12 heures. Par exemple, voici comment configurer un calendrier de tâches AWS CLI qui s'exécute toutes les 12 heures :

```
rate(12 hours)
```

> **Tip**
>
> Pour plus d'informations sur la syntaxe des expressions cron et rate, consultez le guide de l' EventBridge utilisateur Amazon.

Création d'un calendrier de DataSync tâches

Vous pouvez planifier la fréquence d'exécution de votre tâche à l'aide de la DataSync console ou de DataSync l'API. AWS CLI

Utilisation de la DataSync console

Les instructions suivantes décrivent comment configurer un planning lors de la création d'une tâche. Vous pouvez modifier le planning ultérieurement lors de la modification de la tâche.

Dans la console, certaines options de planification vous permettent de spécifier l'heure exacte d'exécution de votre tâche (par exemple, tous les jours à 22 h 30). Si vous n'indiquez pas d'heure pour ces options, votre tâche s'exécute au moment où vous la créez (ou mettez à jour) la tâche.

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour plus d'informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Pour planifier la fréquence, effectuez l'une des opérations suivantes :
   - Choisissez Non planifié si vous ne souhaitez pas que votre tâche soit exécutée selon un calendrier.
   - Choisissez Horaire, puis choisissez la minute pendant l'heure pendant laquelle vous souhaitez que votre tâche soit exécutée.
   - Choisissez Quotidien et entrez l'heure UTC à laquelle vous souhaitez que votre tâche soit exécutée.
   - Choisissez Hebdomadaire et le jour de la semaine, puis entrez l'heure UTC à laquelle vous souhaitez que la tâche s'exécute.
   - Choisissez Jours de la semaine, choisissez un ou plusieurs jours spécifiques et entrez l'heure UTC à laquelle la tâche doit être exécutée au format HH:MM.
   - Choisissez Personnalisé, puis sélectionnez Expression Cron ou Expression Rate. Entrez votre calendrier de tâches avec un intervalle minimum d'une heure.

À l'aide du AWS CLI

Vous pouvez créer un calendrier pour votre DataSync tâche en utilisant le `--schedule` paramètre avec la `start-task-execution` commande `create-taskupdate-task`, ou.

Les instructions suivantes décrivent comment procéder à l'aide de la `create-task` commande.

1. Copiez la `create-task` commande suivante :

```
aws datasync create-task \
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh \
```

```
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-abcdefgh12345678 \
  --schedule '{
    "ScheduleExpression": "cron(0 12 ? * SUN,WED *)"
  }'
```

2. Pour le `--source-location-arn` paramètre, spécifiez l'Amazon Resource Name (ARN) de l'emplacement à partir duquel vous transférez les données.
3. Pour le `--destination-location-arn` paramètre, spécifiez l'ARN de l'emplacement vers lequel vous transférez les données.
4. Pour le `--schedule` paramètre, spécifiez une expression cron ou rate pour votre planning.

   Dans l'exemple, l'expression cron *`cron(0 12 ? * SUN,WED *)`* définit un calendrier de tâches qui s'exécute à 12 h 00 UTC tous les dimanches et mercredis.
5. Exécutez la `create-task` commande pour créer votre tâche avec le planning.

Suspension d'un calendrier de DataSync tâches

Il peut arriver que vous deviez suspendre votre planification des DataSync tâches. Par exemple, il se peut que vous deviez désactiver temporairement un transfert récurrent pour résoudre un problème lié à votre tâche ou effectuer des opérations de maintenance sur votre système de stockage.

DataSync peut désactiver automatiquement votre planification des tâches pour les raisons suivantes :

- Votre tâche échoue à plusieurs reprises avec la même erreur.
- Vous désactivez un Région AWS utilisateur utilisé par votre tâche.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches.
3. Choisissez la tâche pour laquelle vous souhaitez suspendre le planning, puis choisissez Modifier.
4. Pour Planifier, désactivez Activer le calendrier. Sélectionnez Enregistrer les modifications.

À l'aide du AWS CLI

1. Copiez la `update-task` commande suivante :

```
aws datasync update-task \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh \
  --schedule '{
    "ScheduleExpression": "cron(0 12 ? * SUN,WED *)",
    "Status": "DISABLED"
  }'
```

2. Pour le `--task-arn` paramètre, spécifiez l'ARN de la tâche pour laquelle vous souhaitez suspendre le planning.
3. Pour le `--schedule` paramètre, procédez comme suit :
   - Pour`ScheduleExpression`, spécifiez un cron ou une expression de taux pour votre calendrier.

     Dans l'exemple, l'expression *`cron(0 12 ? * SUN,WED *)`* définit un calendrier de tâches qui s'exécute à 12 h 00 UTC tous les dimanches et mercredis.
   - Pour`Status`, spécifiez `DISABLED` de suspendre le calendrier des tâches.
4. Exécutez la commande `update-task`.
5. Pour reprendre le planning, exécutez la même `update-task` commande avec `Status` set to`ENABLED`.

Vérifier l'état d'un planning de DataSync tâches

Vous pouvez voir si votre calendrier de DataSync tâches est activé.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches.
3. Dans la colonne Planification, vérifiez si le calendrier de la tâche est activé ou désactivé.

À l'aide du AWS CLI

1. Copiez la `describe-task` commande suivante :

```
aws datasync describe-task \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

2. Pour le `--task-arn` paramètre, spécifiez l'ARN de la tâche sur laquelle vous souhaitez obtenir des informations.
3. Exécutez la commande `describe-task`.

Vous obtenez une réponse qui fournit des détails sur votre tâche, y compris son calendrier. (L'exemple suivant se concentre principalement sur la configuration du planning des tâches et ne montre pas de `describe-task` réponse complète.)

L'exemple montre que le planning de la tâche est désactivé manuellement. Si la planification est désactivée par le DataSync `SERVICE`, un message d'erreur s'affiche pour vous aider `DisabledReason` à comprendre pourquoi la tâche continue d'échouer. Pour de plus amples informations, veuillez consulter ???.

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh",
    "Status": "AVAILABLE",
    "Schedule": {
        "ScheduleExpression": "cron(0 12 ? * SUN,WED *)",
        "Status": "DISABLED",
        "StatusUpdateTime": 1697736000,
        "DisabledBy": "USER",
        "DisabledReason": "Manually disabled by user."
    },
    ...
}
```

Marquer vos tâches AWS DataSync

Les balises sont des paires clé-valeur qui vous permettent de gérer, de filtrer et de rechercher vos AWS DataSync ressources. Vous pouvez ajouter jusqu'à 50 balises à chaque DataSync tâche et à son exécution.

Par exemple, vous pouvez créer une tâche pour une migration de données volumineuse et lui attribuer la clé **`Project`** et la valeur**`Large Migration`**. Pour mieux organiser la migration, vous pouvez étiqueter une exécution de la tâche avec la clé **`Transfer Date`** et la valeur **`May 2021`** (les exécutions de tâches suivantes peuvent être balisées **`June 2021`**`July 2021`, etc.).

Marquer votre tâche DataSync

Vous ne pouvez étiqueter votre DataSync tâche que lors de sa création.

Utilisation de la console DataSync

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Sur la page Configurer les paramètres, choisissez Ajouter une nouvelle balise pour étiqueter votre tâche.

À l'aide du AWS CLI

1. Copiez la `create-task` commande suivante :

```
aws datasync create-task \
    --source-location-arn 'arn:aws:datasync:region:account-id:location/source-location-id' \
    --destination-location-arn 'arn:aws:datasync:region:account-id:location/destination-location-id' \
    --tags Key=tag-key,Value=tag-value
```

2. Spécifiez les paramètres suivants dans la commande :

   - `--source-location-arn`— Spécifiez le nom de ressource Amazon (ARN) de l'emplacement source lors de votre transfert.
   - `--destination-location-arn`— Spécifiez l'ARN du lieu de destination lors de votre transfert.
   - `--tags`— Spécifiez les balises que vous souhaitez appliquer à la tâche.

Pour plusieurs balises, séparez chaque paire clé-valeur par un espace.

3. (Facultatif) Spécifiez d'autres paramètres adaptés à votre scénario de transfert.

   Pour une liste de`--options`, voir la commande create-task.

4. Exécutez la commande `create-task`.

   Vous obtenez une réponse qui indique la tâche que vous venez de créer.

```
{
    "TaskArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
abcdef01234567890"
}
```

Pour afficher les balises que vous avez ajoutées à cette tâche, vous pouvez utiliser la list-tags-for-resourcecommande.

Marquer l'exécution de vos DataSync tâches

Vous pouvez étiqueter chaque exécution de votre DataSync tâche.

Si votre tâche possède déjà des balises, n'oubliez pas ce qui suit concernant l'utilisation de balises lors de l'exécution des tâches :

- Si vous démarrez votre tâche avec la console, ses balises créées par l'utilisateur sont automatiquement appliquées à l'exécution de la tâche. Toutefois, les balises créées par le système qui commencent par ne `aws:` sont pas appliquées.
- Si vous démarrez votre tâche avec l' DataSync API ou AWS CLI si ses balises ne sont pas appliquées automatiquement à l'exécution de la tâche.

Utilisation de la console DataSync

Pour ajouter, modifier ou supprimer des balises lors de l'exécution d'une tâche, vous devez démarrer la tâche avec des options de remplacement.

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches.

3. Choisissez la tâche.
4. Choisissez Démarrer, puis choisissez l'une des options suivantes :
   - Commencez par les valeurs par défaut : applique toutes les balises associées à votre tâche.
   - Commencez par remplacer les options : vous permet d'ajouter, de modifier ou de supprimer des balises pour l'exécution de cette tâche particulière.

À l'aide du AWS CLI

1. Copiez la `start-task-execution` commande suivante :

```
aws datasync start-task-execution \
    --task-arn 'arn:aws:datasync:region:account-id:task/task-id' \
    --tags Key=tag-key,Value=tag-value
```

2. Spécifiez les paramètres suivants dans la commande :
   - `--task-arn`— Spécifiez l'ARN de la tâche que vous souhaitez démarrer.
   - `--tags`— Spécifiez les balises que vous souhaitez appliquer à cette exécution spécifique de la tâche.

     Pour plusieurs balises, séparez chaque paire clé-valeur par un espace.
3. (Facultatif) Spécifiez d'autres paramètres adaptés à votre situation.

   Pour plus d'informations, consultez la commande start-task-execution.
4. Exécutez la commande `start-task-execution`.

   Vous obtenez une réponse qui indique l'exécution de la tâche que vous venez de démarrer.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
abcdef01234567890"
}
```

Pour afficher les balises que vous avez ajoutées à cette tâche, vous pouvez utiliser la list-tags-for-resourcecommande.

Lancer une tâche pour transférer vos données

Une fois que vous avez créé votre tâche de AWS DataSync transfert, vous pouvez commencer à déplacer les données. Chaque exécution d'une tâche est appelée exécution de tâche. Pour plus d'informations sur ce qui se passe lors de l'exécution d'une tâche, consultezComment DataSync transférer des fichiers, des objets et des répertoires.

> **Important**
>
> Si vous prévoyez de transférer des données depuis ou vers un site Amazon S3, examinez comment cela DataSync peut affecter les frais de votre demande S3 et la page de DataSync tarification avant de commencer.

Démarrage de votre tâche

Une fois que vous avez créé votre tâche, vous pouvez commencer à déplacer les données immédiatement.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches.
3. Choisissez la tâche que vous souhaitez exécuter.

   Assurez-vous que le statut de la tâche est disponible. Vous pouvez également sélectionner plusieurs tâches.
4. Choisissez Actions, puis choisissez l'une des options suivantes :
   - Démarrer : exécute la tâche (ou les tâches si vous en avez sélectionné plusieurs).
   - Commencez par remplacer les options : vous permet de modifier certains paramètres de vos tâches avant de commencer à déplacer des données. Lorsque vous êtes prêt, choisissez Démarrer.
5. Choisissez Voir les détails de l'exécution pour afficher les détails relatifs à l'exécution de la tâche en cours.

En utilisant le AWS CLI

Pour démarrer votre DataSync tâche, il vous suffit de spécifier le nom de ressource Amazon (ARN) de la tâche que vous souhaitez exécuter. Voici un exemple de `start-task-execution` commande :

```
aws datasync start-task-execution \
    --task-arn 'arn:aws:datasync:region:account-id:task/task-id'
```

L'exemple suivant démarre une tâche avec quelques paramètres différents des paramètres par défaut de la tâche :

```
aws datasync start-task-execution \
    --override-options VerifyMode=NONE,OverwriteMode=NEVER,PosixPermissions=NONE
```

La commande renvoie un ARN pour l'exécution de votre tâche, comme dans l'exemple suivant :

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:209870788375:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"
}
```

> **Note**
>
> Chaque agent peut exécuter une seule tâche à la fois.

Utilisation de l' DataSync API

Vous pouvez démarrer votre tâche en utilisant l'StartTaskExecutionopération. Utilisez l'DescribeTaskExecutionopération pour obtenir des informations sur l'exécution de la tâche en cours.

Une fois démarrée, vous pouvez vérifier l'état de l'exécution de la tâche au fur et à mesure que vos données sont DataSync copiées. Vous pouvez également limiter la bande passante d'exécution des tâches si nécessaire.

Statuts d'exécution des tâches

Lorsque vous démarrez une DataSync tâche, ces statuts peuvent s'afficher. (Les statuts des tâches sont différents des statuts d'exécution des tâches.)

État de la console	État de l'API	Description
Mise en file d'attente	`QUEUED`	Une autre exécution de tâche est en cours d'exécution et utilise le même DataSync agent. Pour de plus amples informations, veuillez consulter Savoir quand votre tâche est en file d'attente.
Lancement	`LAUNCHING`	DataSync initialise l'exécution de la tâche. Ce statut disparaît généralement rapidement, mais peut prendre jusqu'à quelques minutes.
Lancé	`LAUNCHED`	DataSync a lancé l'exécution de la tâche.
Preparing	`PREPARING`	DataSync détermine les données à transférer. La préparation peut prendre quelques minutes, quelques heures, voire plus, selon le nombre de fichiers, d'objets ou de répertoires présents dans les deux emplaceme nts et selon la façon dont vous configurez votre tâche. Le fonctionnement de la préparation dépend également de votre mode de tâche. Pour de plus amples informati ons, veuillez consulter Comment DataSync prépare votre transfert de données.
Transfert	`TRANSFERR ING`	DataSync effectue le transfert de données proprement dit.
Vérification en cours	`VERIFYING`	DataSync vérifie l'intégrité de vos données à la fin du transfert.
Réussite	`SUCCESS`	L'exécution de la tâche a réussi.
Annulation	`CANCELLING`	L'exécution de la tâche est en cours d'annulation.
Erreur	`ERROR`	L'exécution de la tâche a échoué.

Savoir quand votre tâche est en file d'attente

Lorsque vous exécutez plusieurs tâches (par exemple, si vous transférez un ensemble de données volumineux), vous DataSync pouvez mettre en file d'attente les tâches à exécuter en série (premier entré, premier sorti). Voici quelques exemples de situations dans lesquelles cela se produit :

- Vous exécutez différentes tâches qui utilisent le même DataSync agent. Bien que vous puissiez utiliser le même agent pour plusieurs tâches, un agent ne peut exécuter qu'une seule tâche à la fois.
- L'exécution d'une tâche est en cours et vous lancez d'autres exécutions de la même tâche à l'aide de filtres ou de manifestes différents.

Dans chaque exemple, les tâches en file d'attente ne démarrent pas tant que la tâche qui les attend n'est pas terminée.

Annulation de l'exécution de vos tâches

Vous pouvez arrêter l'exécution de toute DataSync tâche en cours ou en file d'attente.

Pour annuler l'exécution d'une tâche à l'aide de la console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches.
3. Sélectionnez l'ID de tâche pour la tâche en cours d'exécution que vous souhaitez surveiller.

   L'état de la tâche doit être En cours d'exécution.
4. Choisissez Historique pour afficher les exécutions de la tâche.
5. Sélectionnez l'exécution de la tâche que vous souhaitez arrêter, puis choisissez Arrêter.
6. Dans la boîte de dialogue, choisissez Stop.

Pour annuler une tâche en cours ou en file d'attente à l'aide de l' DataSync API, consultez. CancelTaskExecution

Annulation automatique des tâches bloquées

Parfois, l'exécution d'une DataSync tâche en cours peut être bloquée.

Surveillance de vos AWS DataSync transferts

La surveillance est importante pour maintenir la fiabilité et les performances de vos activités de AWS DataSync transfert. Nous vous recommandons de collecter des données de surveillance afin de pouvoir corriger plus facilement les erreurs éventuelles. Avant de commencer la surveillance DataSync, créez toutefois un plan de surveillance qui inclut les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

AWS fournit divers services et outils de surveillance DataSync. Vous pouvez configurer certains d'entre eux pour effectuer la surveillance à votre place, mais d'autres nécessitent une intervention manuelle. Nous vous recommandons d'automatiser le plus possible les tâches de supervision.

Rubriques

- Comprendre les compteurs de performance du transfert de données
- Surveillance des transferts de données avec Amazon CloudWatch Metrics
- Surveillance de vos transferts de données à l'aide de rapports de tâches
- Surveillance des transferts de données avec Amazon CloudWatch Logs
- Journalisation des appels d' AWS DataSync API avec AWS CloudTrail
- Surveillance des événements à l'aide d'Amazon EventBridge
- Surveillance AWS DataSync à l'aide d'outils manuels

Comprendre les compteurs de performance du transfert de données

Lorsque vous démarrez une tâche, AWS DataSync fournit des compteurs pour vous aider à suivre les performances et la progression de votre transfert de données.

Utilisez les informations suivantes pour comprendre ce que représente chaque compteur. Vous pouvez consulter ces compteurs dans la DataSync console ou dans une DescribeTaskExecutionréponse. Certains compteurs ne sont pas disponibles dans tous les modes de tâche.

console	**DescribeTaskExecution**	Support du mode tâche	Description
–	`BytesWritten`	Amélioré, basique	Le nombre d'octets logiques qui écrivent DataSync réellement sur l'emplacement de destination.
Débit de données	–	Amélioré, basique	Vitesse à laquelle les octets DataSync logiques sont écrits vers l'emplacement de destination. Si vous utilisez DescribeTaskExecution, la façon dont vous calculez ce compteur dépend de votre mode de tâche : • Mode amélioré : Diviser `BytesWritten` par `TotalDuration` • Mode de base : Diviser `BytesWritten` par `TransferDuration`

console	**DescribeTaskExecution**	Support du mode tâche	Description
Données transférées	`BytesTransferred`	Amélioré, basique	Nombre d'octets DataSync envoyés au réseau avant la compression (si la compression est possible). Pour connaître le nombre d'octets transférés sur le réseau, consultez le compteur de débit réseau (dans la console) ou `BytesCompressed` (dans DescribeTaskExecution) le compteur.

console	**DescribeTaskExecution**	Support du mode tâche	Description
Supprimé de la destination	`FilesDeleted`	Amélioré, basique	Le nombre de fichiers, d'objets et de répertoires DataSync réellement supprimés dans votre emplacement de destination. Si vous ne configurez pas votre tâche pour supprimer des données dans la destination qui ne figurent pas dans la source : • Supprimé de la destination ne s'affiche pas dans la console. • `FilesDeleted` affiche toujours une valeur de `0`.
–	`EstimatedBytesToTransfer`	Amélioré, basique	Le nombre d'octets logiques qui DataSync devraient écrire sur l'emplacement de destination.

console	**DescribeTaskExecution**	Support du mode tâche	Description
–	`Estimated FilesToDelete`	Amélioré, basique	Le nombre de fichiers, d'objets et de répertoires qui DataSync devraient être supprimés dans votre emplacement de destination. Si vous ne configurez pas votre tâche pour supprimer des données dans la destination qui ne figurent pas dans la source, la valeur est toujours`0`.

console	**DescribeTaskExecution**	Support du mode tâche	Description
–	`EstimatedFilesToTransfer`	Amélioré, basique	Le nombre de fichiers, d'objets et de répertoires qui DataSync devraient être transférés sur le réseau. Cette valeur est calculée lors de la DataSync préparation du transfert. La façon dont cela est calculé dépend principalement du mode de transfert que vous utilisez : • Si le mode de transfert est configuré pour transférer uniquement les données modifiées : le calcul est basé sur la comparaison du contenu des emplacements source et de destination et sur la détermination de la différence à transférer. La différence peut inclure :

console	`DescribeTaskExecution`	Support du mode tâche	Description
			• Tout ce qui est ajouté ou modifié à l'emplacement source. • Tout ce qui se trouve aux deux emplacements et qui est modifié à la destination après un transfert initial (sauf si vous configurez votre tâche pour ne pas remplacer les données dans la destination). • (Mode de base uniquement) Nombre d'éléments qui devraient DataSync être supprimés (si vous configurez votre tâche pour supprimer des données dans la destination). • Si le mode de transfert est configuré pour transférer toutes les données : le

console	**DescribeTaskExecution**	Support du mode tâche	Description
			calcul est basé uniquement sur les éléments DataSync trouvés à l'emplacement source.
Débit de fichiers	–	Amélioré, basique	Vitesse à laquelle DataSync les fichiers, les objets et les répertoires sont transférés sur le réseau. Si vous utilisez DescribeTaskExecution, la façon dont vous calculez ce compteur dépend de votre mode de tâche : • Mode amélioré : Diviser `FilesTransferred` par `TotalDuration` • Mode de base : Diviser `FilesTransferred` par `TransferDuration`

console	**DescribeTaskExecution**	Support du mode tâche	Description
–	`FilesFailed`	Amélioré	Nombre d'objets dont la préparation, le transfert, la vérification et la suppression DataSync échouent lors de l'exécution de la tâche. En cas d'échec, vous pouvez les voir à côté des compteurs Préparé, Transféré, Ignoré et Supprimé de la console de destination, respectivement.

console	**DescribeTaskExecution**	Support du mode tâche	Description
Répertorié à la source	`FilesListed.AtSource`	Amélioré	Le nombre d'objets DataSync trouvés à votre emplacement source. • Dans le cas d'un manifeste, DataSync répertorie uniquement le contenu de votre manifeste (et non tout ce qui se trouve dans votre emplacement source). • Avec un filtre d'inclusion, DataSync répertorie uniquement ce qui correspond au filtre à votre emplacement source. • Avec un filtre d'exclusion, DataSync répertorie tout ce qui se trouve à votre emplacement source avant d'appliquer le filtre.

console	**DescribeTaskExecution**	Support du mode tâche	Description
–	`FilesListed.AtDestinationForDelete`	Amélioré	Le nombre d'objets trouvés DataSync sur votre lieu de destination. Ce compteur n'est applicable que si vous configurez votre tâche pour supprimer des données dans la destination qui ne figurent pas dans la source.

console	**`DescribeTaskExecution`**	Support du mode tâche	Description
Débit du réseau*	`BytesCompressed`	Amélioré, basique	Nombre d'octets physiques DataSync transférés sur le réseau après compression (si la compression est possible). Ce nombre est généralement inférieur aux données transférées (dans la console) ou `BytesTransferred` (dans DescribeTaskExecution), sauf si les données ne sont pas compressibles. * — Pour le mode amélioré, le débit réseau ne s'affiche pas dans la console.

console	**`DescribeTaskExecution`**	Support du mode tâche	Description
Pourcentage compressé	–	Base	Pourcentage de données de transfert DataSync compressé es avant de les envoyer sur le réseau. Si vous utilisez DescribeTaskExecution, vous pouvez calculer ce compteur avec`1 - BytesCompressed / BytesWritten` .

console	**`DescribeTaskExecution`**	Support du mode tâche	Description
Préparé	`FilesPrepared`	Amélioré	Le nombre d'objets qui DataSync tenteront d'être transférés après avoir comparé vos emplacements source et de destination. Dans la console, ce compteur peut également vous indiquer le nombre d'objets DataSync ignorés lors de la préparation. Pour de plus amples informations, veuillez consulter Comment DataSync prépare votre transfert de données. Ce compteur n'est pas applicable si vous configurez votre tâche pour transférer toutes les données. Dans ce scénario, DataSync copie tout de la source vers la destination sans comparer les différences entre les emplacements.

console	**DescribeTaskExecution**	Support du mode tâche	Description
Taux de traitement	–	Amélioré, basique	La vitesse à laquelle DataSync les fichiers, les objets et les répertoires sont lus dans votre emplacement source. Le taux de traitement est basé sur plusieurs CloudWatch indicateurs. Les mesures exactes dépendent du mode de tâche que vous utilisez. Mode amélioré : • `FilesListedSource` • `FilesPrepared` • `FilesTransferred` • `FilesVerified` Mode de base : • `FilesPreparedSource` • `FilesPreparedDestination` • `FilesTransferred`

console	**DescribeTaskExecution**	Support du mode tâche	Description
			• `FilesVerifiedSource` • `FilesVerifiedDestination`
Restant	–	Base	Le nombre restant de fichiers, d'objets et de répertoires qui DataSync devraient être transférés sur le réseau. Si vous utilisez DescribeTaskExecution, vous pouvez calculer ce compteur en soustrayant de. `FilesTransferred` `EstimatedFilesToTransfer`

console	**DescribeTaskExecution**	Support du mode tâche	Description
Ignoré*	`FilesSkipped`	Amélioré, basique	Le nombre de fichiers, d'objets et de répertoires DataSync ignorés lors de votre transfert. * — Pour le mode amélioré, Skipped ne s'affiche pas dans la console. Au lieu de cela, les éléments ignorés sont inclus dans le compteur préparé lorsque vous transférez uniquement les données modifiées ou dans le compteur transféré lors du transfert de toutes les données.

console	**`DescribeTaskExecution`**	Support du mode tâche	Description
Transféré	`FilesTransferred`	Amélioré, basique	Le nombre de fichiers, d'objets et de répertoires DataSync transférés sur le réseau. Cette valeur est mise à jour régulièrement pendant l'exécution de la tâche lorsqu'un élément est lu depuis la source et envoyé sur le réseau. En cas d' DataSync échec du transfert, cette valeur peut être inférieure à `Estimated FilesToTransfer`. Dans certains cas, cette valeur peut également être supérieure à `Estimated FilesToTransfer`. Ce compteur est spécifique à l'implémentation de certains types d'emplacement. Ne l'utilisez donc pas pour indiquer exactement ce qui est transféré ou pour

console	**DescribeTaskExecution**	Support du mode tâche	Description
			surveiller l'exécution de vos tâches. Dans la console, ce compteur peut également vous indiquer le nombre d'objets DataSync ignorés lors du transfert d'une tâche en mode amélioré. Pour de plus amples informations, veuillez consulter Comment DataSync transfèrent vos données.
Vérifié	`FilesVerified`	Amélioré, basique	Le nombre de fichiers, d'objets et de répertoires qui sont DataSync vérifiés lors de votre transfert. Lorsque vous configurez votre tâche pour vérifier uniquement les données transférées, DataSync elle ne vérifie pas les répertoires dans certains cas, ni les fichiers ou objets dont le transfert échoue.

Surveillance des transferts de données avec Amazon CloudWatch Metrics

Amazon CloudWatch fournit des indicateurs pour suivre les performances des DataSync transferts et résoudre les problèmes liés à votre tâche de transfert.

Vous pouvez surveiller les performances des AWS DataSync transferts à l'aide CloudWatch des métriques Amazon. DataSync les métriques sont automatiquement envoyées CloudWatch à intervalles de 5 minutes (quelle que soit la façon dont vous configurez la journalisation). Les indicateurs sont conservés pendant une période de 15 mois.

Pour consulter CloudWatch les statistiques relatives à DataSync, vous pouvez utiliser les outils suivants :

- La CloudWatch console
- La CloudWatch CLI
- L' CloudWatch API
- La DataSync console (sur la page de détails de l'exécution de la tâche)

Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

CloudWatch métriques pour DataSync

DataSync les métriques utilisent l'espace de `aws/datasync` noms et fournissent des métriques pour les dimensions suivantes :

- AgentId— L'identifiant unique de l'agent (si votre tâche utilise un agent).
- TaskId— L'identifiant unique de la tâche. Elle prend la forme suivante : `task-01234567890abcdef`.

L'espace de noms `aws/datasync` inclut les métriques suivantes. Certains indicateurs ne sont pas disponibles dans tous les modes de tâche.

CloudWatch métrique	Support du mode tâche	Description
`BytesCompressed`	Base	Nombre d'octets physiques DataSync transférés sur le réseau après compression (si la compression est possible). Ce nombre est généralement inférieur à `BytesTransferred` sauf si les données ne sont pas compressibles. Unité : octets
`BytesPreparedDestination`	Base	Nombre d'octets logiques préparés DataSync à l'emplacement de destination. Unité : octets
`BytesPreparedSource`	Base	Nombre d'octets logiques préparés DataSync à l'emplacement source. Unité : octets
`BytesTransferred`	Base	Nombre d'octets DataSync envoyés au réseau avant la compression (si la compression est possible). Pour le nombre d'octets transférés sur le réseau, consultez la `BytesCompressed` métrique. Unité : octets
`BytesVerifiedDestination`	Base	Le nombre d'octets logiques qui sont DataSync vérifiés à l'emplacement de destination. Unité : octets
`BytesVerifiedSource`	Base	Nombre d'octets logiques qui DataSync vérifient à l'emplacement source. Unités : octets
`BytesWritten`	Amélioré, basique	Nombre d'octets logiques qui DataSync écrivent sur l'emplacement de destination.

CloudWatch métrique	Support du mode tâche	Description
		Unité : octets
`FilesDeleted`	Amélioré, basique	Le nombre de fichiers, d'objets et de répertoires DataSync supprimés dans votre emplacement de destination. Si vous ne configurez pas votre tâche pour supprimer des données dans la destination qui ne figurent pas dans la source, la valeur est toujours`0`. Unité : nombre
`FilesListedSource`	Amélioré	Le nombre d'objets DataSync trouvés à votre emplacement source. Unité : nombre
`FilesPrepared`	Amélioré	Le nombre d'objets qui DataSync tenteront d'être transférés après avoir comparé vos emplacements source et de destination. Pour de plus amples informations, veuillez consulter Comment DataSync prépare votre transfert de données. Cette métrique n'est pas applicable si vous configurez votre tâche pour transférer toutes les données. Dans ce scénario, DataSync copie tout de la source vers la destination sans comparer les différences entre les emplacements. Unité : nombre
`FilesPreparedDestination`	Base	Nombre de fichiers, d'objets et de répertoires préparés DataSync à l'emplacement de destination. Unité : nombre

CloudWatch métrique	Support du mode tâche	Description
`FilesPreparedSource`	Base	Nombre de fichiers, d'objets et de répertoires DataSync préparés à l'emplacement source. Unité : nombre
`FilesSkipped`	Base	Le nombre de fichiers, d'objets et de répertoires DataSync ignorés lors de votre transfert. Unité : nombre
`FilesTransferred`	Amélioré, basique	Le nombre de fichiers, d'objets et de répertoires DataSync transférés sur le réseau. Cette valeur est mise à jour périodiquement pendant l'exécution de la tâche lorsqu'un élément est lu depuis la source et envoyé sur le réseau. **Note** Cette valeur peut être inférieure à celle d'une `EstimatedFilesToTransfer` DescribeTaskExecutionréponse en cas d' DataSync échec du transfert. Dans certains cas, cette valeur peut également être supérieure à `EstimatedFilesToTransfer`. Cette métrique est spécifique à l'implémentation pour certains types de sites. Ne l'utilisez donc pas comme une indication exacte de ce qui a été transféré ou pour surveiller l'exécution de vos tâches. Unité : nombre

CloudWatch métrique	Support du mode tâche	Description
`FilesVerified`	Amélioré	Le nombre d'objets qui sont DataSync vérifiés lors de votre transfert. Unité : nombre
`FilesVerifiedDestination`	Base	Nombre de fichiers, d'objets et de répertoires DataSync vérifiés à l'emplacement de destination. Unité : nombre
`FilesVerifiedSource`	Base	Nombre de fichiers, d'objets et de répertoires DataSync vérifiés à l'emplacement source. Unité : nombre

Surveillance de vos transferts de données à l'aide de rapports de tâches

Les rapports de tâches fournissent des informations détaillées sur les AWS DataSync tentatives de transfert, d'omission, de vérification et de suppression au cours de l'exécution d'une tâche. Pour de plus amples informations, veuillez consulter Comment DataSync transférer des fichiers, des objets et des répertoires.

Les rapports de tâches sont générés au format JSON. Vous pouvez personnaliser le niveau de détail de vos rapports :

- Les rapports de tâches récapitulatifs vous fournissent les détails nécessaires sur l'exécution de vos tâches, tels que le nombre de fichiers transférés et la DataSync possibilité de vérifier l'intégrité des données de ces fichiers.
- Les rapports de tâches standard incluent un résumé ainsi que des rapports détaillés répertoriant chaque fichier, objet ou dossier DataSync tenté de transférer, d'ignorer, de vérifier ou de supprimer. Avec un rapport de tâches standard, vous pouvez également spécifier le niveau du rapport pour n'afficher que les erreurs d'exécution de la tâche ou ses réussites et erreurs.

Cas d'utilisation

Voici quelques situations dans lesquelles les rapports de tâches peuvent vous aider à surveiller et à auditer vos transferts de données :

- Lorsque vous migrez des millions de fichiers, identifiez rapidement les fichiers DataSync présentant des problèmes de transfert.
- Vérifiez chain-of-custody les processus relatifs à vos fichiers.

Rapports de tâches récapitulatifs uniquement

Un rapport qui n'est qu'un résumé de l'exécution d'une tâche inclut les détails suivants :

- Celui Compte AWS qui a exécuté l'exécution de la tâche
- Les lieux d'origine et de destination
- Nombre total de fichiers, d'objets et de dossiers ignorés, transférés, vérifiés et supprimés
- Nombre total d'octets (logiques et physiques) transférés
- Si l'exécution de la tâche a été terminée, annulée ou a rencontré une erreur
- Les heures de début et de fin (y compris la durée totale du transfert)
- Les paramètres de la tâche (tels que les limites de bande passante, la vérification de l'intégrité des données et les autres options de DataSync transfert)

Rapports de tâches standard

Un rapport de tâches standard inclut un résumé de l'exécution de vos tâches ainsi que des rapports détaillés sur les DataSync tentatives de transfert, d'omission, de vérification et de suppression.

Rubriques

- Niveau du rapport
- Rapports transférés
- Rapports ignorés
- Rapports vérifiés
- Rapports supprimés

Niveau du rapport

Avec les rapports de tâches standard, vous pouvez choisir l'un des niveaux de rapport suivants :

- Erreurs uniquement
- Succès et erreurs (essentiellement une liste de tout ce qui s'est passé pendant l'exécution de votre tâche)

Par exemple, vous souhaiterez peut-être voir quels fichiers DataSync ont été ignorés avec succès lors de votre transfert et ceux qui n'ont pas été ignorés. Les fichiers qui DataSync ont été correctement ignorés peuvent être ceux que vous DataSync souhaitez délibérément exclure car ils existent déjà dans votre emplacement de destination. Cependant, une erreur ignorée, par exemple, peut indiquer que vous DataSync ne disposez pas des autorisations nécessaires pour lire un fichier.

Rapports transférés

Liste des fichiers, objets et répertoires qui DataSync ont tenté d'être transférés lors de l'exécution de la tâche. Un rapport transféré inclut les informations suivantes :

- Les chemins d'accès aux données transférées
- Ce qui a été transféré (contenu, métadonnées ou les deux)
- Les métadonnées, qui incluent le type de données, la taille du contenu (objets et fichiers uniquement), etc.
- Heure à laquelle un article a été transféré
- La version de l'objet (si la destination est un compartiment Amazon S3 sur lequel la gestion des versions est activée)
- Si quelque chose a été remplacé dans la destination
- Si un article a été transféré avec succès

> **Note**
>
> Lorsque vous déplacez des données entre des compartiments S3, le préfixe que vous spécifiez dans votre emplacement source peut apparaître dans votre rapport (ou dans les CloudWatch journaux Amazon), même si ce préfixe n'existe pas en tant qu'objet dans votre

emplacement de destination. (Dans la DataSync console, vous remarquerez peut-être également que ce préfixe apparaît sous forme de données ignorées ou vérifiées.)

Rapports ignorés

Liste de fichiers, d'objets et de répertoires trouvés dans DataSync votre emplacement source mais dont le transfert n'a pas été tenté. Les raisons pour lesquelles des DataSync données sont ignorées peuvent dépendre de plusieurs facteurs, tels que la manière dont vous configurez vos tâches et les autorisations du système de stockage. Voici quelques exemples :

- Un fichier existe dans vos emplacements source et de destination. Le fichier de la source n'a pas été modifié depuis l'exécution précédente de la tâche. Comme vous ne transférez que des données modifiées, ce fichier DataSync ne sera pas transféré la prochaine fois que vous exécuterez votre tâche.
- Un objet qui existe dans vos deux emplacements change dans votre source. Lorsque vous exécutez votre tâche, cet objet DataSync est ignoré dans votre destination car votre tâche ne remplace pas les données dans la destination.
- DataSync ignore un objet de votre source qui utilise une classe de stockage d'archivage et qui n'est pas restauré. Vous devez restaurer un objet archivé DataSync pour pouvoir le lire.
- DataSync ignore un fichier, un objet ou un répertoire dans votre emplacement source car il ne peut pas le lire. Si cela se produit et n'est pas prévu, vérifiez les autorisations d'accès de votre espace de stockage et assurez-vous qu'il DataSync peut lire ce qui a été ignoré.

Un rapport ignoré inclut les informations suivantes :

- Les chemins pour les données ignorées
- Heure à laquelle un élément a été ignoré
- La raison pour laquelle il a été ignoré
- Si un élément a été ignoré avec succès

> **Note**
>
> Les rapports ignorés peuvent être volumineux lorsqu'ils incluent des réussites et des erreurs, que vous configurez votre tâche pour ne transférer que les données modifiées et que les données sources existent déjà dans la destination.

Rapports vérifiés

Liste des fichiers, objets et répertoires dont l'intégrité DataSync a été testée lors de l'exécution de la tâche. Un rapport de données vérifié inclut les informations suivantes :

- Les chemins d'accès aux données vérifiées
- Heure à laquelle un article a été vérifié
- La raison de l'erreur de vérification (le cas échéant)
- Les SHA256 checksums de la source et de la destination (fichiers uniquement)
- Si un article a été vérifié avec succès

Notez ce qui suit à propos des rapports vérifiés :

- Lorsque vous configurez votre tâche pour vérifier uniquement les données transférées, DataSync elle ne vérifie pas les répertoires dans certains cas, ni les fichiers ou objets dont le transfert échoue. Dans les deux cas, DataSync n'inclut pas les données non vérifiées dans ce rapport.
- Si vous utilisez le mode amélioré, la vérification peut prendre plus de temps que d'habitude si vous transférez des objets volumineux.

Rapports supprimés

Liste des fichiers, des répertoires et des objets qui ont été supprimés lors de l'exécution de la tâche. DataSync génère ce rapport uniquement si vous configurez votre tâche pour supprimer des données dans l'emplacement de destination qui ne se trouve pas dans la source. Un rapport de données supprimé inclut les informations suivantes :

- Les chemins pour les données supprimées
- Si un élément a été correctement supprimé
- Heure à laquelle un élément a été supprimé

Exemples de rapports de tâches

Le niveau de détail de votre rapport de tâches dépend de vous. Voici quelques exemples de rapports de données transférés avec la configuration suivante :

- Type de rapport — Standard
- Niveau du rapport — Succès et erreurs

> **Note**
>
> Les rapports utilisent la norme ISO-8601 pour le format d'horodatage. Les temps sont exprimés en UTC et mesurés en nanosecondes. Ce comportement est différent de la façon dont certains autres indicateurs des rapports de tâches sont mesurés. Par exemple, les détails de l'exécution des tâches, tels que `TransferDuration` et`VerifyDuration`, sont mesurés en millisecondes.

Les rapports de tâches en mode amélioré utilisent un schéma légèrement différent de celui des rapports de tâches en mode de base. Les exemples suivants peuvent vous aider à savoir à quoi vous attendre de vos rapports en fonction du mode de tâche que vous utilisez.

Exemples de rapports de données transférés avec statut de réussite

Les rapports suivants indiquent les transferts réussis pour un objet nommé`object1.txt`.

Enhanced mode

```
{
    "TaskExecutionId": "exec-abcdefgh12345678",
    "Transferred": [{
        "RelativePath": "object1.txt",
        "SourceMetadata": {
            "Type": "Object",
            "ContentSize": 6,
            "LastModified": "2024-10-04T14:40:55Z",
            "SystemMetadata": {
                "ContentType": "binary/octet-stream",
                "ETag": "\"9b2d7e1f8054c3a2041905d0378e6f14\"",
                "ServerSideEncryption": "AES256"
            },
            "UserMetadata": {},
```

```
            "Tags": []
        },
        "Overwrite": "False",
        "DstS3VersionId": "jtqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
        "TransferTimestamp": "2024-10-04T14:48:39.748862183Z",
        "TransferType": "CONTENT_AND_METADATA",
        "TransferStatus": "SUCCESS"
    }]
}
```

Basic mode

```
{
    "TaskExecutionId": "exec-abcdefgh12345678",
    "Transferred": [{
        "RelativePath": "/object1.txt",
        "SrcMetadata": {
            "Type": "Regular",
            "ContentSize": 6,
            "Mtime": "2022-01-07T16:59:26.136114671Z",
            "Atime": "2022-01-07T16:59:26.136114671Z",
            "Uid": 0,
            "Gid": 0,
            "Mode": "0644"
        },
        "Overwrite": "False",
        "DstS3VersionId": "jtqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
        "TransferTimestamp": "2022-01-07T16:59:45.747270957Z",
        "TransferType": "CONTENT_AND_METADATA",
        "TransferStatus": "SUCCESS"
    }]
}
```

Exemples de rapports de données transférés avec statut d'erreur

Les rapports suivants fournissent des exemples de situations dans lesquelles il est DataSync impossible de transférer un objet nommé`object1.txt`.

Enhanced mode

Ce rapport montre qu'il est DataSync impossible d'accéder à un objet nommé en `object1.txt` raison d'un problème d' AWS KMS autorisation. (Si une erreur de ce type s'affiche, consultezAccès aux compartiments S3 à l'aide du chiffrement côté serveur.)

```
{
    "TaskExecutionId": "exec-abcdefgh12345678",
    "Transferred": [{
        "RelativePath": "object1.txt",
        "SourceMetadata": {
            "Type": "Object",
            "ContentSize": 6,
            "LastModified": "2022-10-07T20:48:32Z",
            "SystemMetadata": {
                "ContentType": "binary/octet-stream",
                "ETag": "\"3a7c0b2f1d9e5c4a6f8b2e0d1c9f7a3b2\"",
                "ServerSideEncryption": "AES256"
            },
            "UserMetadata": {},
            "Tags": []
        },
        "Overwrite": "False",
        "TransferTimestamp": "2022-10-09T16:05:11.134040717Z",
        "TransferType": "CONTENT_AND_METADATA",
        "TransferStatus": "FAILED",
        "ErrorCode": "AccessDenied",
        "ErrorDetail": "User: arn:aws:sts::111222333444:assumed-role/
AWSDataSyncS3Bucket/AwsSync-loc-0b3017fc4ba4a2d8d is not authorized
 to perform: kms:GenerateDataKey on resource: arn:aws:kms:us-
east-1:111222333444:key/1111aaaa-22bb-33cc-44d-5555eeee6666 because no identity-
based policy allows the kms:GenerateDataKey action"
    }]
}
```

Basic mode

Ce rapport indique qu'un objet nommé `object1.txt` n'a pas été transféré en raison d'un problème d'autorisation du compartiment S3. (Si une erreur de ce type s'affiche, consultez Fournir DataSync un accès aux compartiments S3.)

```
{
    "TaskExecutionId": "exec-abcdefgh12345678",
    "Transferred": [{
        "RelativePath": "/object1.txt",
        "SrcMetadata": {
            "Type": "Regular",
            "ContentSize": 6,
            "Mtime": "2022-01-07T16:59:26.136114671Z",
```

```
            "Atime": "2022-01-07T16:59:26.136114671Z",
            "Uid": 0,
            "Gid": 0,
            "Mode": "0644"
        },
        "Overwrite": "False",
        "DstS3VersionId": "jtqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
        "TransferTimestamp": "2022-01-07T16:59:45.747270957Z",
        "TransferType": "CONTENT_AND_METADATA",
        "TransferStatus": "FAILED",
        "FailureReason": "S3 Get Object Failed",
        "FailureCode": 40974
    }]
}
```

Limites

- Les rapports de tâches individuels ne peuvent pas dépasser 5 Mo. Si vous copiez un grand nombre de fichiers, votre rapport de tâches peut être divisé en plusieurs rapports.
- Dans certains cas, la création de rapports de tâches peut affecter les performances de votre transfert de données. Par exemple, vous pouvez le remarquer lorsque votre connexion réseau présente une latence élevée et que les fichiers que vous transférez sont petits ou que vous ne copiez que les modifications de métadonnées.

Création de vos rapports de DataSync tâches

AWS DataSync les rapports de tâches ne peuvent être qu'un résumé de l'exécution de vos tâches ou un ensemble de rapports détaillés sur les DataSync tentatives de transfert, d'omission, de vérification et de suppression.

Prérequis

Avant de créer un rapport de tâches, vous devez effectuer les opérations suivantes.

Rubriques

- Créez un compartiment S3 pour vos rapports de tâches
- DataSync Autoriser le téléchargement de rapports de tâches dans votre compartiment S3

Créez un compartiment S3 pour vos rapports de tâches

Si vous n'en avez pas déjà un, créez un compartiment S3 dans lequel DataSync vous pourrez télécharger votre rapport de tâches. Les rapports sont stockés dans la classe de stockage S3 Standard.

Nous recommandons ce qui suit pour ce compartiment :

- Si vous envisagez de transférer des données vers un compartiment S3, n'utilisez pas le même compartiment pour votre rapport de tâches si vous désactivez l'option Conserver les fichiers supprimés. Sinon, tous les rapports de tâches précédents DataSync seront supprimés chaque fois que vous exécuterez une tâche, car ces rapports n'existent pas dans votre emplacement source.
- Pour éviter une configuration complexe des autorisations d'accès, assurez-vous que le compartiment de votre rapport de tâches se trouve dans la même Compte AWS région que votre tâche de DataSync transfert.

DataSync Autoriser le téléchargement de rapports de tâches dans votre compartiment S3

Vous devez configurer un rôle AWS Identity and Access Management (IAM) qui permet de DataSync télécharger un rapport de tâches dans votre compartiment S3.

Dans la DataSync console, vous pouvez créer un rôle IAM qui, dans la plupart des cas, inclut automatiquement les autorisations nécessaires pour télécharger un rapport de tâches dans votre compartiment. N'oubliez pas que ce rôle généré automatiquement peut ne pas répondre à vos besoins du point de vue du moindre privilège. Ce rôle ne fonctionnera pas non plus si votre compartiment est chiffré à l'aide d'une clé gérée par le client AWS Key Management Service (AWS KMS) (SSE-KMS). Dans ces cas, vous pouvez créer le rôle manuellement à condition que le rôle effectue au moins les tâches suivantes :

- Empêche le problème de confusion entre les services au sein de l'entité de confiance associée au rôle.

  L'exemple complet suivant montre comment utiliser les touches contextuelles de condition `aws:SourceAccount` globale `aws:SourceArn` et les touches contextuelles pour éviter le problème de confusion lié aux adjoints DataSync.

  JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "datasync.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                "aws:SourceArn": "arn:aws:datasync:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

- Permet DataSync de télécharger un rapport de tâches dans votre compartiment S3.

  Pour ce faire, l'exemple suivant inclut l'`s3:PutObject`action uniquement pour un préfixe spécifique (`reports/`) dans votre compartiment.

  JSON

```
{
        "Version": "2012-10-17",
        "Statement": [{
            "Action": [
                "s3:PutObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::your-task-reports-bucket/reports/*"
        }]
}
```

- Si votre compartiment S3 est chiffré à l'aide d'une clé SSE-KMS gérée par le client, la politique de la clé doit inclure le rôle IAM DataSync utilisé pour accéder au compartiment.

  Pour de plus amples informations, veuillez consulter Accès aux compartiments S3 à l'aide du chiffrement côté serveur.

Création d'un rapport de tâches récapitulatif uniquement

Vous pouvez configurer un rapport de tâche qui inclut un résumé uniquement lors de la création, du démarrage ou de la mise à jour de la tâche. DataSync

Les étapes suivantes montrent comment configurer un rapport de tâches récapitulatif uniquement lors de la création d'une tâche.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Faites défiler la page vers le bas jusqu'à la section Rapport des tâches. Pour le type de rapport, sélectionnez Résumé uniquement.
5. Pour le compartiment S3 pour les rapports, choisissez un compartiment S3 dans lequel vous DataSync souhaitez télécharger votre rapport de tâches.

   > **Tip**
   >
   > Si vous envisagez de transférer des données vers un compartiment S3, n'utilisez pas le même compartiment pour votre rapport de tâches si vous désactivez l'option Conserver les fichiers supprimés. Sinon, tous les rapports de tâches précédents DataSync seront supprimés chaque fois que vous exécuterez une tâche, car ces rapports n'existent pas dans votre emplacement source.
6. Pour Dossier, entrez un préfixe à utiliser pour votre rapport de tâches lors du DataSync téléchargement du rapport dans votre compartiment S3 (par exemple,**`reports/`**).

   Assurez-vous d'inclure le caractère délimiteur approprié à la fin de votre préfixe. Ce caractère est généralement une barre oblique (`/`). Pour plus d'informations, consultez la section Organisation des objets à l'aide de préfixes dans le guide de l'utilisateur Amazon S3.
7. Pour IAM role (Rôle IAM), effectuez l'une des opérations suivantes :

- Choisissez Autogenerate pour créer DataSync automatiquement un rôle IAM avec les autorisations requises pour accéder au compartiment S3.

  Si un rôle IAM a DataSync déjà été créé pour ce compartiment S3, ce rôle est choisi par défaut.

- Choisissez un rôle IAM personnalisé que vous avez créé.

  Dans certains cas, il se peut que vous deviez créer le rôle vous-même. Pour de plus amples informations, veuillez consulter DataSync Autoriser le téléchargement de rapports de tâches dans votre compartiment S3.

  > **Important**
  > Si votre compartiment S3 est chiffré à l'aide d'une clé SSE-KMS gérée par le client, la politique de la clé doit inclure le rôle IAM DataSync utilisé pour accéder au compartiment.
  > Pour de plus amples informations, veuillez consulter Accès aux compartiments S3 à l'aide du chiffrement côté serveur.

8. Terminez la création de votre tâche, puis lancez-la pour commencer à transférer vos données.

Lorsque votre transfert est terminé, vous pouvez consulter votre rapport de tâches.

En utilisant le AWS CLI

1. Copiez la commande suivante `create-task` AWS Command Line Interface (AWS CLI) :

```
aws datasync create-task \
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh \
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-abcdefgh12345678 \
  --task-report-config '{
    "Destination":{
      "S3":{
        "Subdirectory":"reports/",
        "S3BucketArn":"arn:aws:s3:::your-task-reports-bucket",
        "BucketAccessRoleArn":"arn:aws:iam::123456789012:role/bucket-iam-role"
        }
```

```
    },
    "OutputType":"SUMMARY_ONLY"
  }'
```

2. Pour le `--source-location-arn` paramètre, spécifiez l'Amazon Resource Name (ARN) de l'emplacement source de votre transfert. Remplacez *us-east-1* par le numéro approprié Région AWS, remplacez *123456789012* par le Compte AWS numéro approprié et remplacez *12345678abcdefgh* par l'ID d'emplacement source approprié.
3. Pour le `--destination-location-arn` paramètre, spécifiez l'ARN de l'emplacement de destination de votre transfert. Remplacez *us-east-1* par le numéro approprié Région AWS, remplacez *123456789012* par le Compte AWS numéro approprié et remplacez *abcdefgh12345678* par le numéro de localisation de destination approprié.
4. Pour le `--task-report-config` paramètre, procédez comme suit :

   - `Subdirectory`— *reports/* Remplacez-le par le préfixe de votre compartiment S3 dans lequel vous DataSync souhaitez télécharger vos rapports de tâches.

     Assurez-vous d'inclure le caractère délimiteur approprié à la fin de votre préfixe. Ce caractère est généralement une barre oblique (`/`). Pour plus d'informations, consultez la section Organisation des objets à l'aide de préfixes dans le guide de l'utilisateur Amazon S3.
   - `S3BucketArn`— Spécifiez l'ARN du compartiment S3 dans lequel vous souhaitez télécharger votre rapport de tâches.

     > **Tip**
     >
     > Si vous envisagez de transférer des données vers un compartiment S3, n'utilisez pas le même compartiment pour votre rapport de tâches si vous désactivez l'option Conserver les fichiers supprimés. Sinon, tous les rapports de tâches précédents DataSync seront supprimés chaque fois que vous exécuterez une tâche, car ces rapports n'existent pas dans votre emplacement source.
   - `BucketAccessRoleArn`— Spécifiez le rôle IAM qui permet DataSync de télécharger un rapport de tâches dans votre compartiment S3.

     Pour de plus amples informations, veuillez consulter DataSync Autoriser le téléchargement de rapports de tâches dans votre compartiment S3.

> **Important**
>
> Si votre compartiment S3 est chiffré à l'aide d'une clé SSE-KMS gérée par le client, la politique de la clé doit inclure le rôle IAM DataSync utilisé pour accéder au compartiment.
> Pour de plus amples informations, veuillez consulter Accès aux compartiments S3 à l'aide du chiffrement côté serveur.

- `OutputType`— Spécifiez`SUMMARY_ONLY`.

  Pour de plus amples informations, veuillez consulter Rapports de tâches récapitulatifs uniquement.

5. Exécutez la `create-task` commande pour créer votre tâche.

   Vous obtenez une réponse semblable à la suivante qui indique l'ARN de la tâche que vous avez créée. Vous aurez besoin de cet ARN pour exécuter la `start-task-execution` commande.

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
}
```

6. Copiez la `start-task-execution` commande suivante.

```
aws datasync-task-report start-task-execution \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

7. Pour le `--task-arn` paramètre, spécifiez l'ARN de la tâche que vous démarrez. Utilisez l'ARN que vous avez reçu lors de l'exécution de la `create-task` commande.
8. Exécutez la commande `start-task-execution`.

Lorsque votre transfert est terminé, vous pouvez consulter votre rapport de tâches.

Création d'un rapport de tâches standard

Vous pouvez configurer un rapport de tâche standard lors de la création, du démarrage ou de la mise à jour de la tâche. DataSync

Les étapes suivantes montrent comment configurer un rapport de tâche standard lors de la création d'une tâche.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.
3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.
4. Faites défiler la page vers le bas jusqu'à la section Rapport des tâches. Pour Type de rapport, choisissez Rapport standard.
5. Pour le niveau du rapport, choisissez l'une des options suivantes :

   - Erreurs uniquement : votre rapport de tâches inclut uniquement les problèmes liés aux DataSync tentatives de transfert, d'omission, de vérification et de suppression.
   - Succès et erreurs : votre rapport de tâches indique ce qui a été transféré, ignoré, vérifié et supprimé DataSync avec succès et ce qui n'a pas été le cas.
   - Personnalisé : vous permet de choisir si vous souhaitez voir uniquement les erreurs ou les réussites et les erreurs pour des aspects spécifiques de votre rapport de tâches.

     Par exemple, vous pouvez sélectionner Succès et erreurs pour la liste des fichiers transférés, mais Erreurs uniquement pour le reste du rapport.
6. Si vous effectuez un transfert vers un compartiment S3 qui utilise la gestion des versions d'objets, maintenez l'option Inclure les versions d'objets Amazon S3 sélectionnée si vous souhaitez que votre rapport inclue la nouvelle version pour chaque objet transféré.
7. Pour le compartiment S3 pour les rapports, choisissez un compartiment S3 dans lequel vous DataSync souhaitez télécharger votre rapport de tâches.

> **Tip**
>
> Si vous envisagez de transférer des données vers un compartiment S3, n'utilisez pas le même compartiment pour votre rapport de tâches si vous désactivez l'option Conserver les fichiers supprimés. Sinon, tous les rapports de tâches précédents DataSync seront supprimés chaque fois que vous exécuterez une tâche, car ces rapports n'existent pas dans votre emplacement source.

8. Pour Dossier, entrez un préfixe à utiliser pour votre rapport de tâches lors du DataSync téléchargement du rapport dans votre compartiment S3 (par exemple,**`reports/`**). Assurez-vous d'inclure le caractère délimiteur approprié à la fin de votre préfixe. Ce caractère est généralement une barre oblique (`/`). Pour plus d'informations, consultez la section Organisation des objets à l'aide de préfixes dans le guide de l'utilisateur Amazon S3.
9. Pour IAM role (Rôle IAM), effectuez l'une des opérations suivantes :
   - Choisissez Autogenerate pour créer DataSync automatiquement un rôle IAM avec les autorisations requises pour accéder au compartiment S3.

     Si un rôle IAM a DataSync déjà été créé pour ce compartiment S3, ce rôle est choisi par défaut.
   - Choisissez un rôle IAM personnalisé que vous avez créé.

     Dans certains cas, il se peut que vous deviez créer le rôle vous-même. Pour de plus amples informations, veuillez consulter DataSync Autoriser le téléchargement de rapports de tâches dans votre compartiment S3.

     > **Important**
     >
     > Si votre compartiment S3 est chiffré à l'aide d'une clé SSE-KMS gérée par le client, la politique de la clé doit inclure le rôle IAM DataSync utilisé pour accéder au compartiment.
     > Pour de plus amples informations, veuillez consulter Accès aux compartiments S3 à l'aide du chiffrement côté serveur.
10. Terminez la création de votre tâche et lancez-la pour commencer à transférer vos données.

Lorsque votre transfert est terminé, vous pouvez consulter votre rapport de tâches.

En utilisant le AWS CLI

1. Copiez la `create-task` commande suivante :

```
aws datasync create-task \
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh \
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-abcdefgh12345678 \
```

```
--task-report-config '{
  "Destination":{
    "S3":{
      "Subdirectory":"reports/",
      "S3BucketArn":"arn:aws:s3:::your-task-reports-bucket",
      "BucketAccessRoleArn":"arn:aws:iam::123456789012:role/bucket-iam-role"
      }
  },
  "OutputType":"STANDARD",
  "ReportLevel":"level-of-detail",
  "ObjectVersionIds":"include-or-not"
}'
```

2. Pour le `--source-location-arn` paramètre, spécifiez l'ARN de l'emplacement source dans votre transfert. Remplacez *`us-east-1`* par le numéro approprié Région AWS, remplacez *`123456789012`* par le Compte AWS numéro approprié et remplacez *`12345678abcdefgh`* par l'ID d'emplacement source approprié.
3. Pour le `--destination-location-arn` paramètre, spécifiez l'ARN de l'emplacement de destination de votre transfert. Remplacez *`us-east-1`* par le numéro approprié Région AWS, remplacez *`123456789012`* par le Compte AWS numéro approprié et remplacez *`abcdefgh12345678`* par le numéro de localisation de destination approprié.
4. Pour le `--task-report-config` paramètre, procédez comme suit :
   - `Subdirectory`— *`reports/`* Remplacez-le par le préfixe de votre compartiment S3 dans lequel vous DataSync souhaitez télécharger vos rapports de tâches. Assurez-vous d'inclure le caractère délimiteur approprié à la fin de votre préfixe. Ce caractère est généralement une barre oblique (`/`). Pour plus d'informations, consultez la section Organisation des objets à l'aide de préfixes dans le guide de l'utilisateur Amazon S3.
   - `S3BucketArn`— Spécifiez l'ARN du compartiment S3 dans lequel vous souhaitez télécharger votre rapport de tâches.

> **Tip**
>
> Si vous envisagez de transférer des données vers un compartiment S3, n'utilisez pas le même compartiment pour votre rapport de tâches si vous désactivez l'option Conserver les fichiers supprimés. Sinon, tous les rapports de tâches précédents DataSync seront supprimés chaque fois que vous exécuterez une tâche, car ces rapports n'existent pas dans votre emplacement source.

- `BucketAccessRoleArn`— Spécifiez le rôle IAM qui permet DataSync de télécharger un rapport de tâches dans votre compartiment S3.

  Pour de plus amples informations, veuillez consulter DataSync Autoriser le téléchargement de rapports de tâches dans votre compartiment S3.

  > **Important**
  >
  > Si votre compartiment S3 est chiffré à l'aide d'une clé SSE-KMS gérée par le client, la politique de la clé doit inclure le rôle IAM DataSync utilisé pour accéder au compartiment.
  > Pour de plus amples informations, veuillez consulter Accès aux compartiments S3 à l'aide du chiffrement côté serveur.

- `OutputType`— Spécifiez `STANDARD` le rapport.

  Pour plus d'informations, consultez la section Rapports de tâches standard Types de rapports de tâches.

- (Facultatif) `ReportLevel` — Spécifiez si vous le souhaitez `ERRORS_ONLY` (par défaut) ou `SUCCESSES_AND_ERRORS` dans votre rapport.
- (Facultatif) `ObjectVersionIds` — Si vous effectuez un transfert vers un compartiment S3 qui utilise le contrôle de version des objets, spécifiez `NONE` si vous ne souhaitez pas inclure la nouvelle version pour chaque objet transféré dans le rapport.

  Par défaut, cette option est définie sur`INCLUDE`.

- (Facultatif) `Overrides` — Personnalisez un aspect particulier de votre rapport. `ReportLevel`

  Par exemple, vous voudrez peut-être voir `SUCCESSES_AND_ERRORS` la liste de ce qui est DataSync supprimé dans votre lieu de destination, mais vous voulez tout `ERRORS_ONLY` le reste. Dans cet exemple, vous devez ajouter l'`Overrides`option suivante au `--task-report-config` paramètre :

  ```
  "Overrides":{
    "Deleted":{
      "ReportLevel":"SUCCESSES_AND_ERRORS"
    }
  }
  ```

Si vous ne l'utilisez pas`Overrides`, l'ensemble de votre rapport utilise `ReportLevel` ce que vous spécifiez.

5. Exécutez la `create-task` commande pour créer votre tâche.

   Vous obtenez une réponse semblable à la suivante qui indique l'ARN de la tâche que vous avez créée. Vous aurez besoin de cet ARN pour exécuter la `start-task-execution` commande.

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
}
```

6. Copiez la `start-task-execution` commande suivante.

```
aws datasync-task-report start-task-execution \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

7. Pour le `--task-arn` paramètre, spécifiez l'ARN de la tâche que vous exécutez. Utilisez l'ARN que vous avez reçu lors de l'exécution de la `create-task` commande.
8. Exécutez la commande `start-task-execution`.

Lorsque votre transfert est terminé, vous pouvez consulter votre rapport de tâches.

Afficher vos rapports DataSync de tâches

DataSync crée des rapports de tâches pour chaque exécution de tâche. Lorsque votre exécution est terminée, vous pouvez trouver les rapports de tâches correspondants dans votre compartiment S3. Les rapports de tâches sont organisés sous des préfixes qui incluent IDs les tâches et leur exécution.

Pour vous aider à localiser les rapports de tâches dans votre compartiment S3, utilisez les exemples suivants :

- Rapport de tâches récapitulatif uniquement — *reports-prefix*/Summary-Reports/*task-id-folder*/*task-execution-id-folder*
- Rapport de tâches standard — *reports-prefix*/Detailed-Reports/*task-id-folder*/*task-execution-id-folder*

Les rapports de tâches étant au format JSON, plusieurs options s'offrent à vous pour les consulter :

- Consultez un rapport à l'aide d'Amazon S3 Select.
- Visualisez les rapports à l'aide de AWS services tels qu' AWS Glue Amazon Athena et Amazon. QuickSight Pour plus d'informations sur la visualisation de vos rapports de tâches, consultez le blog sur le AWS stockage.

Surveillance des transferts de données avec Amazon CloudWatch Logs

Vous pouvez surveiller votre AWS DataSync transfert à l'aide CloudWatch des journaux. Nous vous recommandons de configurer votre tâche de manière à consigner au moins les informations de base (telles que les erreurs de transfert).

DataSync Autoriser le téléchargement de journaux dans un groupe de CloudWatch journaux

Pour configurer la journalisation de votre DataSync tâche, vous avez besoin d'un groupe de CloudWatch journaux autorisé à envoyer des journaux. DataSync Vous configurez cet accès via un rôle AWS Identity and Access Management (IAM). La manière dont cela fonctionne spécifiquement dépend de votre mode de tâche.

Enhanced mode

Avec le mode amélioré, envoie DataSync automatiquement les journaux des tâches à un groupe de journaux nommé`/aws/datasync`. Si ce groupe de journaux n'existe pas dans votre compte Région AWS, DataSync crée le groupe de journaux en votre nom en utilisant un rôle lié à un service IAM lorsque vous créez votre tâche.

Basic mode

Le mode de base permet de configurer un groupe de CloudWatch journaux pour une DataSync tâche de plusieurs manières. Dans la console, vous pouvez créer automatiquement un rôle IAM qui inclut dans la plupart des cas les autorisations nécessaires pour DataSync télécharger des journaux. N'oubliez pas que ce rôle généré automatiquement peut ne pas répondre à vos besoins du point de vue du moindre privilège.

Si vous souhaitez utiliser un groupe de CloudWatch journaux existant ou si vous créez vos tâches par programmation, vous devez créer vous-même le rôle IAM.

L'exemple suivant est une politique IAM qui accorde ces autorisations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DataSyncLogsToCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogStream"
            ],
            "Principal": {
                "Service": "datasync.amazonaws.com"
            },
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": [
                    "arn:aws:datasync:us-east-1:444455556666:task/*"
                    ]
                },
                "StringEquals": {
                "aws:SourceAccount": "444455556666"
                }
            },
            "Resource": "arn:aws:logs:us-east-1:444455556666:log-group:*:*"
        }
    ]
}
```

La politique utilise `Condition` des instructions pour garantir que seules DataSync les tâches du compte spécifié ont accès au groupe de CloudWatch journaux spécifié. Nous vous recommandons d'utiliser les clés contextuelles aws:SourceArnet les clés de contexte de condition aws:SourceAccountglobale dans ces `Condition` instructions afin de vous protéger contre le problème de confusion des adjoints. Pour de plus amples informations, veuillez consulter Prévention du problème de l'adjoint confus entre services.

Pour spécifier la DataSync ou les tâches, *`region`* remplacez-les par le code de région correspondant à l' Région AWS emplacement des tâches (par exemple,`us-west-2`) et remplacez-le par *`account-id`* l' Compte AWS ID du compte contenant les tâches. Pour spécifier le groupe de CloudWatch journaux, remplacez les mêmes valeurs. Vous pouvez également modifier l'`Resource`instruction pour cibler des groupes de journaux spécifiques. Pour plus

d'informations sur l'utilisation de `SourceArn` et`SourceAccount`, consultez la section Clés de condition globales dans le guide de l'utilisateur IAM.

Pour appliquer la stratégie, enregistrez cette instruction de stratégie dans un fichier sur votre ordinateur local. Exécutez ensuite la AWS CLI commande suivante pour appliquer la politique de ressources. Pour utiliser cet exemple de commande, *`full-path-to-policy-file`* remplacez-le par le chemin du fichier contenant votre déclaration de politique.

```
aws logs put-resource-policy --policy-name trust-datasync --policy-document
 file://full-path-to-policy-file
```

> **Note**
>
> Exécutez cette commande en utilisant la même commande Compte AWS et en utilisant l' Région AWS endroit où vous avez activé votre DataSync agent.

Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.

Configuration de la journalisation pour votre DataSync tâche

Nous vous recommandons de configurer au moins un certain niveau de journalisation pour votre DataSync tâche.

Avant de commencer

DataSync a besoin d'une autorisation pour télécharger des journaux dans un groupe de CloudWatch journaux. Pour de plus amples informations, veuillez consulter DataSync Autoriser le téléchargement de journaux dans un groupe de CloudWatch journaux.

Utilisation de la console DataSync

Les instructions suivantes décrivent comment configurer la CloudWatch journalisation lors de la création d'une tâche. Vous pouvez également configurer la journalisation lorsque vous modifiez une tâche.

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches, puis choisissez Créer une tâche.

3. Configurez les emplacements source et de destination de votre tâche.

   Pour de plus amples informations, consultez Où puis-je transférer mes données AWS DataSync ?.

4. Sur la page Configurer les paramètres, choisissez un mode de tâche et toute autre option.

   Certaines des options suivantes pourraient vous intéresser :

   - Spécifiez les données à transférer à l'aide d'un manifeste ou de filtres.
   - Configurez le mode de gestion des métadonnées des fichiers et de vérification de l'intégrité des données.

5. Pour le niveau de journalisation, choisissez l'une des options suivantes :

   - Enregistrez les informations de base telles que les erreurs de transfert : publiez des journaux contenant uniquement des informations de base (telles que les erreurs de transfert).
   - Enregistrez tous les objets et fichiers transférés : publiez des journaux pour tous les fichiers ou objets qui DataSync transfèrent et effectuent des contrôles d'intégrité des données.
   - Ne générez pas de journaux

6. Procédez de l'une des manières suivantes en fonction du mode de tâche que vous utilisez pour créer ou spécifier un groupe de CloudWatch journaux :

   Enhanced mode

   Lorsque vous choisissez Créer une tâche, utilise (ou crée) DataSync automatiquement un groupe de journaux nommé`/aws/datasync`.

   Basic mode

   Pour le groupe de CloudWatch journaux, spécifiez un groupe de journaux autorisé à télécharger des journaux en effectuant l'une des opérations suivantes : DataSync

   - Choisissez Autogenerate pour créer automatiquement un groupe de journaux qui permet DataSync d'y télécharger des journaux.
   - Choisissez un groupe de journaux existant dans votre groupe actuel Région AWS.

     Si vous choisissez un groupe de journaux existant, assurez-vous qu'il DataSync est autorisé à télécharger des journaux dans ce groupe de journaux.

7. Choisissez Créer tâche.

Vous êtes prêt à commencer votre tâche.

En utilisant le AWS CLI

1. Copiez la `create-task` commande suivante :

```
aws datasync create-task \
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --task-mode "ENHANCED-or-BASIC" \
  --name "task-name" \
  --options '{"LogLevel": "log-level"}' \
  --cloudwatch-log-group-arn "arn:aws:logs:us-east-1:account-id:log-group:log-group-name:*"
```

2. Pour`--source-location-arn`, spécifiez l'Amazon Resource Name (ARN) de votre emplacement source.
3. Pour`--destination-location-arn`, spécifiez l'ARN de votre position de destination.

   Si vous transférez plusieurs Régions AWS comptes, assurez-vous que l'ARN inclut l'autre région ou l'autre identifiant de compte.
4. Pour`--task-mode`, spécifiez `ENHANCED` ou`BASIC`.
5. (Recommandé) Pour`--name`, spécifiez un nom mémorisable pour votre tâche.
6. Pour`LogLevel`, spécifiez l'une des options suivantes :
   - `BASIC`— Publiez des journaux contenant uniquement des informations de base (telles que les erreurs de transfert).
   - `TRANSFER`— Publiez des journaux pour tous les fichiers ou objets qui DataSync transfèrent et vérifient l'intégrité des données.
   - `NONE`— Ne générez pas de journaux.
7. Pour `--cloudwatch-log-group-arn`, spécifiez l'ARN d'un groupe de CloudWatch journaux.

> **Important**
>
> Si `--task-mode` c'est le cas`ENHANCED`, il n'est pas nécessaire de spécifier cette option. Pour de plus amples informations, veuillez consulter DataSync Autoriser le téléchargement de journaux dans un groupe de CloudWatch journaux.

8. Exécutez la commande `create-task`.

   Si la commande aboutit, vous obtenez une réponse indiquant l'ARN de la tâche que vous avez créée. Par exemple :

```
{
    "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Vous êtes prêt à commencer votre tâche.

Utilisation de l' DataSync API

Vous pouvez configurer la CloudWatch journalisation de votre tâche en utilisant le `CloudWatchLogGroupArn` paramètre avec l'une des opérations suivantes :

- CreateTask
- UpdateTask

Afficher les journaux des DataSync tâches

Lorsque vous démarrez votre tâche, vous pouvez consulter les journaux d'exécution de la tâche à l'aide de la CloudWatch console ou AWS CLI (entre autres options). Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.

DataSync fournit des journaux structurés en JSON pour les tâches en mode amélioré. Les tâches en mode de base ont des journaux non structurés. Les exemples suivants montrent comment les erreurs de vérification s'affichent dans les journaux en mode amélioré par rapport aux journaux en mode de base.

Enhanced mode log example

```
{
    "Action": "VERIFY",
    "Source": {
        "LocationId": "loc-abcdef01234567890",
        "RelativePath": "directory1/directory2/file1.txt"
    },
    "Destination": {
        "LocationId": "loc-05ab2fdc272204a5f",
        "RelativePath": "directory1/directory2/file1.txt",
        "Metadata": {
            "Type": "Object",
            "ContentSize": 66060288,
            "LastModified": "2024-10-03T20:46:58Z",
            "S3": {
                "SystemMetadata": {
                    "ContentType": "binary/octet-stream",
                    "ETag": "\"1234abcd5678efgh9012ijkl3456mnop\"",
                    "ServerSideEncryption": "AES256"
                },
                "UserMetadata": {
                    "file-mtime": "1602647222/222919600"
                },
                "Tags": {}
            }
        }
    },
    "ErrorCode": "FileNotAtSource",
    "ErrorDetail": "Verification failed due to file being present at the destination
 but not at the source"
}
```

Basic mode log example

```
[NOTICE] Verification failed > /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt   dstMeta: type=R mode=0755 uid=65534
 gid=65534 size=8972938 atime=1728657659/0 mtime=1728657659/0 extAttrsHash=0
[NOTICE]   dstHash: f9c2cca900301d38b0930367d8d587153154af467da0fdcf1bebc0848ec72c0d
```

Journalisation des appels d' AWS DataSync API avec AWS CloudTrail

AWS DataSync est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS utilisateur DataSync. CloudTrail capture tous les appels d'API DataSync sous forme d'événements. Les appels capturés incluent les appels provenant de la DataSync console et les appels de code aux opérations d' DataSync API.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour AWS DataSync. 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 AWS DataSync, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Utilisation des DataSync informations contenues dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS DataSync, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votre Compte AWS, y compris les événements pour AWS DataSync, créez un journal d'activité. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements provenant de tous Régions AWS les utilisateurs de la même AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- 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

Toutes les DataSync actions sont enregistrées par CloudTrail. (Pour plus d'informations, consultez la référence de DataSync l'API.)

Par exemple, les appels aux `ListLocations` opérations `CreateAgentCreateTask`, 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 des informations d'identification root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

Pour plus d'informations, consultez CloudTrail. userIdentity élément du guide de AWS CloudTrail l'utilisateur.

Comprendre les entrées du fichier DataSync journal

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 illustrant l'`CreateTask`opération.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::123456789012:user/user1",
```

```
        "accountId": "123456789012",
        "accessKeyId": "access key",
        "userName": "user1",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-12-13T14:56:46Z"
            }
        },
        "invokedBy": "signin.amazonaws.com"
    },
    "eventTime": "2018-12-13T14:57:02Z",
    "eventSource": "datasync.amazonaws.com",
    "eventName": "CreateTask",
    "awsRegion": "ap-southeast-1",
    "sourceIPAddress": "192.0.2.1",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "cloudWatchLogGroupArn": "arn:aws:logs:ap-southeast-1:123456789012:log-
group:MyLogGroup",
        "name": "MyTask-NTIzMzY1",
        "tags": [],
        "destinationLocationArn": "arn:aws:datasync:ap-
southeast-1:123456789012:location/loc-abcdef01234567890",
        "options": {
            "bytesPerSecond": -1,
            "verifyMode": "POINT_IN_TIME_CONSISTENT",
            "uid": "INT_VALUE",
            "posixPermissions": "PRESERVE",
            "mtime": "PRESERVE",
            "gid": "INT_VALUE",
            "preserveDevices": "NONE",
            "preserveDeletedFiles": "REMOVE",
            "atime": "BEST_EFFORT"
        },
        "sourceLocationArn": "arn:aws:datasync:ap-southeast-1:123456789012:location/
loc-021345abcdef6789"
    },
    "responseElements": {
        "taskArn": "arn:aws:datasync:ap-southeast-1:123456789012:task/
task-1234567890abcdef0"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
```

```
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Surveillance des événements à l'aide d'Amazon EventBridge

EventBridge Les événements Amazon décrivent les modifications apportées aux DataSync ressources. Vous pouvez configurer des règles pour faire correspondre ces événements et les acheminer vers un ou plusieurs flux ou fonctions cibles. Les événements sont générés sur la base du meilleur effort.

DataSync événements de transfert

Les EventBridge événements suivants sont disponibles pour les DataSync transferts.

Agent state changes

Événement	Description
En ligne	L'agent est correctement configuré et prêt à être utilisé. Il s'agit de l'état de fonctionnement normal d'un agent.
Hors connexion	L'agent est hors de contact avec le DataSync service depuis cinq minutes ou plus. Cela peut se produire pour plusieurs raisons. Pour de plus amples informations, consultez Que dois-je faire si mon agent est hors ligne ?.

Location state changes

Événement	Description
Ajouter	DataSync est en train d'ajouter un lieu.
Disponible	L'emplacement est créé et disponible pour être utilisé.

Task state changes

Agent state changes

Événement	Description
Disponible	La tâche a été créée et est prête à démarrer.
En cours d'exécution	La tâche est en cours et fonctionne correctem ent.
Unavailable	La tâche n'est pas configurée correctement et ne peut pas être utilisée. Cet événement peut se produire lorsqu'un agent associé à la tâche se déconnecte.
Mis en file d'attente	Une autre tâche est en cours d'exécution et utilise le même agent. DataSync exécute des tâches en série (premier entré, premier sorti).

Task execution state changes

Événement	Description
Mise en file d'attente	Une autre exécution de tâche est en cours d'exécution et utilise le même DataSync agent. Pour de plus amples informations, veuillez consulter Savoir quand votre tâche est en file d'attente.
Lancement	DataSync initialise l'exécution de la tâche. Ce statut disparaît généralement rapidement, mais peut prendre jusqu'à quelques minutes.

Agent state changes	
Preparing	DataSync détermine les données à transférer. Cette étape peut prendre quelques minutes ou quelques heures selon le nombre de fichiers, d'objets ou de répertoires présents dans les deux emplacements et selon la façon dont vous configurez votre tâche. La préparation peut également ne pas s'appliquer à votre tâche. Pour de plus amples informations, veuillez consulter Comment DataSync prépare votre transfert de données.
Transférer	DataSync effectue le transfert de données proprement dit.
Vérification en cours	DataSync effectue une vérification de l'intégrité des données à la fin du transfert.
Réussite	L'exécution de la tâche a réussi.
Annulation	L'exécution de la tâche est en cours d'annulat ion.
Erreur	L'exécution de la tâche a échoué.

Surveillance AWS DataSync à l'aide d'outils manuels

Vous pouvez suivre vos AWS DataSync transferts depuis la console ou depuis la ligne de commande.

Surveillance de votre transfert à l'aide de la DataSync console

Vous pouvez surveiller votre DataSync transfert à l'aide de la console, qui fournit des indicateurs en temps réel tels que les données transférées, le débit des données et des fichiers, et la compression des données.

Pour surveiller votre transfert à l'aide de la DataSync console

1. Après avoir démarré votre DataSync tâche, choisissez Voir les détails de l'exécution.
2. Consultez les statistiques relatives à votre transfert.

Surveillez votre transfert à l'aide du AWS CLI

Vous pouvez contrôler votre DataSync transfert en utilisant le AWS Command Line Interface (AWS CLI).

Copiez la `describe-task-execution` commande suivante. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws datasync describe-task-execution \
  --task-execution-arn 'arn:aws:datasync:region:account-id:task/task-id/execution/task-execution-id'
```

Cette commande renvoie des informations sur une exécution de tâche, similaires à celles indiquées ci-après.

```
{
    "BytesCompressed": 3500,
    "BytesTransferred": 5000,
    "BytesWritten": 5000,
    "EstimatedBytesToTransfer": 5000,
    "EstimatedFilesToDelete": 10,
    "EstimatedFilesToTransfer": 100,
    "FilesDeleted": 10,
    "FilesSkipped": 0,
    "FilesTransferred": 100,
    "FilesVerified": 100,
    "Result": {
        "ErrorCode": "??????",
        "ErrorDetail": "??????",
        "PrepareDuration": 100,
        "PrepareStatus": "SUCCESS",
        "TransferDuration": 60,
        "TransferStatus": "AVAILABLE",
        "VerifyDuration": 30,
        "VerifyStatus": "SUCCESS"
    },
```

```
    "StartTime": 1532660733.39,
    "Status": "SUCCESS",
    "OverrideOptions": {
        "Atime": "BEST_EFFORT",
        "BytesPerSecond": "1000",
        "Gid": "NONE",
        "Mtime": "PRESERVE",
        "PosixPermissions": "PRESERVE",
        "PreserveDevices": "NONE",
        "PreserveDeletedFiles": "PRESERVE",
        "Uid": "NONE",
        "VerifyMode": "POINT_IN_TIME_CONSISTENT"
    },
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/execution/exec-1234abcd1234abcd1",
    "TaskReportConfig": {
        "Destination": {
            "S3": {
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-datasync-
role",
                "S3BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket/*",
                "Subdirectory": "reports"
            }
        },
        "ObjectVersionIds": "INCLUDE",
        "OutputType": "STANDARD",
        "Overrides": {
            "Deleted": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Skipped": {
                "ReportLevel": "SUCCESSES_AND_ERRORS"
            },
            "Transferred": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Verified": {
                "ReportLevel": "ERRORS_ONLY"
            }
        },
        "ReportLevel": "ERRORS_ONLY"
    }
}
```

- Si l'exécution de la tâche est réussie, la valeur du Statut passe à SUCCESS (RÉUSSITE). Pour plus d'informations sur la signification des éléments de réponse, consultezDescribeTaskExecution.
- Si l'exécution de la tâche échoue, le résultat envoie des codes d'erreur qui peuvent vous aider à résoudre les problèmes. Pour plus d'informations sur les codes d'erreur, consultezTaskExecutionResultDetail.

Surveillance de votre transfert à l'aide de l'`watch`utilitaire

Pour suivre la progression de votre tâche en temps réel à partir de la ligne de commande, vous pouvez utiliser l'`watch`utilitaire Unix standard. Les valeurs de durée d'exécution des tâches sont mesurées en millisecondes.

L'`watch`utilitaire ne reconnaît pas l' DataSync alias. L'exemple suivant montre comment invoquer directement la CLI. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
# pass '-n 1' to update every second and '-d' to highlight differences
        $ watch -n 1 -d \ "aws datasync describe-task-execution --task-execution-arn
 'arn:aws:datasync:region:account-id:task/task-id/execution/task execution-id'"
```

Gestion des AWS DataSync ressources

Découvrez comment gérer vos AWS DataSync ressources, telles que les agents, les sites et les tâches.

Gérer votre DataSync agent

Une fois que vous avez activé un DataSync agent, il AWS gère l'agent pour vous (y compris les mises à jour logicielles). En savoir plus

Tester la connectivité et les ressources système de votre DataSync agent

Bien AWS que vous DataSync gériez votre agent une fois qu'il est déployé et activé, il peut arriver que vous deviez modifier les paramètres de votre agent ou résoudre un problème. En savoir plus

Remplacement de votre DataSync agent

Pour remplacer un DataSync agent, vous devez créer un nouvel agent et mettre à jour tous les sites utilisant l'ancien agent. En savoir plus

Nettoyage des DataSync ressources

Si vous l'avez utilisé DataSync pour un test ou si vous n'avez tout simplement plus besoin de ses ressources, supprimez ces ressources afin qu'elles ne vous soient pas facturées. En savoir plus

Réutilisation de l'infrastructure d'un DataSync agent

Après avoir supprimé une ressource d'agent DataSync, vous pouvez toujours utiliser la machine virtuelle ou l' EC2 instance Amazon de l'agent pour activer un nouvel agent. En savoir plus

Gérer votre AWS DataSync agent

Une fois que vous avez activé un AWS DataSync agent, il AWS gère l'appliance de machine virtuelle (VM) pour vous.

Mises à jour logicielles des agents

AWS met automatiquement à jour le logiciel de votre agent, y compris le système d'exploitation sous-jacent et les DataSync progiciels associés.

DataSync met à jour votre agent uniquement lorsqu'il est inactif. Par exemple, votre agent ne sera pas mis à jour tant que votre transfert ne sera pas terminé.

L'agent peut se déconnecter brièvement après les mises à jour. Cela peut se produire, par exemple, peu de temps après l'activation de l'agent lors de AWS sa mise à jour.

> **Important**
>
> - DataSync applique automatiquement et régulièrement des correctifs aux agents pour garantir leur sécurité et leur stabilité. DataSync les agents utilisent Amazon Linux 2 comme système d'exploitation de base. Vous pouvez consulter l'état actuel des problèmes de vulnérabilité et d'exposition courants (CVE) détectés sur le Amazon Linux Security Center. Les correctifs CVE sont automatiquement appliqués dans les 30 jours suivant leur date de publication, comme indiqué sur le Amazon Linux Security Center. L'application de correctifs se produit tant que votre agent est en ligne et n'exécute pas activement une tâche.
> - DataSync ne prend pas en charge la mise à jour manuelle d'un EC2 agent Amazon avec les directives cloud-init. Si vous mettez à jour un agent de cette façon, vous pouvez rencontrer des problèmes d' DataSync interopérabilité car vous ne pouvez pas activer ou utiliser l'agent.

Statuts des agents

Le tableau suivant décrit le statut des DataSync agents.

Statut de l'agent	Signification
En ligne	L'agent est correctement configuré et prêt à être utilisé. Il s'agit de l'état de fonctionnement normal d'un agent.
Hors connexion	L'agent est hors de contact avec le DataSync service depuis cinq

Statut de l'agent	Signification
	minutes ou plus. Cela peut se produire pour plusieurs raisons. Pour plus d'informations, consultez Que dois-je faire si mon agent est hors ligne ?.

Résolution des problèmes liés à votre agent

Bien AWS que vous gériez l' DataSync agent pour vous, il peut arriver que vous deviez à nouveau travailler directement avec lui. Par exemple, si votre agent se déconnecte ou perd sa connexion à votre système de stockage sur site, vous pouvez essayer de résoudre ces problèmes dans la console locale de l'agent.

Pour plus d'informations, consultez la section relative DataSync aux agents de dépannage.

Effectuer la maintenance de votre agent

Bien AWS que vous AWS DataSync gériez votre agent une fois qu'il est déployé et activé, il peut arriver que vous deviez modifier les paramètres de votre agent ou résoudre un problème. Voici quelques exemples des raisons pour lesquelles vous pourriez travailler avec votre agent via sa console locale :

- Attribuez manuellement une adresse IP à l'agent.
- Vérifiez les ressources système de votre agent.

> **Important**
>
> Il n'est pas nécessaire d'utiliser la console locale de l'agent pour bénéficier des DataSync fonctionnalités standard.

Accès à la console locale de votre agent

La manière dont vous accédez à la console locale dépend du type d'agent que vous utilisez.

Accès à la console locale (VMware ESXiLinux KVM ou Microsoft Hyper-V)

Pour des raisons de sécurité, vous ne pouvez pas vous connecter à distance à la console locale de la machine virtuelle (VM) de l' DataSync agent.

- Si c'est la première fois que vous utilisez la console locale, connectez-vous avec les informations d'identification par défaut. Par défaut, le nom d'utilisateur est **`admin`** et le mot de passe est **`password`**. Il vous sera demandé de modifier le mot de passe lors de votre première connexion.

> **Note**
>
> Après avoir configuré votre mot de passe initial, vous pouvez le modifier à tout moment. Dans le menu principal de la console, entrez le numéro à côté de Command Prompt, puis exécutez la `passwd` commande pour modifier le mot de passe.

Accès à la console locale (Amazon EC2)

Pour vous connecter à la console locale d'un EC2 agent Amazon, vous devez utiliser SSH.

Avant de commencer : assurez-vous que le groupe de sécurité de votre EC2 instance autorise l'accès via SSH (port TCP 22).

1. Ouvrez un terminal et copiez la `ssh` commande suivante :

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

   - Pour*`/path/key-pair-name`*, spécifiez le chemin et le nom de fichier (`.pem`) de la clé privée requise pour vous connecter à votre instance.
   - Pour *`instance-user-name`*, spécifiez `admin`.
   - Pour*`instance-public-ip-address`*, spécifiez l'adresse IP publique de votre instance.
2. Exécutez la `ssh` commande pour vous connecter à l'instance.

Une fois connecté, le menu principal de la console locale de l'agent s'affiche.

Configuration des paramètres DHCP, DNS et IP de votre agent

La configuration du réseau par défaut pour l'agent est le protocole DHCP (Dynamic Host Configuration Protocol). Avec le protocole DHCP, votre agent reçoit automatiquement une adresse IP. Dans certains cas, vous devrez peut-être affecter manuellement l'IP de votre agent comme adresse IP statique, comme décrit ci-après.

1. Connectez-vous à la console locale de votre agent.
2. Dans le menu principal AWS DataSync Activation - Configuration, entrez **1** pour commencer à configurer votre réseau.
3. Choisissez l'une des options suivantes dans le menu Network Configuration (Configuration du réseau).

Pour	Faites ceci

Collecter des informations sur votre carte réseau	Saisissez **1**.
	
	La liste des noms d'adaptateurs s'affiche et vous êtes invité à saisir un nom d'adaptateur, par exemple,. **eth0** Si l'adaptateur que vous spécifiez est en cours d'utilisation, les informati ons réseau relatives à cet adaptateur sont affichées, comme dans l'exemple suivant :
	
	`IP Preference: IPv4`
	`MAC address: 52:54:12:a4:f7:7d`
	
	`IPv4 address: 192.168.100.482`
	`Netmask: 255.255.255.0`
	`Gateway: 192.168.100.4`
	`DHCP enabled: Yes`
	
	`IPv6 address: abcd:4444:e5ee:fd0`
	`0::4daf`
	`Prefix length: 128`
	`Gateway: fe80::5021:ff:ff88:4acd`
	`DHCPV6 enabled: Yes`
	
	`DNS: abcd:4444:e5ee:fd00::1`

Pour	Faites ceci
	`DNS: 192.168.100.4` Vous utilisez le même nom d'adaptateur lorsque vous configurez une adresse IP statique (option 3) que lorsque vous définisse z la carte de routage par défaut de votre agent (option 5).
Configurer DHCP	Saisissez **2**. Choisissez la version IP à utiliser, puis configurez l'interface réseau pour qu'elle utilise le protocole DHCP.
Configurer une adresse IP statique pour votre agent	Saisissez **3**. Vous êtes invité à choisir le protocole IP à utiliser IPv4 IPv6, ou les deux. Vous êtes ensuite invité à saisir le nom de l'adaptateur réseau pour configurer une adresse IP statique. **Important** Si votre agent a déjà été activé, vous devez l'arrêter et le redémarrer depuis la DataSync console pour que les paramètres prennent effet.

Pour	Faites ceci
Réinitialiser la configuration du réseau de votre agent sur DHCP	Saisissez **4**. Choisissez la version IP à réinitialiser sur DHCP. Toutes les interfaces réseau de la version IP choisie sont configurées pour utiliser le protocole DHCP. **Important** Si votre agent a déjà été activé, vous devez l'arrêter et le redémarrer depuis la DataSync console pour que les paramètres prennent effet.
Définir la carte de routage par défaut de l'agent	Saisissez **5**. Les adaptateurs disponibles pour votre agent sont affichés, et vous êtes invité à choisir l'un des adaptateurs, par exemple,. **`eth0`**
Modifiez la configuration du système de noms de domaine (DNS) de votre agent	Saisissez **6**. Les cartes disponibles sur les serveurs DNS principaux et secondaires s'affichent. Vous êtes invité à indiquer la nouvelle adresse IP.

Pour	Faites ceci
Afficher la configuration DNS de votre agent	Saisissez **7**. Les cartes disponibles sur les serveurs DNS principaux et secondaires s'affichent. **Note** Pour certaines versions de l' VMware hyperviseur, vous pouvez modifier la configuration de l'adaptateur dans ce menu.
Consultation des tables de routage	Saisissez **8**. Choisissez la version IP (ou IPv4 IPv6 les deux) pour afficher la table de routage par défaut de votre agent.
Afficher la version IP de votre agent pour les transferts de données	Saisissez **9**. Le paramètre de version IP de l'agent pour les transferts de données s'affiche`IPv4`, soit`IPv6`,`IPv4 (auto)`, soit`IPv6 (auto)`.

Pour	Faites ceci
Modifiez le protocole IP de votre agent pour les transferts de données	Saisissez **10**. Les paramètres de version IP disponibles pour les transferts de données s'affichent. Vous pouvez choisir entre `IPv4``IPv6`,`IPv4 (auto)`, ou`IPv6 (auto)`. Pour plus d'informations sur le réglage de la version IP de votre agent pour les transferts de données, consultezthe section called "IPv6 soutien".

Vérification des ressources système de votre agent

Lorsque vous vous connectez à la console de votre agent, les cœurs de processeur virtuels, la taille du volume racine et la RAM sont automatiquement vérifiés. S'il y a des erreurs ou des avertissements, ils sont signalés sur l'écran du menu de la console par une bannière qui fournit des détails sur ces erreurs ou avertissements.

S'il n'y a pas d'erreur ou d'avertissement au démarrage de la console, le menu affiche du texte blanc. L'option Afficher la vérification des ressources du système s'affiche`(0 Errors)`.

En cas d'erreurs ou d'avertissements, le menu de la console affiche le nombre d'erreurs et d'avertissements, respectivement en rouge et en jaune, dans une bannière en haut du menu. Par exemple, `(1 ERROR, 1 WARNING)`.

Pour vérifier les ressources système de votre agent

1. Connectez-vous à la console locale de votre agent.
2. Dans le menu principal AWS DataSync Activation - Configuration, entrez **4** pour afficher les résultats de la vérification des ressources du système.

   La console affiche un message [OK], [Avertissement] ou [ECHEC] pour chaque ressource, comme décrit dans le tableau suivant.

   Pour les EC2 instances Amazon, le contrôle des ressources système vérifie que le type d'instance est l'une des instances recommandées pour une utilisation avec DataSync. Si le type d'instance correspond à cette liste, un seul résultat est affiché en vert, comme suit.

```
[ OK ] Instance Type Check
```

Si l' EC2 instance Amazon ne figure pas sur la liste recommandée, le contrôle des ressources système vérifie les ressources suivantes.

- Vérification des cœurs du processeur : au moins quatre cœurs sont nécessaires.
- Contrôle de la taille du disque : un minimum de 80 Go d'espace disque disponible est requis.
- Vérification de la RAM :
  - 32 Go de RAM affectés à l'instance pour exécuter des tâches avec un maximum de 20 millions de fichiers, d'objets ou de répertoires.
  - 64 Go de RAM affectés à l'instance pour exécuter des tâches avec plus de 20 millions de fichiers, d'objets ou de répertoires.
- Vérification des indicateurs du processeur : le processeur de la machine virtuelle de l'agent doit avoir soit des indicateurs, SSSE3 soit des indicateurs de jeu SSE4 d'instructions.

Si l' EC2 instance Amazon ne figure pas dans la liste des instances recommandées pour DataSync, mais qu'elle dispose de ressources suffisantes, le résultat de la vérification des ressources du système affiche quatre résultats, tous en texte vert.

Les mêmes ressources sont vérifiées pour les agents déployés dans Hyper-V, la machine virtuelle basée sur le noyau Linux (KVM) et. VMware VMs

VMware les agents sont également vérifiés pour les versions prises en charge ; les versions non prises en charge provoquent une erreur de bannière rouge. Les versions prises en charge incluent VMware les versions 6.5 et 6.7.

Synchronisation de l'heure de votre agent VMware

Si vous utilisez un VMware agent, vous pouvez consulter ou modifier la configuration de votre serveur NTP (Network Time Protocol) et synchroniser l'heure de l'agent avec l'hôte de votre VMware hyperviseur.

1. Connectez-vous à la console locale de votre agent.
2. Dans le menu principal AWS DataSync Activation - Configuration, entrez**5**.
3. Dans le menu Gestion du temps du système, effectuez l'une des opérations suivantes :

Pour	Faites ceci
Afficher et synchroniser l'heure de votre machine virtuelle avec l'heure du serveur NTP	Saisissez **1**. L'heure actuelle de votre agent s'affiche. Votre agent détermine le décalage horaire entre votre agent et le serveur NTP et vous invite à synchroniser les heures. Dans certaines situations, le temps de travail d'un agent peut varier. Par exemple, il se peut qu'il y ait une panne réseau prolongée et que l'hôte et l'agent de votre hyperviseur ne soient pas informés de l'heure. L'heure de votre agent est donc différente de l'heure réelle. Lorsqu'il y a une telle dérive temporelle, un écart se produit entre les heures indiquées auxquelle s les opérations (telles que les instantanés se produisent) et les heures réelles auxquelles les opérations se produisent.
Modifier la configuration du serveur NTP	Saisissez **2**. Vous êtes invité à fournir une configuration de serveur NTP.
Afficher la configuration du serveur NTP	Saisissez **3**. La configuration de votre serveur NTP s'affiche .

Exécution de commandes liées à la maintenance pour votre agent

Dans la console locale de votre DataSync agent, vous pouvez effectuer certaines tâches de maintenance et diagnostiquer des problèmes avec votre agent.

Pour exécuter une commande de configuration ou de diagnostic dans la console locale de votre agent

1. Connectez-vous à la console locale de votre agent.
2. Dans le menu principal AWS DataSync Activation - Configuration, entrez **5** (ou **6** pour une VMware machine virtuelle) l'invite de commande.
3. Utilisez les commandes suivantes pour effectuer les tâches suivantes avec votre agent.

Command	Description
`dig`	Consultez les informations DNS relatives à l'hôte.
`diskclean`	Effectuez le nettoyage du disque.
`exit`	Retournez au menu de configuration de la console.
`h`	Afficher la liste des commandes disponibles.
`ifconfig`	Affichez ou configurez les interfaces réseau.
`ip`	Affichez ou configurez le routage, les appareils et les tunnels.
`iptables`	Configurez et gérez le filtrage des IPv4 paquets et le NAT.
`ip6tables`	Configurez et gérez le filtrage des IPv6 paquets et le NAT.
`ncport`	Testez la connectivité à un port TCP réseau spécifique.
`nping`	Obtenez des informations pour résoudre les problèmes de réseau.
`passwd`	Changez le mot de passe utilisateur.

Command	Description
`save-iptables`	Enregistrez définitivement les règles de pare-feu des IPv4 tables.
`save-ip6tables`	Enregistrez définitivement les règles de pare-feu des IPv6 tables.
`save-routing-table`	Enregistrez une entrée de table de routage récemment ajoutée.
`sslcheck`	Vérifiez si un certificat SSL est valide.
`tcptraceroute`	Collectez la `traceroute` sortie sur le trafic TCP vers une destination.

4. Suivez les instructions à l'écran.

Remplacement de votre AWS DataSync agent

Pour remplacer un AWS DataSync agent, vous devez créer un nouvel agent et mettre à jour tous les sites de transfert utilisant l'ancien agent.

Création d'un nouvel agent

Pour créer votre nouvel DataSync agent, suivez le même processus que lorsque vous avez créé votre ancien agent :

1. Déployez un agent dans votre environnement de stockage.
2. Choisissez un point de terminaison de service avec lequel l'agent communique AWS.
3. Configurez votre réseau afin que l'agent puisse communiquer avec votre système de stockage et AWS.
4. Activez votre agent.
5. Une fois activé, notez le nom de ressource Amazon (ARN) de l'agent.

   Vous avez besoin de cet ARN lorsque vous mettez à jour votre DataSync position pour utiliser le nouvel agent.

Mettre à jour votre position avec le nouvel agent

Une fois que vous avez créé un nouvel agent, vous pouvez mettre à jour un DataSync emplacement existant pour utiliser cet agent. Dans la plupart des cas, vous devez également saisir à nouveau les informations d'accès pour mettre à jour l'emplacement. Cela est dû au fait que DataSync les informations de localisation sont stockées de manière à ce que seul votre agent puisse les utiliser.

Utilisation de la DataSync console

Les instructions suivantes décrivent comment mettre à jour les emplacements avec un nouvel agent à l'aide de la DataSync console.

NFS

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.
3. Choisissez l'emplacement que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Pour les agents, choisissez votre nouvel agent.

   Vous pouvez choisir plusieurs agents si vous remplacez plusieurs agents par point de vente.
5. Sélectionnez Enregistrer les modifications.

SMB

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.
3. Choisissez l'emplacement que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Pour les agents, choisissez votre nouvel agent.

   Vous pouvez choisir plusieurs agents si vous remplacez plusieurs agents par point de vente.
5. Dans Mot de passe, entrez le mot de passe de l'utilisateur qui peut monter votre serveur de fichiers SMB et qui est autorisé à accéder aux fichiers et dossiers concernés par votre transfert.
6. Sélectionnez Enregistrer les modifications.

HDFS

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.
3. Choisissez l'emplacement que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Pour les agents, choisissez votre nouvel agent.

   Vous pouvez choisir plusieurs agents si vous remplacez plusieurs agents par point de vente.
5. Si vous utilisez l'authentification Kerberos, téléchargez votre fichier Keytab et votre fichier de configuration Kerberos.
6. Sélectionnez Enregistrer les modifications.

Object storage

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.
3. Choisissez l'emplacement que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Pour les agents, choisissez votre nouvel agent.

   Vous pouvez choisir plusieurs agents si vous remplacez plusieurs agents par point de vente.
5. Si votre emplacement nécessite des informations d'identification, entrez la clé secrète qui permet d'accéder DataSync à votre compartiment de stockage d'objets.
6. Sélectionnez Enregistrer les modifications.

Azure Blob Storage

Procédez comme suit pour mettre à jour votre Microsoft Azure Blob Storage lieu :

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.
3. Choisissez l'emplacement que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Pour les agents, choisissez votre nouvel agent.

Vous pouvez choisir plusieurs agents si vous remplacez plusieurs agents par point de vente.

5. Pour le jeton SAS, entrez le jeton de signature d'accès partagé (SAS) qui permet DataSync d'accéder à votre stockage blob.
6. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

Les instructions suivantes décrivent comment mettre à jour les emplacements avec un nouvel agent à l'aide du AWS CLI. (Vous pouvez également le faire en utilisant l'DataSync API.)

NFS

1. Copiez la update-location-nfscommande suivante :

```
aws datasync update-location-nfs \
  --location-arn datasync-nfs-location-arn \
  --on-prem-config AgentArns=new-datasync-agent-arn
```

2. Pour le `--location-arn` paramètre, spécifiez l'ARN de l'emplacement NFS que vous mettez à jour.
3. Pour l'`AgentArns`option du `--on-prem-config` paramètre, spécifiez l'ARN de votre nouvel agent.

   Vous pouvez spécifier plusieurs ARN si vous remplacez plusieurs agents pour un même emplacement.
4. Exécutez la `update-location-nfs` commande pour mettre à jour l'emplacement.

SMB

1. Copiez la update-location-smbcommande suivante :

```
aws datasync update-location-smb \
  --location-arn datasync-smb-location-arn \
  --agent-arns new-datasync-agent-arn \
  --password smb-file-server-password
```

2. Pour le `--location-arn` paramètre, spécifiez l'ARN de l'emplacement SMB que vous mettez à jour.

3. Pour le `--agent-arns` paramètre, spécifiez l'ARN de votre nouvel agent.

   Vous pouvez spécifier plusieurs ARN si vous remplacez plusieurs agents pour un même emplacement.

4. Pour le `--password` paramètre, spécifiez le mot de passe de l'utilisateur qui peut monter votre serveur de fichiers SMB et qui est autorisé à accéder aux fichiers et dossiers concernés par votre transfert.

5. Exécutez la `update-location-smb` commande pour mettre à jour l'emplacement.

HDFS

1. Copiez la update-location-hdfscommande suivante :

```
aws datasync update-location-hdfs \
  --location-arn datasync-hdfs-location-arn \
  --agent-arns new-datasync-agent-arn \
  --kerberos-keytab keytab-file \
  --kerberos-krb5-conf krb5-conf-file
```

2. Pour le `--location-arn` paramètre, spécifiez l'ARN de l'emplacement HDFS que vous mettez à jour.

3. Pour le `--agent-arns` paramètre, spécifiez l'ARN de votre nouvel agent.

   Vous pouvez spécifier plusieurs ARN si vous remplacez plusieurs agents pour un même emplacement.

4. Si vous utilisez l'authentification Kerberos, incluez les paramètres `--kerberos-keytab` et `--kerberos-krb5-conf` :

   - Pour le `--kerberos-keytab` paramètre, spécifiez la table des clés Kerberos (keytab) qui contient les mappages entre les clés principales Kerberos définies et les clés chiffrées.

     Vous pouvez spécifier le fichier keytab en fournissant l'adresse du fichier.

   - Pour le `--kerberos-krb5-conf` paramètre, spécifiez le fichier contenant la configuration de votre domaine Kerberos.

     Vous pouvez spécifier le `krb5.conf` fichier en fournissant son adresse.

Si vous utilisez l'authentification simple, il n'est pas nécessaire d'inclure ces paramètres liés à Kerberos dans votre commande.

5. Exécutez la `update-location-hdfs` commande pour mettre à jour l'emplacement.

Object storage

1. Copiez la update-location-object-storagecommande suivante :

```
aws datasync update-location-object-storage \
  --location-arn datasync-object-storage-location-arn \
  --agent-arns new-datasync-agent-arn \
  --secret-key bucket-secret-key
```

2. Pour le `--location-arn` paramètre, spécifiez l'ARN de l'emplacement de stockage d'objets que vous mettez à jour.
3. Pour le `--agent-arns` paramètre, spécifiez l'ARN de votre nouvel agent.

   Vous pouvez spécifier plusieurs ARN si vous remplacez plusieurs agents pour un même emplacement.
4. Procédez comme suit selon que votre emplacement de stockage d'objets nécessite des informations d'identification d'accès :

   - Si votre emplacement nécessite des informations d'identification : pour le `--secret-key` paramètre, spécifiez la clé secrète qui permet d'accéder DataSync à votre bucket de stockage d'objets.
   - Si votre position nécessite des informations d'identification, spécifiez des chaînes vides pour les `--secret-key` paramètres `--access-key` et. Voici un exemple de commande :

```
aws datasync update-location-object-storage \
  --location-arn arn:aws:datasync:us-east-2:111122223333:location/
loc-abcdef01234567890 \
  --agent-arns arn:aws:datasync:us-east-2:111122223333:agent/
agent-1234567890abcdef0 \
  --access-key "" \
  --secret-key ""
```

5. Exécutez la `update-location-object-storage` commande pour mettre à jour l'emplacement.

Azure Blob Storage

1. Copiez la update-location-azure-blobcommande suivante :

```
aws datasync update-location-azure-blob \
  --location-arn datasync-azure-blob-storage-location-arn \
  --agent-arns new-datasync-agent-arn \
  --sas-configuration '{
      "Token": "sas-token-for-azure-blob-storage"
    }'
```

2. Pour le `--location-arn` paramètre, spécifiez l'ARN du Azure Blob Storage emplacement que vous êtes en train de mettre à jour.
3. Pour le `--agent-arns` paramètre, spécifiez l'ARN de votre nouvel agent.

   Vous pouvez spécifier plusieurs ARN si vous remplacez plusieurs agents pour un même emplacement.
4. Pour l'`Token`option du `--sas-configuration` paramètre, spécifiez le jeton SAS qui permet d'accéder DataSync à votre stockage blob.
5. Exécutez la `update-location-azure-blob` commande pour mettre à jour l'emplacement.

Étapes suivantes

1. Supprimez votre ancien agent. Si vous avez des DataSync tâches en cours d'exécution à l'aide de cet agent, attendez qu'elles soient terminées avant de les supprimer.
2. Si vous devez remplacer les agents de plusieurs sites, répétez les étapes précédentes.
3. Lorsque vous avez terminé, vous pouvez reprendre l'exécution de vos tâches.

> **Note**
>
> Remplacement d'agents par des tâches planifiées : si vous remplacez un agent pour une tâche planifiée, vous devez démarrer cette tâche manuellement si le nouvel agent utilise un type de point de terminaison de service différent de celui de votre ancien agent. Si

vous n'exécutez pas la tâche manuellement avant sa prochaine exécution planifiée, elle échoue.
Par exemple, si votre ancien agent utilisait un point de terminaison de service public, mais que le nouvel agent utilise un point de terminaison VPC, lancez cette tâche manuellement à l'aide de la console ou `StartTaskExecution` de l'opération. Ensuite, votre tâche reprendra son exécution selon son calendrier.

Filtrer AWS DataSync les ressources

Vous pouvez filtrer vos AWS DataSync emplacements et vos tâches à l'aide des opérations `ListTasks` d'API `ListLocations` et du AWS CLI. Par exemple, récupérez la liste de vos tâches les plus récentes.

Paramètres de filtrage

Vous pouvez utiliser les filtres d'API pour affiner la liste des ressources renvoyées par `ListTasks` et`ListLocations`. Par exemple, pour récupérer tous vos sites Amazon S3, vous pouvez utiliser `ListLocations` avec le nom du filtre `LocationType` *`S3`*et `Operator` *`Equals`*.

Pour filtrer les résultats de l'API, vous devez spécifier un nom, un opérateur et une valeur de filtre.

- `Name`— Le nom du filtre utilisé. Chaque appel d'API prend en charge une liste de filtres disponibles pour celui-ci (par exemple, `LocationType` pour`ListLocations`).
- `Values`— Les valeurs que vous souhaitez filtrer. Par exemple, vous souhaiterez peut-être afficher uniquement les emplacements Amazon S3.
- `Operator`— L'opérateur utilisé pour comparer les valeurs des filtres (par exemple, `Equals` ou`Contains`).

Le tableau suivant répertorie les opérateurs disponibles.

Opérateur	Types de clé
`Equals`	Chaîne, numéro
`NotEquals`	Chaîne, numéro

Opérateur	Types de clé
`LessThan`	Nombre
`LessThanOrEqual`	Nombre
`GreaterThan`	Nombre
`GreaterThanOrEqual`	Nombre
`In`	Chaîne
`Contains`	Chaîne
`NotContains`	Chaîne
`BeginsWith`	Chaîne

Filtrer par localisation

`ListLocations`prend en charge les noms de filtres suivants :

- `LocationType`— Filtres selon le type de localisation :
  - `SMB`
  - `NFS`
  - `HDFS`
  - `OBJECT_STORAGE`
  - `S3`
  - `OUTPOST_S3`
  - `FSX_WINDOWS`
  - `FSX_LUSTRE`
  - `FSX_OPENZFS_NFS`
  - `FSX_ONTAP_NFS`
  - `FSX_ONTAP_SMB`

- `LocationUri`— Filtres sur l'identifiant de ressource uniforme (URI) attribué à l'emplacement, tel que renvoyé par l'appel d'`DescribeLocation`*API (par exemple, `s3://`*`bucket-name`*`/`*`your-prefix`* pour les sites Amazon S3).
- `CreationTime`— Filtre en fonction de l'heure à laquelle le lieu a été créé. Le format d'entrée est `yyyy-MM-dd:mm:ss` en temps universel coordonné (UTC).

L' AWS CLI exemple suivant répertorie tous les emplacements de type Amazon S3 dont l'URI commence par la chaîne `"s3://amzn-s3-demo-bucket"` et qui ont été créés le 15/12/2019 à 17:15:20 UTC ou après cette date.

```
aws datasync list-locations \
    --filters [{Name=LocationType, Values=["S3"], Operator=Equals},
 {Name=LocationUri, Values=["s3://amzn-s3-demo-bucket"], Operator=BeginsWith},
 {Name=CreationTime,Values=["2019-12-15 17:15:20"],Operator=GreaterThanOrEqual}]
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit.

```
{
    "Locations": [
        {
            "LocationArn": "arn:aws:datasync:us-east-1:111122223333:location/
loc-333333333abcdef0",
            "LocationUri": "s3://amzn-s3-demo-bucket1/"
        },
        {
            "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-987654321abcdef0",
            "LocationUri": "s3://amzn-s3-demo-bucket2/"
        }
    ]
}
```

Filtrer par tâche

`ListTasks`prend en charge les noms de filtres suivants.

- `LocationId`— Filtre à la fois les emplacements source et de destination en fonction des valeurs Amazon Resource Name (ARN).

- `CreationTime`— Filtre en fonction de l'heure à laquelle la tâche a été créée. Le format d'entrée est `yyyy-MM-dd:mm:ss` en UTC.

L' AWS CLI exemple suivant montre la syntaxe lors du filtrage activé`LocationId`.

```
aws datasync list-tasks \
    --filters Name=LocationId,Values=arn:aws:datasync:us-east-1:your-account-id:location/your-location-id,Operator=Contains
```

Le résultat de cette commande ressemble à ce qui suit.

```
{
    "Tasks": [
        {
            "TaskArn": "arn:aws:datasync:us-east-1:your-account-id:task/your-task-id",
            "Status": "AVAILABLE",
            "Name": "amzn-s3-demo-bucket"
        }
    ]
}
```

Nettoyer vos AWS DataSync ressources

Si vous les avez utilisées AWS DataSync pour un test ou si vous n'avez pas besoin des AWS ressources que vous avez créées, supprimez-les afin de ne pas être facturées pour des ressources que vous n'avez pas l'intention d'utiliser.

> **Note**
>
> Si vous désactivez DataSync des ressources dans une région optionnelle, elles ne sont pas automatiquement supprimées. Les ressources sont toujours disponibles si vous réactivez cette région.

Supprimer un DataSync agent

Lorsque vous supprimez un agent de AWS DataSync, la ressource d'agent n'est plus associée à votre compte Compte AWS et ne peut pas être annulée.

N'oubliez pas que la suppression d'un agent DataSync n'entraîne pas la suppression de sa machine virtuelle (VM) ou de son EC2 instance Amazon de votre environnement de stockage. Vous pouvez supprimer la machine virtuelle ou l'instance ou la réutiliser pour activer un nouvel agent.

Prérequis

Ne supprimez pas un agent tant que vous n'avez pas mis à jour ou supprimé les DataSync ressources qui en dépendent. Si vous remplacez un agent, mettez à jour vos lieux de transfert avec le nouvel agent. Si vous ne remplacez pas un agent, supprimez d'abord les tâches de transfert et les sites utilisant cet agent.

Supprimer l'agent

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, sélectionnez Agents.
3. Choisissez l'agent que vous souhaitez supprimer.
4. Choisissez Supprimer, entrez **`delete`** dans la zone de texte qui apparaît, puis choisissez Supprimer.
5. Si vous ne prévoyez pas de réutiliser l'infrastructure de l'agent pour d'autres DataSync activités, supprimez la machine virtuelle ou l' EC2 instance Amazon de l'agent pour la retirer de votre environnement de stockage.

Réutilisation de l'infrastructure d'un DataSync agent

Vous pouvez supprimer une ressource d'agent DataSync et continuer à utiliser la machine virtuelle ou l' EC2 instance Amazon sous-jacente de l'agent pour activer un nouvel agent.

Pour réutiliser l'infrastructure d'un agent

1. Testez la connexion de l'agent à AWS. Si les tests réseau réussissent, passez à l'étape suivante.

   Les tests de réseau doivent réussir avant que vous puissiez passer à l'étape suivante.
2. Supprimez la ressource de l'agent DataSync , mais ne supprimez pas la machine virtuelle ou l' EC2 instance Amazon de l'agent.
3. Répétez l'étape 1 pour tester à AWS nouveau la connexion de l'agent à. Si les tests réseau réussissent, passez à l'étape suivante.

4. Environ trois minutes après avoir supprimé la ressource de l'agent DataSync, vérifiez si le port 80 est ouvert sur la machine virtuelle de l'agent ou sur l' EC2 instance Amazon. Si c'est le cas, passez à l'étape suivante.
5. Activez un nouvel agent avec la machine virtuelle ou l' EC2 instance Amazon existante.

   Vous pouvez activer le nouvel agent dans un autre Région AWS type de point de terminaison de service. Compte AWS Si vous utilisez un autre type de point de terminaison de service, vous devez ajuster la configuration de votre réseau.

Supprimer un DataSync emplacement

Il est recommandé de supprimer les AWS DataSync emplacements dont vous n'avez plus besoin.

Pour supprimer un emplacement à l'aide de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.
3. Choisissez l'emplacement que vous souhaitez supprimer.
4. Sélectionnez Delete (Supprimer). Confirmez la suppression en entrant**`delete`**, puis en choisissant Supprimer.

Supprimer une DataSync tâche

Si vous n'avez plus besoin d'une AWS DataSync tâche, vous pouvez la supprimer ainsi que les AWS ressources associées.

Prérequis

Lorsque vous exécutez une tâche, crée et gère DataSync automatiquement les interfaces réseau pour le trafic de transfert de données. Lorsque vous supprimez une tâche, vous supprimez également les interfaces réseau associées, à condition que vous disposiez des autorisations suivantes :

- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`

Ces autorisations sont disponibles dans la politique AWS géréeAWSDataSyncFullAccess. Pour de plus amples informations, veuillez consulter AWS politiques gérées pour AWS DataSync.

Supprimer la tâche

Une fois que vous avez supprimé une tâche, vous ne pouvez pas la restaurer.

Utilisation de la DataSync console

1. Ouvrez la AWS DataSync console à l'adresse https://console.aws.amazon.com/datasync/.
2. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Tâches.
3. Sélectionnez la tâche que vous souhaitez supprimer.
4. Choisissez Actions, puis Delete (Supprimer).
5. Dans la boîte de dialogue , , choisissez Supprimer.

En utilisant le AWS CLI

1. Copiez la `delete-task` commande suivante :

```
aws datasync delete-task \
      --task-arn "task-to-delete"
```

2. Pour le `--task-arn` paramètre, spécifiez le nom de ressource Amazon (ARN) de la tâche que vous supprimez (par exemple,`arn:aws:datasync:us-east-2:123456789012:task/task-012345678abcd0123`).
3. Exécutez la commande `delete-task`.

Sécurité dans AWS DataSync

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture 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 AWS cloud. 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 de plus amples informations sur les programmes de conformité qui s'appliquent à AWS DataSync, veuillez consulter Services AWS concernés par le 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 la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation DataSync. Les rubriques suivantes expliquent comment procéder à la configuration DataSync pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos DataSync ressources.

Rubriques

- Protection des données dans AWS DataSync
- Gestion des identités et des accès dans AWS DataSync
- Validation de conformité pour AWS DataSync
- Résilience dans AWS DataSync
- Sécurité de l'infrastructure dans AWS DataSync
- Sécurisation des identifiants de localisation de stockage

Protection des données dans AWS DataSync

AWS DataSync transfère en toute sécurité les données entre les systèmes de stockage autogérés et les services AWS de stockage, ainsi qu'entre les services AWS de stockage. La manière dont vos données de stockage sont cryptées pendant le transfert dépend en partie des emplacements concernés par le transfert.

Une fois le transfert terminé, les données sont cryptées au repos par le système ou le service qui les stocke (non DataSync).

Rubriques

- AWS DataSync chiffrement en transit
- AWS DataSync chiffrement au repos
- Confidentialité du trafic inter-réseau

AWS DataSync chiffrement en transit

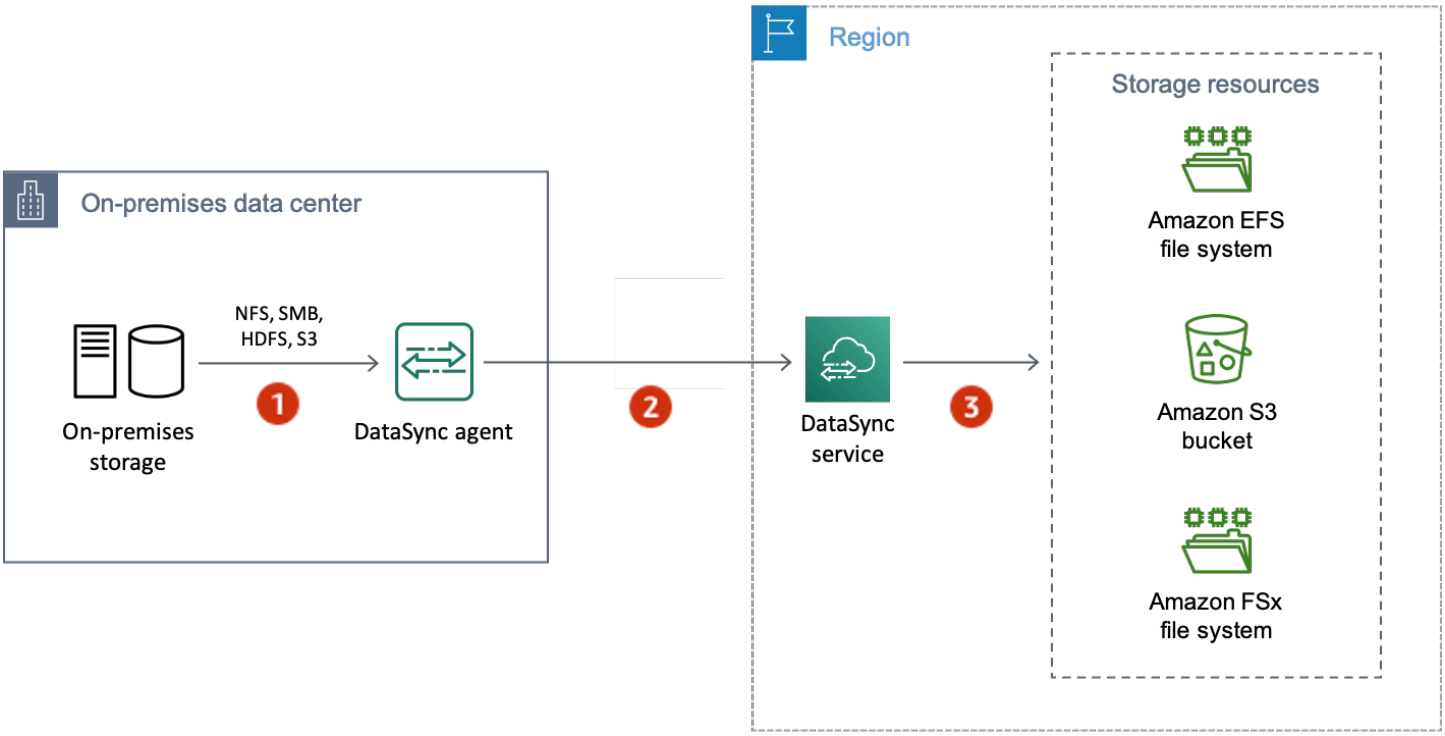
Vos données de stockage (y compris les métadonnées) sont cryptées pendant le transfert, mais la manière dont elles sont cryptées tout au long du transfert dépend de vos emplacements source et de destination.

Lorsque vous vous connectez à un emplacement, DataSync utilise les options les plus sécurisées fournies par le protocole d'accès aux données de cet emplacement. Par exemple, lorsque vous vous connectez à un système de fichiers à l'aide de Server Message Block (SMB), DataSync utilise les fonctionnalités de sécurité fournies par SMB.

Connexions réseau lors d'un transfert

DataSync nécessite trois connexions réseau pour copier des données : une connexion pour lire des données depuis un emplacement source, une autre pour transférer des données entre des sites et une autre pour écrire des données vers un emplacement de destination.

Le schéma suivant illustre les connexions réseau DataSync utilisées pour transférer des données d'un système de stockage sur site vers un service AWS de stockage. Pour comprendre où se produisent les connexions et comment les données sont protégées lors de leur transfert via chaque connexion, utilisez le tableau ci-joint.



Référence	Connexion réseau	Description
1	Lecture de données depuis l'emplacement source	DataSync se connecte en utilisant le protocole du système de stockage pour accéder aux données (par exemple, SMB ou l'API Amazon S3). Pour cette connexion, les données sont protégées à l'aide des fonctionnalités de sécurité du système de stockage, sauf si celui-ci DataSync ne prend pas en charge ces fonctionnalités. Par exemple, il ne prend DataSync actuellement pas en charge l'authentification Kerberos avec les serveurs de fichiers NFS ou lors de l'utilisation du chiffrement TDE avec HDFS.
2	Transfert de données entre sites	Pour cette connexion, DataSync chiffre tout le trafic réseau avec le

Référence	Connexion réseau	Description
		protocole MTLS (Transport Layer Security) 1.3 mutuel.
3	Écrire des données vers le lieu de destination	Comme pour l'emplacement de la source, DataSync se connecte en utilisant le protocole du système de stockage pour accéder aux données. Les données sont à nouveau protégées à l'aide des fonctionn alités de sécurité du système de stockage, sauf DataSync s'il n'est pas compatible avec ces fonctionn alités.

Découvrez comment vos données sont cryptées en transit lorsque vous DataSync vous connectez aux services AWS de stockage suivants :

- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP
- Amazon S3

Chiffrements TLS

Lors du transfert de données entre sites, DataSync utilise différents chiffrements TLS. Le chiffrement TLS dépend du type de point de terminaison de service avec lequel votre agent communique. DataSync (Pour plus d'informations, consultez Choisir un point de terminaison de service pour votre AWS DataSync agent.)

Table des matières

- Points de terminaison publics ou VPC
- Points de terminaison FIPS

Points de terminaison publics ou VPC

Pour les points de terminaison des services de cloud privé public et virtuel (VPC), DataSync utilise l'un des chiffrements TLS suivants :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_ (ecdh_x25519SHA384)
- TLS_ECDHE_RSA_WITH_ 0_ 05_ (ecdh_x25519CHACHA2) POLY13 SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_ (ecdh_x25519SHA256)

Points de terminaison FIPS

Pour les points de terminaison du service FIPS (Federal Information Processing Standard), DataSync utilise le chiffrement TLS suivant :

- TLS_AES_128_GCM_ (SHA256 secp256r1)

AWS DataSync chiffrement au repos

Comme il AWS DataSync s'agit d'un service de transfert, il ne gère généralement pas vos données de stockage au repos. Les services et systèmes de stockage pris DataSync en charge sont chargés de protéger les données dans cet état. Cependant, certaines données relatives aux services sont DataSync gérées au repos.

Qu'est-ce qui est crypté ?

Les seules données traitées DataSync au repos concernent les informations dont elles ont besoin pour effectuer votre transfert. DataSync stocke les données suivantes avec un chiffrement complet au repos dans Amazon DynamoDB :

- Configurations des tâches (par exemple, détails sur les lieux concernés par votre transfert).
- Informations d'identification utilisateur qui permettent à votre DataSync agent de s'authentifier auprès d'un emplacement. Ces informations d'identification sont cryptées à l'aide des clés publiques de votre agent. L'agent peut déchiffrer ces clés selon les besoins à l'aide de ses clés privées.

Pour plus d'informations, consultez la section Chiffrement DynamoDB au repos dans le manuel Amazon DynamoDB Developer Guide.

Gestion des clés

Vous ne pouvez pas gérer les clés de chiffrement DataSync utilisées pour stocker les informations relatives à l'exécution de votre tâche dans DynamoDB. Ces informations incluent la configuration de vos tâches et les informations d'identification utilisées par les agents pour s'authentifier auprès d'un emplacement de stockage.

Qu'est-ce qui n'est pas crypté ?

Bien que DataSync cela ne contrôle pas la manière dont vos données de stockage sont cryptées au repos, nous vous recommandons tout de même de configurer vos sites avec le niveau de sécurité le plus élevé qu'ils prennent en charge. Par exemple, vous pouvez chiffrer des objets avec des clés de chiffrement gérées par Amazon S3 (SSE-S3) ou des clés (KMS) AWS Key Management Service (AWS SSE-KMS).

En savoir plus sur la façon dont les services AWS de stockage cryptent les données au repos :

- Amazon S3
- Amazon EFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon FSx pour Lustre
- Amazon FSx pour OpenZFS
- Amazon FSx pour NetApp ONTAP

Confidentialité du trafic inter-réseau

Nous vous recommandons de configurer vos emplacements source et de destination avec le niveau de sécurité le plus élevé que chacun d'entre eux prend en charge. Lorsque vous vous connectez à un emplacement, AWS DataSync fonctionne avec la version la plus sécurisée du protocole d'accès aux données utilisé par le système de stockage. En outre, pensez à limiter le trafic de sous-réseau aux protocoles et services connus.

DataSync sécurise la connexion entre les sites, y compris entre Comptes AWS, et les zones de disponibilité Régions AWS, en utilisant le protocole TLS (Transport Layer Security) 1.3.

Gestion des identités et des accès dans AWS DataSync

AWS utilise des identifiants de sécurité pour vous identifier et vous donner accès à vos AWS ressources. Vous pouvez utiliser les fonctionnalités de AWS Identity and Access Management (IAM) pour permettre à d'autres utilisateurs, services et applications d'utiliser vos AWS ressources dans leur intégralité ou de manière limitée, sans partager vos informations d'identification de sécurité.

Par défaut, les identités IAM (utilisateurs, groupes et rôles) ne sont pas autorisées à créer, afficher ou modifier AWS des ressources. Pour permettre aux utilisateurs, aux groupes et aux rôles d'accéder aux AWS DataSync ressources et d'interagir avec la DataSync console et l'API, nous vous recommandons d'utiliser une politique IAM qui leur accorde l'autorisation d'utiliser les ressources et les actions d'API spécifiques dont ils auront besoin. Ensuite, vous attachez la stratégie à l'identité IAM qui requiert l'accès. Pour obtenir une présentation des éléments d'une stratégie, consultez Gestion des accès pour AWS DataSync.

Rubriques

- Gestion des accès pour AWS DataSync
- AWS politiques gérées pour AWS DataSync
- Politiques gérées par le client IAM pour AWS DataSync
- Utilisation des rôles liés aux services pour DataSync
- Autorisations pour le balisage des DataSync ressources lors de la création
- Prévention du problème de l'adjoint confus entre services

Gestion des accès pour AWS DataSync

Chaque AWS ressource appartient à un Compte AWS. Les autorisations pour créer ou accéder à un ressource sont gérées par des stratégies d'autorisations. Un administrateur de compte peut associer des politiques d'autorisation aux identités AWS Identity and Access Management (IAM). Certains services (tels que AWS Lambda) permettent également d'associer des politiques d'autorisation aux ressources.

> **Note**
>
> Un administrateur de compte est un utilisateur doté de privilèges d'administrateur dans un Compte AWS. Pour plus d'informations, consultez Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Rubriques

- DataSync ressources et opérations
- Présentation de la propriété des ressources
- Gestion de l'accès aux ressources
- Spécification des éléments d'une politique : actions, effets, ressources et principaux
- Spécification de conditions dans une politique

DataSync ressources et opérations

Dans DataSync, les ressources principales sont l'agent, l'emplacement, la tâche et l'exécution des tâches.

Ces ressources sont associées à des noms de ressources Amazon uniques (ARNs), comme indiqué dans le tableau suivant.

Type de ressource	Format ARN
ARN de l'agent	`arn:aws:datasync: region:account-id :agent/agent-id`
ARN de l'emplacement	`arn:aws:datasync: region:account-id :location/ location-id`
ARN de tâche	`arn:aws:datasync: region:account-id :task/task-id`
ARN d'exécution des tâches	`arn:aws:datasync: region:account-id :task/task-id/execution/ exec-id`

L'octroi d'autorisations pour des opérations d'API spécifiques, telles que la création d'une tâche, DataSync définit un ensemble d'actions que vous pouvez spécifier dans une politique d'autorisation. Une opération d'API peut exiger des autorisations pour plusieurs actions.

Présentation de la propriété des ressources

Le propriétaire de la ressource est celui Compte AWS qui a créé la ressource. C'est-à-dire que le propriétaire Compte AWS de la ressource est l'entité principale (par exemple, un rôle IAM) qui authentifie la demande qui crée la ressource. Les exemples suivants illustrent le fonctionnement de ce comportement :

- Si vous utilisez les informations d'identification de votre compte root Compte AWS pour créer une tâche, vous Compte AWS êtes le propriétaire de la ressource (dans DataSync, la ressource est la tâche).
- Si vous créez un rôle IAM dans votre Compte AWS et que vous accordez des autorisations pour l'`CreateTask`action à cet utilisateur, celui-ci peut créer une tâche. Cependant, c'est à vous Compte AWS, à laquelle appartient l'utilisateur, que appartient la ressource de tâche.
- Si vous créez un rôle IAM Compte AWS avec les autorisations nécessaires pour créer une tâche, toute personne capable d'assumer ce rôle peut créer une tâche. C'est à vous Compte AWS, à qui appartient le rôle, que appartient la ressource de tâche.

Gestion de l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

> **Note**
>
> Cette section décrit l'utilisation d'IAM dans le contexte de DataSync. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, consultez la rubrique Qu'est-ce que IAM ? dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, consultez la référence des AWS Identity and Access Management politiques dans le Guide de l'utilisateur IAM.

Les politiques associées à une identité IAM sont appelées politiques basées sur l'identité (politiques IAM) et les politiques associées à une ressource sont appelées politiques basées sur les ressources. DataSync prend uniquement en charge les politiques basées sur l'identité (politiques IAM).

Rubriques

- Politiques basées sur l'identité

- Politiques basées sur les ressources

Politiques basées sur l'identité

Vous pouvez gérer l'accès aux DataSync ressources à l'aide de politiques IAM. Ces politiques peuvent aider un Compte AWS administrateur à effectuer les opérations suivantes avec DataSync :

- Accordez des autorisations pour créer et gérer DataSync des ressources : créez une politique IAM qui permet à un rôle IAM de Compte AWS créer et de gérer des DataSync ressources, telles que des agents, des sites et des tâches.
- Accorder des autorisations à un rôle dans un autre Compte AWS ou un Service AWS — Créez une politique IAM qui accorde des autorisations à un rôle IAM dans un autre Compte AWS ou un. Service AWS Par exemple :
  1. L'administrateur du compte A crée un rôle IAM et associe une politique d'autorisation au rôle qui accorde des autorisations sur les ressources du compte A.
  2. L'administrateur du compte A attache une politique de confiance au rôle qui identifie le compte B comme le principal habilité à assumer le rôle.

     Pour accorder à un Service AWS utilisateur l'autorisation d'assumer ce rôle, l'administrateur du compte A peut spécifier un Service AWS comme principal dans la politique de confiance.
  3. L'administrateur du compte B peut ensuite déléguer les autorisations nécessaires pour assumer le rôle à n'importe quel utilisateur du compte B. Cela permet à toute personne utilisant le rôle dans le compte B de créer ou d'accéder aux ressources du compte A.

  Pour plus d'informations sur l'utilisation d'IAM pour déléguer des autorisations, veuillez consulter la section Access management (français non garanti) dans le Guide de l'utilisateur IAM.

L'exemple de politique suivant accorde des autorisations à toutes les `List*` actions sur toutes les ressources. Cette action est en lecture seule et n'autorise pas la modification des ressources.

JSON

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

```
            "Effect": "Allow",
            "Action": [
                "datasync:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur l'utilisation de politiques basées sur l'identité avec DataSync, consultez les sections Politiques AWS gérées et Politiques gérées par le client. Pour plus d'informations sur les identités IAM, consultez le guide de l'utilisateur IAM.

Politiques basées sur les ressources

D'autres services, tels qu'Amazon S3, prennent en charge les politiques d'autorisation basées sur les ressources. Par exemple, vous pouvez attacher une politique à un compartiment Amazon S3 pour gérer les autorisations d'accès à ce compartiment. Toutefois, DataSync ne prend pas en charge les politiques basées sur les ressources.

Spécification des éléments d'une politique : actions, effets, ressources et principaux

Pour chaque DataSync ressource, le service définit un ensemble d'opérations d'API (voir Actions). Pour accorder des autorisations pour ces opérations d'API DataSync , définissez un ensemble d'actions que vous pouvez spécifier dans une politique. Par exemple, pour la DataSync ressource, les actions suivantes sont définies : `CreateTaskDeleteTask`, et`DescribeTask`. Une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments les plus élémentaires d'une politique :

- Ressource : dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique. Pour les ressources DataSync, vous pouvez utiliser le caractère générique `(*)` dans les stratégies IAM. Pour de plus amples informations, veuillez consulter DataSync ressources et opérations.
- Action : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, en fonction de l'`Effect`élément spécifié, l'`datasync:CreateTask`autorisation autorise ou refuse à l'utilisateur l'autorisation d'effectuer l' DataSync `CreateTask`opération.

- Effet : vous spécifiez l'effet lorsque l'utilisateur demande l'action spécifique. Cet effet peut être soit soit`Allow`. `Deny` Si vous n'accordez pas explicitement l'accès à (`Allow`) une ressource, l'accès est implicitement refusé. Vous pouvez également refuser explicitement l'accès à une ressource, ce que vous pouvez faire pour vous assurer qu'un utilisateur ne peut pas y accéder, même si une politique différente accorde cet accès à cet utilisateur. Pour plus d'informations, consultez la section Autorisation dans le guide de l'utilisateur IAM.
- Principal – dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur les ressources, vous spécifiez l'utilisateur, le compte, le service ou toute autre entité pour lequel vous souhaitez recevoir des autorisations (s'applique uniquement aux politiques basées sur les ressources). DataSync ne prend pas en charge les politiques basées sur les ressources.

Pour en savoir plus sur la syntaxe et les descriptions des politiques IAM, consultez la référence aux AWS Identity and Access Management politiques dans le Guide de l'utilisateur IAM.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage de stratégie IAM pour spécifier les conditions définissant à quel moment une stratégie doit prendre effet lors de l'octroi des autorisations. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification des conditions dans le langage des politiques, consultez la section Condition du guide de l'utilisateur IAM.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Il n'existe pas de clés de condition spécifiques à DataSync. Cependant, il existe de AWS larges clés de condition que vous pouvez utiliser selon les besoins. Pour obtenir la liste complète des touches AWS larges, consultez la section Clés disponibles dans le guide de l'utilisateur IAM.

AWS politiques gérées pour AWS DataSync

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

Services AWS maintenir et mettre à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` AWS gérée fournit un accès en lecture seule à toutes Services AWS les ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSDataSyncReadOnlyAccess

Vous pouvez associer la politique `AWSDataSyncReadOnlyAccess` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule pour. DataSync

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DataSyncReadOnlyAccessPermissions",
        "Effect": "Allow",
        "Action": [
            "datasync:Describe*",
            "datasync:List*",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "elasticfilesystem:DescribeFileSystems",
```

```
            "elasticfilesystem:DescribeMountTargets",
            "fsx:DescribeFileSystems",
            "iam:GetRole",
            "iam:ListRoles",
            "logs:DescribeLogGroups",
            "logs:DescribeResourcePolicies",
            "s3:ListAllMyBuckets",
            "s3:ListBucket"
        ],
        "Resource": "*"
    }]
}
```

AWS politique gérée : AWSDataSyncFullAccess

Vous pouvez associer la politique `AWSDataSyncFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives DataSync et est requise pour AWS Management Console accéder au service. `AWSDataSyncFullAccess`fournit un accès complet aux opérations d' DataSync API et aux opérations qui interagissent avec les ressources associées (telles que les compartiments Amazon S3, les systèmes de fichiers Amazon EFS, AWS KMS les clés et les secrets de Secrets Manager). La politique accorde également des autorisations à Amazon CloudWatch, y compris la création de groupes de journaux et la création ou la mise à jour d'une politique de ressources.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DataSyncFullAccessPermissions",
            "Effect": "Allow",
            "Action": [
                "datasync:*",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeVpcEndpoints",
                "ec2:ModifyNetworkInterfaceAttribute",
                "fsx:DescribeFileSystems",
                "fsx:DescribeStorageVirtualMachines",
                "elasticfilesystem:DescribeAccessPoints",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeMountTargets",
                "iam:GetRole",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "logs:DescribeResourcePolicies",
                "outposts:ListOutposts",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3-outposts:ListAccessPoints",
                "s3-outposts:ListRegionalBuckets",
                "secretsmanager:ListSecrets",
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DataSyncPassRolePermissions",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datasync.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "DataSyncCreateSLRPermissions",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
datasync.amazonaws.com/AWSServiceRoleForDataSync",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "datasync.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DataSyncSecretsManagerCreateAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret"
            ],
            "Resource": [
                "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "DataSyncSecretsManagerAccess",
            "Effect": "Allow",
            "Action": [

                "secretsmanager:DeleteSecret",
                "secretsmanager:UpdateSecret",
                "secretsmanager:PutSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:aws-datasync!*"
            ],
            "Condition": {
                "StringEquals": {
                    "secretsmanager:ResourceTag/
aws:secretsmanager:owningService": "aws-datasync",
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
```

```
        }
    ]
}
```

AWS politique gérée : AWSDataSyncServiceRolePolicy

Vous ne pouvez pas associer la `AWSDataSyncServiceRolePolicy` politique à vos identités IAM. Cette politique est associée à un rôle lié à un service qui permet d' DataSync effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés aux services pour DataSync.

Cette politique accorde des autorisations administratives qui permettent au rôle lié au service de créer des CloudWatch journaux Amazon pour les DataSync tâches utilisant le mode amélioré.

Mises à jour des politiques

Modification	Description	Date
AWSDataSyncFullAccess—Modification	DataSync déclarations d'autorisation modifiées pour `AWSDataSyncFullAccess` : Les instructions mises à jour suppriment les conditions de balisage des autorisations DataSync utilisées pour créer des secrets Secrets Manager.	13 mai 2025
AWSDataSyncFullAccess—Modification	DataSync a ajouté de nouvelles autorisations pour `AWSDataSyncFullAccess` : • `secretsmanager:CreateSecret`	7 mai 2025

Modification	Description	Date
	• `secretsmanager:PutSecretValue` • `secretsmanager:DeleteSecret` • `secretsmanager:UpdateSecret` Ces autorisations permettent de DataSync créer, de modifier et de supprimer AWS Secrets Manager des secrets.	
AWSDataSyncFullAccess—Modification	DataSync a ajouté de nouvelles autorisations pour `AWSDataSyncFullAccess` : • `secretsmanager:ListSecrets` • `kms:ListAliases` • `kms:DescribeKey` Ces autorisations permettent de DataSync récupérer des métadonnées concernant vos AWS Secrets Manager secrets et vos AWS KMS clés, y compris les alias associés à vos clés.	23 avril 2025

Modification	Description	Date
AWSDataSyncService RolePolicy— Modification	DataSync a ajouté de nouvelles autorisations à la `AWSDataSyncServiceRolePolicy` politique utilisée par le rôle DataSync lié au service : `AWSServiceRoleForDataSync` • `secretsmanager:DescribeSecret` • `secretsmanager:GetSecretValue` Ces autorisations permettent de DataSync lire les métadonnées et les valeurs des secrets gérés par AWS Secrets Manager.	15 avril 2025
AWSDataSyncService RolePolicy : nouvelle politique	DataSync a ajouté une politique qui est utilisée par le rôle DataSync lié au service. `AWSServiceRoleForDataSync` Cette nouvelle politique gérée crée automatiquement des CloudWatch journaux Amazon pour vos DataSync tâches qui utilisent le mode amélioré.	30 octobre 2024

Modification	Description	Date
AWSDataSyncFullAccess—Modification	DataSync a ajouté une nouvelle autorisation pour `AWSDataSyncFullAccess` : • `iam:CreateServiceLinkedRole` Cette autorisation permet de DataSync créer des rôles liés à un service pour vous.	30 octobre 2024
AWSDataSyncFullAccess—Modification	DataSync a ajouté une nouvelle autorisation pour `AWSDataSyncFullAccess` : • `ec2:DescribeRegions` Cette autorisation vous permet de choisir des régions facultatives lors de la création d'une DataSync tâche pour les transferts entre Régions AWS celles-ci.	22 juillet 2024

Modification	Description	Date
AWSDataSyncFullAccess—Modification	DataSync a ajouté une nouvelle autorisation pour `AWSDataSyncFullAccess` : • `s3:ListBucketVersions` Cette autorisation vous permet de choisir une version spécifique de votre DataSync manifeste.	16 février 2024

Modification	Description	Date
AWSDataSyncFullAccess—Modification	DataSync a ajouté de nouvelles autorisations pour `AWSDataSyncFullAccess` : • `ec2:DescribeVpcEndpoints` • `elasticfilesystem:DescribeAccessPoints` • `fsx:DescribeStorageVirtualMachines` • `outposts:ListOutposts` • `s3:GetBucketLocation` • `s3-outposts:ListAccessPoints` • `s3-outposts:ListRegionalBuckets` Ces autorisations vous aident à créer DataSync des agents et des emplacements pour Amazon EFS, Amazon FSx for NetApp ONTAP, Amazon S3 et S3 on Outposts.	2 mai 2023
DataSync a commencé à suivre les modifications	DataSync a commencé à suivre les modifications apportées AWS à ses politiques gérées.	1er mars 2021

Politiques gérées par le client IAM pour AWS DataSync

Outre les politiques AWS gérées, vous pouvez également créer vos propres politiques basées sur les identités AWS DataSync et les associer aux identités AWS Identity and Access Management (IAM) qui nécessitent ces autorisations. Ces politiques sont connues sous le nom de politiques gérées par le client, qui sont des politiques autonomes que vous administrez vous-même. Compte AWS

> **Important**
>
> Avant de commencer, nous vous recommandons de vous renseigner sur les concepts de base et les options de gestion de l'accès à vos DataSync ressources. Pour de plus amples informations, veuillez consulter Gestion des accès pour AWS DataSync.

Lorsque vous créez une politique gérée par le client, vous incluez des déclarations concernant les DataSync opérations qui peuvent être utilisées sur certaines AWS ressources. L'exemple de politique suivant comporte deux déclarations (notez les `Resource` éléments `Action` et de chaque déclaration) :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllTasks",
            "Effect": "Allow",
            "Action": [
                "datasync:DescribeTask",
            ],
            "Resource": "arn:aws:datasync:us-east-2:111222333444:task/*"
        },
        {
            "Sid": "ListAllTasks",
            "Effect": "Allow",
            "Action": [
                "datasync:ListTasks"
            ],
            "Resource": "*"
        },
}
```

Les énoncés de la politique ont les objectifs suivants :

- La première instruction autorise l'exécution de l'`datasync:DescribeTask`action sur certaines ressources des tâches de transfert en spécifiant un Amazon Resource Name (ARN) avec un caractère générique (`*`).
- La deuxième instruction autorise l'exécution de l'`datasync:ListTasks`action sur toutes les tâches en spécifiant simplement un caractère générique (`*`).

Exemples de politiques gérées par le client

L'exemple suivant de politiques gérées par le client octroie des autorisations pour diverses DataSync opérations. Les politiques fonctionnent si vous utilisez le AWS Command Line Interface (AWS CLI) ou un AWS SDK. Pour utiliser ces politiques dans la console, vous devez également utiliser la stratégie géréeAWSDataSyncFullAccess.

Rubriques

- Exemple 1 : créer une relation de confiance qui permet DataSync d'accéder à votre compartiment Amazon S3
- Exemple 2 : DataSync Autoriser la lecture et l'écriture dans votre compartiment Amazon S3
- Exemple 3 : Autoriser DataSync le téléchargement de journaux vers des groupes de CloudWatch journaux

Exemple 1 : créer une relation de confiance qui permet DataSync d'accéder à votre compartiment Amazon S3

Voici un exemple de politique de confiance qui permet d' DataSync assumer un rôle IAM. Ce rôle permet DataSync d'accéder à un compartiment Amazon S3. Pour éviter le problème de confusion entre les services adjoints, nous vous recommandons d'utiliser les clés de contexte `aws:SourceArn`et de condition `aws:SourceAccount`globale dans la politique.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "datasync.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": "111111111111"
                },
                "ArnLike": {
                "aws:SourceArn": "arn:aws:datasync:us-east-1:111111111111:*"
                }
            }
        }
    ]
}
```

Exemple 2 : DataSync Autoriser la lecture et l'écriture dans votre compartiment Amazon S3

L'exemple de politique suivant accorde DataSync les autorisations minimales pour lire et écrire des données dans un compartiment S3 utilisé comme emplacement de destination.

> **Note**
>
> La valeur de `aws:ResourceAccount` doit être l'ID de compte qui possède le compartiment Amazon S3 spécifié dans la politique.

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Action": [
             "s3:GetBucketLocation",
             "s3:ListBucket",
             "s3:ListBucketMultipartUploads"
         ],
         "Effect": "Allow",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition": {
             "StringEquals": {
                 "aws:ResourceAccount": "123456789012"
             }
```

```
            }
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectTagging"
              ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "123456789012"
                }
            }
        }
    ]
}
```

Exemple 3 : Autoriser DataSync le téléchargement de journaux vers des groupes de CloudWatch journaux

DataSync nécessite des autorisations pour pouvoir télécharger des journaux dans vos groupes de CloudWatch journaux Amazon. Vous pouvez utiliser des groupes de CloudWatch journaux pour surveiller et déboguer vos tâches.

Pour un exemple de politique IAM qui accorde de telles autorisations, consultez DataSync Autoriser le téléchargement de journaux dans un groupe de CloudWatch journaux.

Utilisation des rôles liés aux services pour DataSync

AWS DataSync utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. DataSync Les rôles liés au service sont prédéfinis par DataSync et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Rubriques

- Utilisation de rôles pour DataSync

Utilisation de rôles pour DataSync

AWS DataSync utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. DataSync Les rôles liés au service sont prédéfinis par DataSync et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration DataSync car vous n'avez pas à ajouter manuellement les autorisations nécessaires. DataSync définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul DataSync peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos DataSync ressources 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 DataSync

DataSync utilise le rôle lié au service nommé AWSServiceRoleForDataSync— Permet d' DataSync effectuer des opérations essentielles pour l'exécution des tâches de transfert, notamment la lecture de secrets et la création de AWS Secrets Manager groupes de CloudWatch journaux et d'événements.

Le rôle AWSService RoleForDataSync lié à un service fait confiance aux services suivants pour assumer le rôle :

- `datasync.amazonaws.com`

Le rôle lié à un service utilise la politique AWS gérée nommée AWSDataSyncServiceRolePolicy, qui permet d' DataSync effectuer les actions suivantes sur les ressources spécifiées :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DataSyncCloudWatchLogCreateAccess",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:*:logs:*:*:log-group:/aws/datasync*"
            ]
        },
        {
            "Sid": "DataSyncCloudWatchLogStreamUpdateAccess",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:*:logs:*:*:log-group:/aws/datasync*:log-stream:*"
            ]
        },
        {
            "Sid": "DataSyncSecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DescribeSecret",
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
            ],
            "Condition": {
                "StringEquals": {
                    "secretsmanager:ResourceTag/
aws:secretsmanager:owningService": "aws-datasync",
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
```

```
    ]
}
```

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles 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 DataSync

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une DataSync tâche dans le AWS Management Console, le ou l' AWS API AWS CLI, vous DataSync créez le rôle lié au service pour vous.

Dans l'API AWS CLI ou dans l' AWS API, vous pouvez créer un rôle lié à un service avec le nom du `datasync.amazonaws.com` service. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

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 une DataSync tâche, le rôle lié au service est à nouveau DataSync créé pour vous.

Si vous supprimez ce rôle lié à un service, vous pouvez utiliser le même processus IAM pour recréer le rôle.

Modification d'un rôle lié à un service pour DataSync

DataSync ne vous permet pas de modifier le rôle AWSService RoleForDataSync lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

Suppression d'un rôle lié à un service pour DataSync

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. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyer un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle.

> **Note**
>
> Si le DataSync service 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 DataSync les ressources utilisées par AWSService RoleForDataSync

1. Supprimez les DataSync agents utilisés par la tâche (s'il y en a).
2. Supprimez les emplacements de la tâche.
3. Supprimez la tâche.

Suppression manuelle du rôle lié au service

Utilisez la console IAM AWS CLI, le ou l' AWS API pour supprimer le rôle lié au AWSService RoleForDataSync service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service DataSync

DataSync prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour de plus amples informations, veuillez consulter AWS Régions et points de terminaison.

Autorisations pour le balisage des DataSync ressources lors de la création

Certaines actions d' AWS DataSync API de création de ressources vous permettent de spécifier des balises lors de la création de la ressource. Vous pouvez utiliser des 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 permettre aux utilisateurs de baliser les ressources lors de leur création, ils doivent être autorisés à utiliser l'action qui crée la ressource (telle que `datasync:CreateAgent`

oudatasync:CreateTask). Si des balises sont spécifiées dans l'action de création de ressources, les utilisateurs doivent également disposer d'autorisations explicites pour utiliser l'datasync:TagResourceaction.

L'action datasync:TagResource est uniquement évaluée si les balises sont appliquées pendant 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'datasync:TagResourceaction si aucune balise n'est spécifiée dans la demande.

Toutefois, si l'utilisateur tente de créer une ressource avec des balises, la demande échoue s'il n'est pas autorisé à utiliser l'datasync:TagResourceaction.

Exemples de déclarations de politique IAM

Utilisez les exemples de déclarations de politique IAM suivants pour accorder des TagResource autorisations aux utilisateurs qui créent DataSync des ressources.

L'instruction suivante permet aux utilisateurs de baliser un DataSync agent lorsqu'ils le créent.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:444455556666:agent/*"
        }
    ]
}
```

L'instruction suivante permet aux utilisateurs de baliser un DataSync emplacement lorsqu'ils le créent.

JSON

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:111122223333:location/*"
        }
    ]
}
```

L'instruction suivante permet aux utilisateurs de baliser une DataSync tâche lorsqu'ils la créent.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "datasync:TagResource",
            "Resource": "arn:aws:datasync:us-east-1:444455556666:task/*"
        }
    ]
}
```

Prévention du problème de l'adjoint confus entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations qui AWS DataSync accordent un autre service à la ressource. Si vous utilisez les

deux clés de contexte de condition globale et que la valeur `aws:SourceArn` contient l'ID de compte, la valeur `aws:SourceAccount` et le compte dans la valeur `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'ils sont utilisés dans la même instruction de politique. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. À utiliser `aws:SourceAccount` si vous souhaitez qu'une ressource de ce compte soit associée à l'utilisation interservices.

La valeur de `aws:SourceArn` doit inclure l'ARN d' DataSync emplacement avec lequel DataSync il est autorisé à assumer le rôle IAM.

Le moyen le plus efficace de se protéger contre le problème de confusion des adjoints est d'utiliser la `aws:SourceArn` clé avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet ou si vous spécifiez plusieurs ressources, utilisez des caractères génériques (`*`) pour les parties inconnues. Voici quelques exemples de la manière de procéder pour DataSync :

- Pour limiter la politique de confiance à un DataSync emplacement existant, incluez l'ARN complet du site dans la politique. DataSync assumera le rôle IAM uniquement lorsqu'il s'agit de cet emplacement particulier.
- Lorsque vous créez un emplacement Amazon S3 pour DataSync, vous ne connaissez pas l'ARN du site. Dans ces scénarios, utilisez le format suivant pour la `aws:SourceArn` clé : `arn:aws:datasync:us-east-2:123456789012:*` Ce format valide la partition (`aws`), l'ID de compte et la région.

L'exemple complet suivant montre comment utiliser les clés de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et les clés de contexte dans une politique de confiance afin d'éviter le problème de confusion lié aux adjoints DataSync.

JSON

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

```
                "StringEquals": {
                "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                "aws:SourceArn": "arn:aws:datasync:us-east-2:123456789012:*"
                }
            }
        }
    ]
}
```

Pour d'autres exemples de politiques indiquant comment utiliser les clés contextuelles de condition `aws:SourceAccount` globale `aws:SourceArn` et les clés contextuelles avec DataSync, consultez les rubriques suivantes :

- Créez une relation de confiance qui permet DataSync d'accéder à votre compartiment Amazon S3
- Configurer un rôle IAM pour accéder à votre compartiment Amazon S3

Validation de conformité pour AWS DataSync

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS DataSync

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

> **Note**
>
> Si une zone de disponibilité vers laquelle vous migrez des données ou à partir de laquelle vous migrez des données échoue pendant que vous exécutez une DataSync tâche, celle-ci échouera également.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure dans AWS DataSync

En tant que service géré, AWS DataSync il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder DataSync via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Sécurisation des identifiants de localisation de stockage

DataSync utilise des emplacements pour accéder à vos ressources de stockage situées sur site, dans d'autres clouds ou dans AWS. Certains types d'emplacement nécessitent que vous fournissiez des informations d'identification, telles qu'une clé d'accès et une clé secrète ou un nom d'utilisateur et

un mot de passe, pour vous authentifier auprès de votre système de stockage. Lorsque vous créez un DataSync emplacement qui nécessite des informations d'identification pour l'authentification, vous pouvez choisir l'une des options suivantes pour contrôler la manière dont le secret de vos informations d'identification est stocké :

- Stockez le secret à AWS Secrets Manager l'aide d'un secret géré par le service crypté avec une clé par défaut.
- Stockez le secret à AWS Secrets Manager l'aide d'un secret géré par un service crypté à l'aide d'une AWS KMS clé que vous gérez.
- Stockez le secret à AWS Secrets Manager l'aide d'un secret et d'une clé que vous créez et gérez. DataSync accède à ce secret à l'aide d'un rôle IAM que vous fournissez.

Dans tous les cas, le secret Secrets Manager est enregistré dans votre compte, ce qui vous permet de le mettre à jour selon vos besoins, indépendamment du DataSync service. Vous n'êtes facturé que pour l'utilisation de secrets que vous créez en dehors de DataSync. Les secrets créés et gérés par DataSync portent le préfixe`aws-datasync`.

Utilisation d'un secret géré par un service chiffré avec une clé par défaut

Lorsque vous créez votre DataSync position, il vous suffit de fournir la chaîne secrète. DataSynccrée une ressource secrète AWS Secrets Manager pour stocker le secret que vous fournissez, et le chiffre avec la clé KMS par défaut de Secrets Manager pour votre compte. Vous pouvez modifier la valeur du secret directement dans Secrets Manager ou en mettant à jour l'emplacement à l'aide de la DataSync console ou du SDK. AWS CLI Lorsque vous supprimez la ressource de localisation ou que vous la mettez à jour pour utiliser un secret personnalisé, la DataSync ressource secrète est automatiquement supprimée.

> **Note**
>
> Pour créer, modifier et supprimer des ressources secrètes dans Secrets Manager, vous DataSync devez disposer des autorisations appropriées. Pour plus d'informations, consultez Politiques gérées par AWS pour DataSync.

Utilisation d'un secret géré par un service chiffré à l'aide d'une clé personnalisée AWS KMS

Lorsque vous créez votre DataSync position, vous fournissez le secret et l'ARN de votre AWS KMS clé. DataSync crée automatiquement une ressource secrète AWS Secrets Manager pour stocker le secret que vous fournissez et le chiffre à l'aide de votre AWS KMS clé. Vous pouvez modifier la valeur du secret directement dans Secrets Manager ou en mettant à jour l'emplacement à l'aide de la DataSync console ou du SDK. AWS CLI Lorsque vous supprimez la ressource de localisation ou que vous la mettez à jour pour utiliser un secret personnalisé, la DataSync ressource secrète est automatiquement supprimée.

> **Note**
>
> Votre AWS KMS clé doit utiliser un chiffrement symétrique avec le type de `ENCRYPT_DECRYPT` clé. Pour plus d'informations, consultez la section Choix d'une AWS Key Management Service clé dans le guide de AWS Secrets Manager l'utilisateur.

Pour créer, modifier et supprimer des ressources secrètes dans Secrets Manager, vous DataSync devez disposer des autorisations appropriées. Pour plus d'informations, consultez Politique gérée par AWS : AWSDataSyncFullAccess.

Outre l'utilisation de la politique DataSync gérée appropriée, vous devez également disposer des autorisations suivantes :

```
{
    "Sid": "DataSyncKmsPermissions",
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": "your-kms-key-arn",
    "Condition": {
        "StringLike": {
            "kms:ViaService": "secretsmanager.*.amazonaws.com"
        }
    }
```

```
}
```

*your-kms-key-arn*Remplacez-le par l'ARN de votre clé KMS.

Pour récupérer et déchiffrer la valeur secrète, utilisez un DataSync rôle lié au service (SLR) pour accéder à votre AWS KMS clé. Pour vous assurer que DataSync vous pouvez utiliser votre clé KMS, ajoutez ce qui suit à la déclaration de politique relative à la clé :

```
{
    "Sid": "Allow DataSync to use the key for decryption",
    "Effect": "Allow",
    "Principal": {
            "AWS": "arn:aws:iam::accountid:role/aws-service-role/
datasync.amazonaws.com/AWSServiceRoleForDataSync"
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

*accountid*Remplacez-le par votre Compte AWS identifiant.

Utiliser un secret que vous gérez

Avant de créer votre DataSync position, créez un secret dans AWS Secrets Manager. La valeur du secret doit uniquement contenir la chaîne secrète elle-même en texte brut. Lorsque vous créez votre DataSync position, vous fournissez l'ARN de votre secret et un rôle IAM qui DataSync permet d'accéder à la fois à votre secret et à la AWS KMS clé utilisée pour le chiffrer. Pour créer un rôle IAM doté des autorisations appropriées, procédez comme suit :

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles, puis sélectionnez Créer un rôle.
3. Sur la page Sélectionner une entité de confiance, pour Type d'entité fiable, sélectionnez AWS service.
4. Pour Cas d'utilisation, DataSyncchoisissez dans la liste déroulante. Choisissez Suivant.
5. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant). Entrez un nom pour votre rôle, puis choisissez Créer un rôle.
6. Sur la page Rôles, recherchez le rôle que vous venez de créer et choisissez son nom.

7. Sur la page Détails du rôle, choisissez l'onglet Autorisations. Choisissez Ajouter des autorisations, puis Créer une politique intégrée.
8. Choisissez l'onglet JSON et ajoutez les autorisations suivantes dans l'éditeur de politiques :

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:your-secret-name"
        }
    ]
}
```

   *your-secret-arn*Remplacez-le par l'ARN de votre secret Secrets Manager.
9. Choisissez Suivant. Entrez un nom pour votre politique, puis choisissez Créer une politique.
10. (Recommandé) Pour éviter le problème de confusion entre les services adjoints, procédez comme suit :

    a. Sur la page Détails du rôle, choisissez l'onglet Relations de confiance. Choisissez Edit trust policy (Modifier la politique d'approbation).
    b. Mettez à jour la politique de confiance en utilisant l'exemple suivant, qui inclut les clés de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale :

       JSON

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

```
            "Principal": {
                "Service": "datasync.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                "aws:SourceArn": "arn:aws:datasync:us-
east-1:111122223333:*"
                }
            }
        }
    ]
}
```

c. Choisissez Mettre à jour une politique.

Vous pouvez spécifier ce rôle lors de la création de votre position. Si votre secret utilise une AWS KMS clé gérée par le client pour le chiffrement, vous devrez également mettre à jour la politique de la clé pour autoriser l'accès à partir du rôle que vous avez créé lors de la procédure précédente. Pour mettre à jour la politique, ajoutez ce qui suit à la déclaration de politique de votre AWS KMS clé :

```
{
    "Sid": "Allow DataSync use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam accountid:role/your-role-name”
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

*accountid*Remplacez-le par votre Compte AWS ID et *your-role-name* par le nom du rôle IAM que vous avez créé lors de la procédure précédente.

> **Note**
>
> Lorsque vous stockez des secrets dans Secrets Manager, des frais Compte AWS vous sont facturés. Pour plus d'informations sur la tarification, consultez Tarification AWS Secrets Manager.

AWS DataSync quotas

Renseignez-vous sur les quotas et les limites de ressources lorsque vous travaillez avec AWS DataSync.

Limites relatives au système de stockage, aux fichiers et aux objets

Le tableau suivant décrit les limites applicables à DataSync l'utilisation de systèmes de stockage, de fichiers et d'objets.

Description	Limite
Longueur totale maximale du chemin de fichier	4,096 bytes
Longueur maximale du composant du chemin de fichier (nom de fichier, répertoire ou sous-répertoire)	255 octets
Longueur maximale du domaine Windows	253 caractères
Longueur maximale du nom d'hôte du serveur	255 caractères
Longueur maximale du nom d'objet Amazon S3	1 024 caractères UTF-8

DataSync quotas

Le tableau suivant décrit les quotas de DataSync ressources dans une région Compte AWS et une région spécifiques.

Ressource	Quota	Ajustable
Nombre maximum de tâches que vous pouvez créer	100	Oui
(Tâches en mode amélioré) Nombre maximal d'objets source et de destination DataSync pouvant être utilisés par exécution de tâche	Pratiquement illimité	N/A

Ressource	Quota	Ajustable
Pour de plus amples informations, consultez Comment DataSync transférer des fichiers, des objets et des répertoires.		

Ressource	Quota	Ajustable
(Tâches en mode de base) Nombre maximal de fichiers, d'objets et de répertoires source et de destination DataSync pouvant être utilisés par exécution de tâche entre le stockage et AWS les services de stockage sur site, autogérés ou autres dans le cloud Pour de plus amples informations, consultez Comment DataSync transférer des fichiers, des objets et des répertoires.	50 millions **Important** N'oubliez pas ce qui suit à propos de ce quota : • Si vous transférez des objets Amazon S3 avec des préfixes, ceux-ci sont traités comme des répertoires et sont pris en compte dans le calcul du quota. Par exemple, DataSync considérez `s3://bucket/foo/bar.txt` comme deux répertoires (`./`et`./foo/`) et un objet (`bar.txt`). • Si votre tâche concerne plus de 20 millions de fichiers, d'objets ou de répertoires, assurez-vous d'allouer un minimum de 64 Go de RAM à votre DataSync agent. Pour plus d'informations, consultez les	Oui **Tip** Au lieu de demander une augmentation, vous pouvez créer des tâches axées sur des annuaires spécifiques à l'aide de filtres d'inclusion et d'exclusion. Pour plus d'informations, consultez la

Ressource	Quota	Ajustable
	exigences relatives aux agents pour les DataSync transferts.	section Filtrage des données transférées par DataSync.

Ressource	Quota	Ajustable
(Tâches en mode de base) Nombre maximal de fichiers, d'objets et de répertoires source et de destination DataSync pouvant être utilisés par exécution de tâche entre les services AWS de stockage Pour de plus amples informations, consultez Comment DataSync transférer des fichiers, des objets et des répertoires.	25 millions **Important** Si vous transférez des objets Amazon S3 avec des préfixes, ceux-ci sont traités comme des répertoires et sont pris en compte dans le calcul du quota. Par exemple, DataSync considérez `s3://bucket/foo/bar.txt` comme deux répertoires (`./`et`./foo/`) et un objet (`bar.txt`).	Oui **Tip** Au lieu de demander une augmentation, vous pouvez créer des tâches axées sur des annuaires spécifiques à l'aide de filtres d'inclusion et d'exclusion. Pour plus d'informations, consultez la

Ressource	Quota	Ajustable
		section Filtrage des données transférées par DataSync.
Débit maximal par tâche (pour les transferts utilisant un DataSync agent)	10 Gbit/s	Non
Débit maximal par tâche (pour les transferts qui n'utilisent pas d' DataSync agent)	5 Gb/s	Non
Nombre maximum de caractères que vous pouvez inclure dans un filtre de tâches	102,400 caractères **Note** Si vous utilisez la DataSync console, cette limite inclut tous les caractères combinés dans vos modèles d'inclusion et d'exclusion.	Non
Nombre maximal d'exécutions en file d'attente pour une seule tâche	50	Non
Nombre maximum d'exécutions simultanées de tâches en mode amélioré	120	Non
Nombre maximal de jours pendant lesquels l'historique d'exécution des tâches est conservé	30	Non

Demander une augmentation de quota

Vous pouvez demander une augmentation pour certains DataSync quotas. Les augmentations ne sont pas accordées immédiatement et peuvent prendre quelques jours pour entrer en vigueur.

Pour demander une augmentation de quota

1. Ouvrez la console Service Quotas sur https://console.aws.amazon.com/servicequotas/.
2. Dans le volet de navigation, sélectionnez AWS services, puis choisissez AWS DataSync.
3. Choisissez le quota que vous souhaitez augmenter, puis choisissez Demander une augmentation au niveau du compte.
4. Entrez le montant total que vous souhaitez attribuer au quota, puis choisissez Request.

   Si vous devez augmenter un autre quota, remplissez une demande séparée.

AWS DataSync Problèmes de résolution des problèmes

Utilisez les informations suivantes pour résoudre les AWS DataSync problèmes et les erreurs.

Rubriques

- Résolution des problèmes liés aux DataSync agents
- Résolution des problèmes liés aux DataSync emplacements
- Résolution des problèmes liés aux DataSync tâches
- Résolution des problèmes de vérification des données
- Résolution des problèmes liés aux coûts de stockage S3 plus élevés que prévu avec DataSync

Résolution des problèmes liés aux DataSync agents

Utilisez les informations suivantes pour résoudre les problèmes liés aux AWS DataSync agents. Certains de ces problèmes peuvent inclure :

- Problème de connexion à la console locale d'un EC2 agent Amazon
- Impossible de récupérer la clé d'activation d'un agent
- Problèmes d'activation d'un agent avec un point de terminaison de service VPC
- La découverte d'un agent est hors ligne

Comment me connecter à la console locale d'un EC2 agent Amazon ?

Pour vous connecter à la console locale d'un EC2 agent Amazon, vous devez utiliser SSH. Assurez-vous que le groupe de sécurité de votre EC2 instance autorise l'accès via SSH (port TCP 22).

Dans un terminal, exécutez la `ssh` commande suivante pour vous connecter à l'instance :

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

- Pour *`/path/key-pair-name`*, spécifiez le chemin et le nom de fichier (`.pem`) de la clé privée requise pour vous connecter à votre instance.
- Pour *`instance-user-name`*, spécifiez `admin`.
- Pour *`instance-public-ip-address`*, spécifiez l'adresse IP publique de votre instance.

Que signifie l'erreur « Impossible de récupérer la clé d'activation de l'agent » ?

Lorsque vous activez votre DataSync agent, celui-ci se connecte au point de terminaison de service que vous spécifiez pour demander une clé d'activation. Cette erreur signifie probablement que les paramètres de sécurité de votre réseau bloquent la connexion.

Action à exécuter

Si vous utilisez un point de terminaison de service de cloud privé virtuel (VPC), vérifiez que les paramètres de votre groupe de sécurité autorisent votre agent à se connecter au point de terminaison VPC. Pour de plus amples informations sur les ports requis, veuillez consulter Configuration réseau requise pour les points de terminaison de service VPC.

Si vous utilisez un point de terminaison FIPS (Federal Information Processing Standard) public ou fédéral, vérifiez que les paramètres de votre pare-feu et de votre routeur autorisent votre agent à se connecter au point de terminaison. Pour plus d'informations, consultez Exigences réseau pour les points de terminaison publics ou de service FIPS.

Je ne parviens toujours pas à activer un agent à l'aide d'un point de terminaison de service VPC

Si vous rencontrez toujours des problèmes pour activer un DataSync agent avec un point de terminaison de service VPC, voir Je ne sais pas ce qui se passe avec mon agent. Quelqu'un peut-il m'aider ?

Que dois-je faire si mon agent est hors ligne ?

Votre DataSync agent peut être hors ligne pour plusieurs raisons, mais vous pourrez peut-être le remettre en ligne. Avant de supprimer l'agent et d'en créer un nouveau, parcourez la liste de contrôle suivante pour vous aider à comprendre ce qui a pu se passer.

- Contactez votre équipe de sauvegarde : si votre agent est hors ligne parce que sa machine virtuelle (VM) a été restaurée à partir d'un instantané ou d'une sauvegarde, vous devrez peut-être remplacer l'agent.
- Vérifiez si la machine virtuelle ou l' EC2 instance Amazon de l'agent est désactivée : selon le type d'agent que vous utilisez, essayez de réactiver la machine virtuelle ou l' EC2 instance si elle est

désactivée. Une fois qu'il est de nouveau activé, testez la connectivité réseau de votre agent à AWS.

- Vérifiez que votre agent répond à la configuration matérielle minimale requise : votre agent est peut-être hors ligne car la configuration de sa machine virtuelle ou de son EC2 instance a été modifiée accidentellement depuis l'activation de l'agent. Par exemple, si votre machine virtuelle ne dispose plus de la mémoire ou de l'espace minimum requis, l'agent peut apparaître comme étant hors ligne. Pour de plus amples informations, veuillez consulter Exigences pour les AWS DataSync agents.
- Attendez que les mises à jour logicielles relatives à l'agent soient terminées : votre agent peut se déconnecter brièvement après les mises à jour logicielles fournies par. AWS Si vous pensez que c'est la raison pour laquelle l'agent est hors ligne, attendez un moment puis vérifiez si l'agent est de nouveau en ligne.
- Vérifiez les paramètres du point de terminaison de votre service VPC : si votre agent hors ligne utilise un point de terminaison de service public et qu'il se trouve également dans le même VPC pour lequel vous avez créé un point de terminaison de service VPC DataSync, vous devrez peut-être désactiver le support DNS privé pour ce point de terminaison VPC.

Si aucune de ces raisons ne semble être la raison pour laquelle l'agent est hors ligne, vous devrez probablement le remplacer.

Je ne sais pas ce qui se passe avec mon agent. Quelqu'un peut-il m'aider ?

Vous pouvez autoriser AWS Support l'accès à votre DataSync agent et aider à résoudre les problèmes liés à l'agent. Vous devez activer cet accès via la console locale de l'agent.

Pour donner Support accès à votre agent

1. Connectez-vous à la console locale de votre agent.
2. À l'invite, entrez **5** pour ouvrir l'invite de commande (pour VMware VMs, utiliser**6**).
3. Saisissez **h** pour ouvrir la fenêtre AVAILABLE COMMANDS (COMMANDES DISPONIBLES).
4. Dans la fenêtre COMMANDES DISPONIBLES, entrez les informations suivantes pour vous connecter à Support :

   ```
   open-support-channel
   ```

   Si vous utilisez l'agent avec des points de terminaison VPC, vous devez fournir une adresse IP de point de terminaison VPC pour votre canal de support, comme suit :

open-support-channel ***vpc-ip-address***

Votre pare-feu doit autoriser le port TCP entrant 22 à initier un canal d'assistance vers. AWS Lorsque vous vous connectez à Support, vous DataSync attribue un numéro d'assistance. Notez ce numéro.

> **Note**
>
> Le numéro de canal n'est pas un numéro de port TCP/UDP. Au lieu de cela, il établit une connexion SSH (TCP 22) aux serveurs et fournit le canal de support pour la connexion.

5. Lorsque le canal d'assistance est établi, fournissez votre numéro de service d'assistance Support afin qu'il puisse fournir une assistance en matière de dépannage.
6. Lorsque la session d'assistance est terminée, appuyez dessus **Enter** pour y mettre fin.
7. Entrez **exit** pour vous déconnecter de la console DataSync locale.
8. Suivez les invites pour quitter la console locale.

Résolution des problèmes liés aux DataSync emplacements

Utilisez les informations suivantes pour vous aider à résoudre les problèmes liés aux AWS DataSync emplacements. Certains de ces problèmes peuvent inclure :

- Permissions et erreurs de montage avec les emplacements NFS
- Problèmes liés à la propriété des fichiers
- Problèmes d'accès aux sites SMB utilisant l'authentification Kerberos
- Problèmes d'autorisation et d'accès liés au stockage d'objets, tels que les emplacements Amazon S3 et Microsoft Azure Blob

Ma tâche a échoué avec un message d'erreur indiquant que les autorisations NFS ont été refusées

Un message d'erreur « autorisations refusées » peut s'afficher si vous configurez votre serveur de fichiers NFS avec `root_squash` ou `all_squash` si vos fichiers ne disposent pas tous d'un accès en lecture.

Action à exécuter

Pour résoudre ce problème, configurez votre exportation NFS avec `no_root_squash` ou assurez-vous que les autorisations associées à tous les fichiers que vous souhaitez transférer autorisent un accès en lecture à tous les utilisateurs.

Pour accéder DataSync aux répertoires, vous devez également activer l'accès à toutes les exécutions. Pour vous assurer que le répertoire peut être monté, vconnectez-vous d'abord à n'importe quel ordinateur possédant la même configuration réseau que votre agent. Exécutez ensuite la commande CLI suivante :

```
mount -t nfs -o nfsvers=<your-nfs-server-version> <your-nfs-server-name>:<nfs-export-path-you-specified> <new-test-folder-on-your-computer>
```

Si le problème n'est toujours pas résolu, contactez le AWS Support centre de contact.

Ma tâche a échoué en raison d'une erreur de montage NFS

L'erreur suivante peut s'afficher lors de l'exécution d'une DataSync tâche impliquant un emplacement de serveur de fichiers NFS :

La tâche n'a pas pu accéder à l'emplacement loc-1111222233334444a : x40016 : mount.nfs : le délai de connexion a expiré

Actions à exécuter

Procédez comme suit jusqu'à ce que l'erreur soit résolue.

1. Assurez-vous que le serveur de fichiers NFS et l'exportation que vous spécifiez dans votre DataSync emplacement sont valides. Si ce n'est pas le cas, supprimez votre emplacement et votre tâche, puis créez un nouvel emplacement et une nouvelle tâche utilisant un serveur de fichiers NFS valide et exportez-les. Pour de plus amples informations, veuillez consulter Utilisation de la console DataSync.
2. Vérifiez la configuration de votre pare-feu entre votre agent et le serveur de fichiers NFS. Pour de plus amples informations, veuillez consulter Exigences en matière de réseau pour le stockage sur site, autogéré, dans d'autres environnements dans le cloud et en périphérie.
3. Assurez-vous que votre agent peut accéder au serveur de fichiers NFS et monter l'exportation. Pour de plus amples informations, veuillez consulter Fournir un DataSync accès aux serveurs de fichiers NFS.

4. Si le message d'erreur persiste, ouvrez un canal d'assistance avec Support. Pour de plus amples informations, veuillez consulter Je ne sais pas ce qui se passe avec mon agent. Quelqu'un peut-il m'aider ?.

Ma tâche a échoué en raison d'une erreur de montage Amazon EFS

L'erreur suivante peut s'afficher lors de l'exécution d'une DataSync tâche impliquant un emplacement Amazon EFS :

La tâche n'a pas pu accéder à l'emplacement loc-1111222233334444a : x40016 : Impossible de se connecter à la cible de montage EFS dont l'adresse IP est : 10.10.1.0.

Cela peut se produire si le chemin de montage du système de fichiers Amazon EFS que vous configurez avec votre position est mis à jour ou supprimé. DataSync n'est pas au courant de ces modifications dans le système de fichiers.

Action à exécuter

Supprimez votre emplacement et votre tâche et créez un nouvel emplacement Amazon EFS avec le nouveau chemin de montage.

La propriété des fichiers n'est pas maintenue avec le transfert NFS

Après votre transfert, vous remarquerez peut-être que les fichiers de votre emplacement de DataSync destination ont un utilisateur IDs (UIDs) ou un groupe IDs (GIDs) différent de celui des fichiers de votre emplacement source. Par exemple, les fichiers de votre destination peuvent avoir un UID de `6553499`, `ounobody`.

Cela peut se produire si un système de fichiers impliqué dans votre transfert utilise le mappage d'identifiants NFS version 4, une fonctionnalité qui DataSync n'est pas prise en charge.

Action à exécuter

Plusieurs options s'offrent à vous pour contourner ce problème :

- Créez un nouvel emplacement pour le système de fichiers qui utilise la version 3 de NFS au lieu de la version 4.
- Désactivez le mappage des identifiants NFS version 4 sur le système de fichiers.

Réessayez le transfert. L'une ou l'autre option devrait résoudre le problème.

Ma tâche ne peut pas accéder à un emplacement SMB qui utilise Kerberos

DataSync les erreurs liées aux sites SMB qui utilisent l'authentification Kerberos sont généralement liées à des incohérences entre votre emplacement et les configurations Kerberos. Il se peut également qu'il y ait un problème de réseau.

Impossible d'accéder à l'emplacement

L'erreur suivante indique qu'il existe peut-être des problèmes de configuration liés à votre emplacement SMB ou à la configuration de Kerberos :

```
Task failed to access location
```

Vérifiez les points suivants :

- Le serveur de fichiers SMB que vous spécifiez pour votre emplacement est un nom de domaine. Pour Kerberos, vous ne pouvez pas spécifier l'adresse IP du serveur de fichiers.
- Le principal Kerberos que vous spécifiez pour votre emplacement correspond au principal que vous utilisez pour créer le fichier de table des clés Kerberos (keytab). Les noms principaux distinguent les majuscules et minuscules.
- Le mot de passe utilisateur mappé du principal Kerberos n'a pas changé depuis que vous avez créé le fichier keytab. Si le mot de passe change (en raison de la rotation du mot de passe ou pour toute autre raison), l'exécution de votre tâche risque d'échouer avec l'erreur suivante :

  La tâche n'a pas pu accéder à l'emplacement loc-1111222233334444a : x40015 : kinit : échec de la préauthentification lors de l'obtention des informations d'identification initiales

Impossible de contacter le royaume KDC

L'erreur suivante indique un problème réseau :

```
kinit: Cannot contact any KDC for realm 'MYDOMAIN.ORG' while getting initial
 credentials"
```

Vérifiez les points suivants :

- Le fichier de configuration Kerberos (`krb5.conf`) que vous avez fourni DataSync contient les informations correctes sur votre domaine Kerberos. Pour un exemple de `krb5.conf` fichier, consultez la section Conditions requises pour l'authentification Kerberos.
- Le port du serveur Kerberos Key Distribution Center (KDC) est ouvert. Le port KDC est généralement le port TCP 88.

- La configuration DNS de votre réseau.

Ma tâche a échoué en raison d'une input/output erreur

Un message d' input/output erreur peut s'afficher si votre système de stockage ne répond pas I/O aux demandes de l' DataSync agent. Cela est souvent dû à une panne de disque du serveur, à une modification de la configuration de votre pare-feu ou à une défaillance du routeur réseau.

Si l'erreur concerne un serveur de fichiers NFS ou un cluster Hadoop Distributed File System (HDFS), suivez les étapes ci-dessous pour résoudre l'erreur.

Actions à entreprendre (NFS)

Vérifiez d'abord les journaux et les indicateurs de votre serveur de fichiers NFS pour déterminer si le problème a commencé sur le serveur NFS. Si c'est le cas, résolvez ce problème.

Ensuite, vérifiez que votre configuration réseau n'a pas changé. Pour vérifier si le serveur de fichiers NFS est correctement configuré et qu'il DataSync peut y accéder, procédez comme suit :

1. Configurez un autre client NFS sur le même sous-réseau réseau que l'agent .
2. Montez votre partage sur ce client.
3. Veillez à ce que le client puisse lire et écrire dans le partage avec succès.

Actions à entreprendre (HDFS)

Procédez comme suit jusqu'à ce que l'erreur soit résolue :

1. Assurez-vous que votre cluster HDFS autorise votre DataSync agent à communiquer avec le cluster NameNode et les DataNode ports.

   Dans la plupart des clusters, vous pouvez trouver les numéros de port utilisés par le cluster dans les fichiers de configuration suivants :

   - Pour trouver le NameNode port, consultez le `core-site.xml` fichier sous la `fs.default.name` propriété `fs.default` or (selon la distribution Hadoop).
   - Pour trouver le DataNode port, consultez le `hdfs-site.xml` fichier situé sous la `dfs.datanode.address` propriété.
2. Dans votre `hdfs-site.xml` dossier, vérifiez que votre `dfs.data.transfer.protection` propriété n'a qu'une seule valeur. Par exemple :

```
<property>
   <name>dfs.data.transfer.protection</name>
   <value>privacy</value>
</property>
```

Erreur: `FsS3UnableToConnectToEndpoint`

DataSync Impossible de se connecter à votre site Amazon S3. Cela peut signifier que le compartiment S3 de l'emplacement n'est pas accessible ou que l'emplacement n'est pas configuré correctement.

Procédez comme suit jusqu'à ce que le problème soit résolu :

- Vérifiez si vous DataSync pouvez accéder à votre compartiment S3.
- Assurez-vous que l'emplacement est correctement configuré à l'aide de la DataSync console ou de l'opération DescribeLocationS3.

Erreur: `FsS3HeadBucketFailed`

DataSync ne peut pas accéder au compartiment S3 vers lequel vous effectuez le transfert ou à partir duquel vous effectuez le transfert. Vérifiez DataSync s'il est autorisé à accéder au compartiment à l'aide de l'HeadBucketopération Amazon S3. Si vous devez modifier vos autorisations, consultezFournir DataSync un accès aux compartiments S3.

Échec de la tâche avec une `Unable to list Azure Blobs on the volume root` erreur

Si votre tâche de DataSync transfert échoue en raison d'une `Unable to list Azure Blobs on the volume root` erreur, il se peut qu'il s'agisse d'un problème lié à votre jeton de signature d'accès partagé (SAS) ou au réseau de votre compte de Azure stockage.

Actions à exécuter

Essayez ce qui suit et réexécutez la tâche jusqu'à ce que le problème soit résolu :

- Assurez-vous que votre jeton SAS dispose des autorisations appropriées pour accéder à votreMicrosoft Azure Blob Storage.

- Si vous utilisez votre DataSync agentAzure, configurez votre compte de stockage pour autoriser l'accès depuis le réseau virtuel sur lequel réside votre agent.
- Si vous utilisez votre agent sur Amazon EC2, configurez votre pare-feu Azure de stockage pour autoriser l'accès depuis l'adresse IP publique de l'agent.

Pour plus d'informations sur la configuration du réseau Azure de votre compte de stockage, consultez la Azure Blob Storagedocumentation.

Erreur: `FsAzureBlobVolRootListBlobsFailed`

Le jeton de signature d'accès partagé (SAS) DataSync utilisé pour accéder à votre compte Microsoft Azure Blob Storage ne dispose pas de l'autorisation de liste.

Pour résoudre le problème, mettez à jour votre position à l'aide d'un jeton doté de l'autorisation de liste et réessayez d'exécuter votre tâche.

Erreur: `SrcLocHitAccess`

DataSync Impossible d'accéder à votre emplacement source. Vérifiez qu'il DataSync est autorisé à accéder à l'emplacement et réessayez d'exécuter votre tâche.

Erreur: `SyncTaskErrorLocationNotAdded`

DataSync Impossible d'accéder à votre position. Vérifiez qu'il DataSync est autorisé à accéder à l'emplacement et réessayez d'exécuter votre tâche.

Erreur: `S3 location creation failed with (InvalidRequestException) when calling the CreateLocationS3 operation`

Cette erreur peut être liée aux autorisations IAM, aux politiques relatives aux compartiments Amazon S3, aux AWS KMS autorisations ou à d'autres problèmes d'autorisation. Si cette erreur s'affiche, utilisez les informations suivantes pour résoudre le problème :

- Résolvez les erreurs d'accès refusé (403 Interdit) dans Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service
- Comment résoudre les erreurs 403 Access Denied depuis Amazon S3 ? sur AWS re:Post

La tâche avec l'emplacement source S3 échoue avec **`HeadObject`** ou sans **`GetObjectTagging`** erreur

Si vous transférez des objets dotés d'une version spécifique IDs depuis un compartiment S3, il se peut qu'une erreur liée à `HeadObject` ou s'affiche`GetObjectTagging`. Par exemple, voici une erreur liée à `GetObjectTagging` :

```
[WARN] Failed to read metadata for file /picture1.png (versionId: 111111): S3 Get
 Object Tagging Failed
[ERROR] S3 Exception: op=GetObjectTagging photos/picture1.png, code=403, type=15,
 exception=AccessDenied,
msg=Access Denied req-hdrs: content-type=application/xml, x-amz-api-version=2006-03-01
 rsp-hdrs: content-type=application/xml,
date=Wed, 07 Feb 2024 20:16:14 GMT, server=AmazonS3, transfer-encoding=chunked,
x-amz-id-2=IOWQ4fDEXAMPLEQM+ey7N9WgVhSnQ6JEXAMPLEZb7hSQDASK+Jd1vEXAMPLEa3Km, x-amz-
request-id=79104EXAMPLEB723
```

Si l'une de ces erreurs s'affiche, vérifiez que le rôle IAM DataSync utilisé pour accéder à votre emplacement source S3 dispose des autorisations suivantes :

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

Si vous devez mettre à jour votre rôle avec ces autorisations, consultez[Création d'un rôle IAM pour accéder DataSync à votre position Amazon S3](#).

Résolution des problèmes liés aux DataSync tâches

Utilisez les informations suivantes pour résoudre les problèmes liés aux AWS DataSync tâches et à leur exécution. Ces problèmes peuvent inclure des problèmes de configuration des tâches, des exécutions de tâches bloquées et des données qui ne sont pas transférées comme prévu.

Erreur : SyncOption valeur non valide. Option : TransferModePreserveDeletedFiles, Valeur : TOUT, SUPPRIMER.

Cette erreur se produit lorsque vous créez ou modifiez votre DataSync tâche et que vous sélectionnez l'option Transférer toutes les données et que vous désélectionnez l'option Conserver les fichiers supprimés.

Lorsque vous transférez toutes les données, DataSync il ne scanne pas votre position de destination et ne sait pas quoi supprimer.

L'exécution de la tâche échoue avec une EniNotFounderreur

Cette erreur se produit si vous supprimez l'une des interfaces réseau de votre tâche dans votre cloud privé virtuel (VPC). Si votre tâche est planifiée ou mise en file d'attente, elle échouera s'il manque une interface réseau requise pour transférer vos données.

Actions à exécuter

Pour contourner ce problème, vous disposez des options suivantes :

- Redémarrez la tâche manuellement. Lorsque vous effectuez cette opération, il DataSync créera toutes les interfaces réseau manquantes dont il a besoin pour exécuter la tâche.
- Si vous devez nettoyer les ressources de votre VPC, veillez à ne pas supprimer les interfaces réseau associées à une DataSync tâche que vous utilisez toujours.

  Pour voir les interfaces réseau allouées à votre tâche, effectuez l'une des opérations suivantes :

  - Utilisez l'DescribeTaskopération. Vous pouvez afficher les interfaces réseau dans les éléments de `DestinationNetworkInterfaceArns` réponse `SourceNetworkInterfaceArns` et.
  - Dans la EC2 console Amazon, recherchez votre ID de tâche (tel que`task-f012345678abcdef0`) pour trouver ses interfaces réseau.
- Envisagez de ne pas exécuter vos tâches automatiquement. Cela peut inclure la désactivation de la mise en file d'attente ou de la planification des tâches (par le biais d'une automatisation personnalisée ou par le biais d' DataSync une automatisation personnalisée).

L'exécution de la tâche échoue avec une erreur « Impossible d'allouer de la mémoire »

Lorsque votre DataSync tâche échoue en raison d'une erreur « Impossible d'allouer de la mémoire », cela peut avoir différentes conséquences.

Action à exécuter

Essayez ce qui suit jusqu'à ce que le problème ne s'affiche plus :

- Si votre transfert implique un agent, assurez-vous que celui-ci répond aux exigences relatives à la machine virtuelle (VM) ou à l' EC2 instance Amazon.

- Divisez votre transfert en plusieurs tâches à l'aide de filtres. Il est possible que vous essayiez de transférer un nombre de fichiers ou d'objets supérieur à ce que peut gérer une seule DataSync tâche.
- Si le problème persiste, contactez Support.

La tâche échoue avec **`Input/Output error`** le système de fichiers Amazon FSx for NetApp ONTAP

Lorsque votre DataSync tâche échoue ou que `Input/Output error` vous transférez des données avec un système de fichiers Amazon FSx for NetApp ONTAP, cela peut être dû à un ou plusieurs des problèmes suivants.

- Le volume FSx for ONTAP a atteint sa capacité maximale de fichiers. Cela se produit lorsque le nombre d'inodes ou de pointeurs de fichiers disponibles sur un volume est épuisé.
- Le volume FSx for ONTAP n'a plus de capacité de stockage disponible.
- L'exécution de la DataSync tâche entraînait une trop grande simultanéité de lecture/écriture et consommait un pourcentage très élevé de la capacité de débit du système de fichiers.

Actions à exécuter

Vous pouvez résoudre ce problème en examinant l'état du volume FSx for ONTAP afin d'en déterminer la cause sous-jacente.

Pour déterminer si le volume a atteint sa capacité maximale de fichiers et résoudre le problème :

- Consultez la capacité de fichiers maximale du volume. Pour plus d'informations, consultez la section Surveillance de la capacité de fichiers d'un volume dans le guide de l'utilisateur d'Amazon FSx pour NetApp ONTAP.
- Augmentez la capacité de fichiers du volume en augmentant le nombre d'inodes ou en augmentant la capacité de stockage. Pour plus d'informations, consultez la section Augmenter la capacité maximale de fichiers d'un volume dans le guide de l'utilisateur d'Amazon FSx for NetApp ONTAP.

Pour déterminer si le volume n'a plus de capacité de stockage disponible et résoudre le problème, procédez comme suit :

- Déterminez la capacité de stockage disponible du volume. Pour plus d'informations, reportez-vous à la section Surveillance de la capacité de stockage du volume dans le Guide FSx de l'utilisateur d'ONTAP.

  Si la capacité de stockage disponible du volume est faible ou nulle, vous devez augmenter la capacité de stockage du volume. Pour plus d'informations, consultez la section Augmenter la capacité de stockage d'un volume dans le guide de l'utilisateur FSx pour ONTAP.
- Pour éviter que le problème d'épuisement de la capacité de stockage disponible du volume ne se reproduise, utilisez la fonction de dimensionnement automatique du volume pour augmenter automatiquement la capacité de stockage du volume en fonction des besoins. Pour plus d'informations, consultez la section Utilisation du dimensionnement automatique des volumes dans le guide de l'utilisateur FSx pour ONTAP.

Pour déterminer si l'exécution de la tâche consommait une trop grande partie de la capacité de débit disponible du système de fichiers :

- Surveillez les performances du système de fichiers à l'aide CloudWatch des métriques disponibles. Pour plus d'informations, consultez la section Surveillance des métriques du système de fichiers dans le guide FSx de l'utilisateur d'ONTAP.
- Surveillez le système de fichiers pour détecter les avertissements relatifs aux performances du serveur de fichiers dans la FSx console Amazon. Pour plus d'informations, consultez la section Avertissements et recommandations en matière de performances dans le guide FSx de l'utilisateur d'ONTAP.

Pour résoudre le problème, vous devez vous assurer que cette tâche n'utilise pas toute la capacité de débit disponible du système de fichiers. Procédez comme suit :

- Définissez la limite de bande passante pour l'exécution de la tâche sur une quantité inférieure à la capacité FSx de débit allouée au système de fichiers ONTAP. Pour de plus amples informations, veuillez consulter the section called “Définition des limites de bande passante”.
- Vous pouvez également augmenter la capacité de débit allouée au système de fichiers. Pour plus d'informations, consultez la section Mise à jour de la capacité de débit dans le guide de l'utilisateur FSx pour ONTAP.

Échec de la tâche **`Connection Reset by peer`** ou **`Host is down`** message correspondant au FSx système de fichiers ONTAP

Lorsque votre DataSync tâche échoue avec un `Host is down` message `Connection Reset by peer` ou lors du transfert de données avec un système de fichiers FSx for ONTAP, cela peut être dû à un ou plusieurs des problèmes suivants.

- Le serveur SMB du système de fichiers a été redémarré ou déconnecté pendant l'exécution de la tâche.
- Le système de fichiers est passé du serveur principal au serveur secondaire (et à l'adresse IP) pendant l'exécution de la tâche. DataSync ne prend pas en charge le basculement vers une adresse IP secondaire lors de l'exécution d'une tâche.

  FSx pour le basculement des systèmes de fichiers ONTAP vers un serveur secondaire et une adresse IP lors des événements suivants :

  - Le serveur principal devient indisponible.
  - La zone de disponibilité du serveur principal devient indisponible (pour les systèmes de fichiers multi-AZ).
  - Lors d'une modification de capacité de débit initiée par l'utilisateur.
  - Pendant la période de maintenance régulière du système de fichiers.

  Pour plus d'informations, reportez-vous au processus FSx de basculement ONTAP dans le guide de l'utilisateur FSx d'ONTAP.

Actions à exécuter

Redémarrez la tâche.

L'exécution de la tâche a un statut de lancement mais rien ne semble se passer

Votre DataSync tâche peut rester bloquée avec un statut de lancement, généralement parce que l'agent est hors tension ou a perdu la connectivité réseau.

Action à exécuter

Assurez-vous que le statut de votre agent est EN LIGNE. Si l'agent est HORS LIGNE, assurez-vous qu'il est allumé.

Si l'agent est allumé et que la tâche est toujours en cours de lancement, il y a probablement un problème de connexion réseau entre votre agent et AWS. Pour obtenir des informations sur le test de la connectivité réseau, consultez Vérification de la connexion de votre agent au DataSync service.

Si le problème persiste, consultezJe ne sais pas ce qui se passe avec mon agent. Quelqu'un peut-il m'aider ?.

L'exécution de la tâche semble bloquée dans l'état de préparation

La durée pendant laquelle votre tâche de DataSync transfert passe à l'état Préparation dépend de la quantité de données présentes dans la source et la destination du transfert, ainsi que des performances de ces systèmes de stockage.

Lorsqu'une tâche démarre, DataSync effectue une liste de répertoires récursive pour découvrir tous les fichiers, objets, répertoires et métadonnées de votre source et de votre destination. DataSync utilise ces listes pour identifier les différences entre les systèmes de stockage et déterminer les éléments à copier. Ce processus peut prendre quelques minutes, voire quelques heures.

Action à exécuter

Tu ne devrais pas avoir à faire quoi que ce soit. Continuez à attendre que le statut de la tâche passe à Transfert. Si le statut ne change toujours pas, contactez le AWS Support centre.

L'exécution de la tâche s'arrête avant la fin du transfert

Si l'exécution de votre DataSync tâche s'arrête prématurément, la configuration de votre tâche peut inclure un Région AWS élément désactivé dans votre Compte AWS.

Actions à exécuter

Procédez comme suit pour exécuter à nouveau votre tâche :

1. Vérifiez le statut d'inscription des régions de votre tâche et assurez-vous qu'elles sont activées.
2. Recommencez la tâche.

L'exécution de la tâche échoue lors du transfert depuis un bucket Google Cloud Storage

Comme il DataSync communique avec Google Cloud Storage à l'aide de l'API Amazon S3, il existe une limite qui peut entraîner l'échec de votre DataSync transfert si vous essayez de copier

des balises d'objets. Le message suivant concernant le problème apparaît dans vos CloudWatch journaux :

[WARN] Impossible de lire les métadonnées du fichier/*your-bucket*/*your-object*: S3 Get Object Tagging Echec : poursuite sans balisage

Pour éviter cela, désélectionnez l'option Copier les balises d'objets lors de la configuration des paramètres de vos tâches de transfert.

Il existe des incohérences entre les horodatages de l'exécution des tâches

Lorsque vous consultez la DataSync console ou les CloudWatch journaux Amazon, vous remarquerez peut-être que les heures de début et de fin de l'exécution de vos DataSync tâches ne correspondent pas aux horodatages que vous voyez dans d'autres outils de surveillance. Cela est dû au fait que la console et CloudWatch les journaux prennent en compte le temps passé par l'exécution d'une tâche dans les états de lancement ou de mise en file d'attente, alors que d'autres outils ne le font pas.

Vous remarquerez peut-être cette différence lorsque vous comparez les horodatages d'exécution entre la DataSync console ou les CloudWatch journaux et les emplacements suivants :

- Journaux du système de fichiers impliqué dans votre transfert
- Date de dernière modification sur un objet Amazon S3 qui DataSync a écrit à
- Trafic réseau provenant de l' DataSync agent
- EventBridge Événements Amazon

L'exécution de la tâche échoue avec une **`NoMem`** erreur

L'ensemble de données que vous essayez de transférer est peut-être trop important pour DataSync. Si cette erreur s'affiche, contactez le AWS Support Centre.

L'objet ne parvient pas à être transféré en raison Azure Blob Storage d'une **`user metadata key`** erreur

Lors du transfert d'un compartiment S3 versAzure Blob Storage, le message d'erreur suivant peut s'afficher :

```
[ERROR] Failed to transfer file /user-metadata/file1: Azure Blob user metadata key must
 be a CSharp identifier
```

Cela signifie que cela `/user-metadata/file1` inclut les métadonnées utilisateur qui n'utilisent pas d'identifiant C# valide. Pour plus d'informations, consultez la documentation Microsoft.

Il y a un `/.aws-datasync` dossier dans l'emplacement de destination

DataSync crée un dossier appelé `/.aws-datasync` dans votre emplacement de destination pour faciliter le transfert de données.

Bien que ce dossier soit DataSync généralement supprimé après votre transfert, il se peut que cela ne se produise pas dans certains cas.

Action à exécuter

Supprimez ce dossier à tout moment tant que vous n'avez pas de copie de tâche en cours d'exécution vers cet emplacement.

Impossible de transférer des liens symboliques entre des sites à l'aide du protocole SMB

Lorsque l'exécution de la tâche est terminée, le message d'erreur suivant s'affiche :

```
Transfer and verification completed. Selected files transferred except for files
 skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please
 contact AWS Support for further assistance.
```

Lors du transfert entre des systèmes de stockage SMB (tels qu'un serveur de fichiers SMB et un système de fichiers Amazon FSx pour Windows File Server), les avertissements et erreurs suivants peuvent s'afficher dans vos CloudWatch journaux :

```
[WARN] Failed to read metadata for file /appraiser/symlink: No data available
[ERROR] Failed to read metadata for directory /appraiser/symlink: No data available
```

Action à exécuter

DataSync ne prend pas en charge le transfert de liens symboliques (ou liens physiques) lors du transfert entre ces types de localisation. Pour de plus amples informations, veuillez consulter Liens et répertoires copiés par AWS DataSync.

Erreurs dans les rapports de tâches

Vous pouvez rencontrer l'une des erreurs suivantes lorsque vous essayez de surveiller votre DataSync transfert à l'aide d'un rapport de tâches.

Message d'erreur	Solution
Le chemin du fichier dépasse la longueur maximale de 4 096 caractères. Impossible d'écrire dans le rapport des tâches	N/A (DataSync impossible de transférer un fichier dont le chemin dépasse 4 096 octets) Pour de plus amples informations, veuillez consulter Limites relatives au système de stockage, aux fichiers et aux objets.
Impossible de télécharger le ou les rapports de tâches vers S3 en raison d'un compartiment ou d'un rôle IAM non valide	Vérifiez que le rôle DataSync IAM dispose des autorisations appropriées pour télécharger un rapport de tâches dans votre compartiment S3.
Une erreur d'exécution s'est produite avant la génération de rapports de tâches	Consultez vos CloudWatch journaux pour déterminer pourquoi l'exécution de votre tâche a échoué.

Résolution des problèmes de vérification des données

AWS DataSync Vérifie par défaut l'intégrité de vos données à la fin d'un transfert. Utilisez les informations suivantes pour vous aider à diagnostiquer les erreurs de vérification et les avertissements courants, tels que la modification ou la suppression de fichiers avant la fin de DataSync la vérification de vos données.

En cas de problèmes de vérification, il est souvent utile de consulter vos CloudWatch journaux (ou rapports de tâches) en plus de l'erreur d'exécution des tâches que vous constatez. DataSyncfournit des journaux structurés en JSON pour les tâches en mode amélioré, tandis que les tâches en mode de base ont des journaux non structurés.

Il existe des incohérences entre le contenu d'un fichier

Lorsque l'exécution de la tâche est terminée, le message d'erreur suivant s'affiche :

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

Dans vos CloudWatch journaux, vous remarquerez peut-être des échecs de vérification pour des contenus qui diffèrent entre les emplacements source et de destination. Cela peut se produire si des fichiers sont modifiés lors de votre transfert.

Par exemple, les journaux suivants indiquent `file1.txt` que `mtime` les `srcHash` `dstHash` valeurs et sont différentes :

Exemple de journal en mode de base

```
[NOTICE] Verification failed <> /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt   srcMeta: type=R mode=0755 uid=65534
 gid=65534 size=534528 atime=1633100003/684349800 mtime=1602647222/222919600
 extAttrsHash=0
[NOTICE]   srcHash: 0c506c26bd1e43bd3ac346734f1a9c16c4ad100d1b43c2903772ca894fd24e44
[NOTICE] /directory1/directory2/file1.txt   dstMeta: type=R mode=0755 uid=65534
 gid=65534 size=511001 atime=1633100003/684349800 mtime=1633106855/859227500
 extAttrsHash=0
[NOTICE]   dstHash: dbd798929f11a7c0201e97f7a61191a83b4e010a449dfc79fbb8233801067c46
```

In DataSync, `mtime` représente la dernière fois qu'un fichier a été écrit avant sa préparation. Lors de la vérification des transferts, DataSync compare `mtime` les valeurs entre les emplacements source et de destination. Un tel échec de vérification se produit si le nom `mtime` d'un fichier n'est pas le même pour les deux emplacements. Les différences entre `srcHash` et `dstHash` indiquent que le contenu du fichier ne correspond pas aux deux emplacements.

Actions à exécuter

Procédez comme suit :

1. Utilisez un convertisseur de temps d'époque pour déterminer si le fichier ou l'objet source ou de destination a été modifié plus récemment. Cela peut aider à identifier la version actuelle.
2. Pour éviter que cette erreur ne se reproduise, planifiez l'exécution de votre tâche pendant une fenêtre de maintenance lorsqu'aucune activité n'est enregistrée à la source et à la destination.

Il existe une incompatibilité entre les métadonnées SMB d'un fichier

Lorsque l'exécution de la tâche est terminée, le message d'erreur suivant s'affiche :

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

Lors du transfert entre des systèmes de stockage prenant en charge le protocole SMB (Server Message Block), cette erreur peut s'afficher lorsque les attributs SMB étendus d'un fichier ne correspondent pas entre la source et la destination.

Par exemple, les journaux suivants indiquent que `file1.txt` la `extAttrsHash` valeur varie d'un emplacement à l'autre, indiquant que le contenu du fichier est identique mais que les attributs étendus n'ont pas été définis à la destination :

Exemple de journal en mode de base

```
[NOTICE] Verification failed <> /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt   srcMeta: type=R mode=0755 uid=65534
 gid=65534 size=1469752 atime=1631354985/174924200 mtime=1536995541/986211400
 extAttrsHash=2272191894
[NOTICE]   srcHash: 38571d42b646ac8f4034b7518636b37dd0899c6fc03cdaa8369be6e81a1a2bb5
[NOTICE] /directory1/directory2/file1.txt   dstMeta: type=R mode=0755 uid=65534
 gid=65534 size=1469752 atime=1631354985/174924200 mtime=1536995541/986211400
 extAttrsHash=3051150340
[NOTICE]   dstHash: 38571d42b646ac8f4034b7518636b37dd0899c6fc03cdaa8369be6e81a1a2bb5
```

Un message d'erreur associé à propos des attributs étendus peut également s'afficher :

```
[ERROR] Deferred error: WriteFileExtAttr2 failed to setextattrlist(filename="/
directory1/directory2/file1.txt"): Input/output error
```

Action à exécuter

Cette erreur se produit généralement lorsque les autorisations sont insuffisantes pour copier les listes de contrôle d'accès (ACLs) vers la destination. Pour résoudre ce problème, consultez les guides de configuration suivants en fonction de votre type de destination :

- Autorisations requises FSx pour les systèmes de fichiers Windows File Server

- Autorisations requises FSx pour les systèmes de fichiers ONTAP qui utilisent SMB

Les fichiers à transférer ne se trouvent plus à l'emplacement source

Lorsque l'exécution de la tâche est terminée, le message d'erreur suivant s'affiche :

```
Transfer and verification completed. Selected files transferred except for files
 skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please
 contact AWS Support for further assistance.
```

Dans vos journaux, vous pouvez voir des erreurs indiquant que les fichiers ne se trouvent pas à l'emplacement source. Cela peut se produire si des fichiers (tels que `file1.dll` et`file2.dll`) sont supprimés après leur préparation mais avant leur DataSync transfert :

Exemple de journal en mode de base

```
[ERROR] Failed to open source file /file1.dll: No such file or directory
[ERROR] Failed to open source file /file2.dll: No such file or directory
```

Action à exécuter

Pour éviter ces situations, planifiez l'exécution de votre tâche lorsqu'il n'y a aucune activité à l'emplacement source.

Par exemple, vous pouvez exécuter votre tâche pendant une fenêtre de maintenance lorsque les utilisateurs et les applications ne travaillent pas activement avec cet emplacement.

Dans certains cas, il est possible que les journaux associés à cette erreur ne s'affichent pas. Dans ce cas, contactez le AWS Support centre.

DataSync Impossible de vérifier les données de destination

Lorsque l'exécution de la tâche est terminée, le message d'erreur suivant s'affiche :

```
Transfer and verification completed. Verification detected mismatches. Files with
 mismatches are listed in Cloud Watch Logs
```

Dans vos journaux, vous remarquerez peut-être qu'il n'est pas DataSync possible de vérifier certains dossiers ou fichiers dans l'emplacement de destination. Ces erreurs peuvent ressembler à ceci :

Exemple de journal en mode de base

```
[ERROR] Failed to read metadata for destination file /directory1/directory2/
file1.txt: No such file or directory
```

Pour les fichiers, vous pouvez rencontrer des échecs de vérification comme celui-ci :

Exemple de journal en mode de base

```
[NOTICE] Verification failed <> /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt   srcMeta: type=R mode=0755 uid=65534
 gid=65534 size=61533 atime=1633099987/747713800 mtime=1536995631/894267700
 extAttrsHash=232104771
[NOTICE]   srcHash: 1426fe40f669a7d36cca1b5329983df31a9aeff8eb9fe3ac885f26de2f8fff6b
[NOTICE] /directory1/directory2/file1.txt   dstMeta: type=R mode=0755 uid=65534
 gid=65534 size=0 atime=0/0 mtime=0/0 extAttrsHash=0
[NOTICE]   dstHash: 0000000000000000000000000000000000000000000000000000000000000000
```

Action à exécuter

Ces journaux indiquent que les données de destination ont été supprimées après le transfert mais avant la vérification. (Les journaux se ressemblent lorsque les données sont téléchargées vers un emplacement source au cours de la même période.)

Pour éviter ces situations, planifiez l'exécution de votre tâche lorsqu'il n'y a aucune activité sur le lieu de destination.

Par exemple, vous pouvez exécuter votre tâche pendant une fenêtre de maintenance lorsque les utilisateurs et les applications ne travaillent pas activement avec cet emplacement.

DataSync Impossible de lire les métadonnées des objets

Lorsque l'exécution de la tâche est terminée, le message d'erreur suivant s'affiche :

```
Transfer and verification completed. Selected files transferred except for files
 skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please
 contact AWS Support for further assistance.
```

Dans vos journaux, vous remarquerez peut-être que cela ne DataSync peut pas être lu en `file1.`png raison de l'échec d'une `HeadObject` demande Amazon S3. DataSync effectue

`HeadObject` des demandes auprès des emplacements S3 lors de la préparation et de la vérification des tâches.

Exemple de journal en mode de base

```
[WARN] Failed to read metadata for file /file1.png: S3 Head Object Failed
```

Actions à exécuter

Pour résoudre ce problème, vérifiez si vous DataSync disposez du niveau d'autorisations approprié pour travailler avec votre compartiment S3 :

- Assurez-vous que le rôle IAM DataSync utilisé pour accéder à vos sites Amazon S3 autorise l'`s3:GetObject`autorisation. Pour de plus amples informations, veuillez consulter Autorisations requises.
- Si votre compartiment S3 utilise le chiffrement côté serveur, assurez-vous qu'il DataSync est autorisé à accéder aux objets de ce compartiment. Pour de plus amples informations, veuillez consulter Accès aux compartiments S3 à l'aide du chiffrement côté serveur.

Les métadonnées définies par le système d'un objet ne correspondent pas

Lorsque l'exécution de vos tâches en mode amélioré entre les compartiments S3 est terminée, le message d'erreur suivant s'affiche :

```
Verification failed due to a difference in metadata
```

Il se peut que vous remarquiez dans vos journaux une incohérence dans les métadonnées définies par le système Amazon S3 d'un objet. Dans cet exemple particulier, l'objet source ne possède pas de `Content-Type` métadonnées, mais l'objet de destination en possède. Cela s'est produit parce que le compartiment S3 de destination appliquait automatiquement `"ContentType": "application/octet-stream"` des métadonnées à l'objet lorsqu'il y était DataSync transféré.

Exemple de journal en mode amélioré

```
{
    "Action": "VERIFY",
    "Source": {
        "LocationId": "loc-0b3017fc4ba4a2d8d",
```

```
        "RelativePath": "encoding/content-null",
        "Metadata": {
            "Type": "Object",
            "ContentSize": 24,
            "LastModified": "2024-12-23T15:48:15Z",
            "S3": {
                "SystemMetadata": {
                    "ETag": "\"68b9c323bb846841ee491481f576ed4a\""
                },
                "UserMetadata": {},
                "Tags": {}
            }
        }
    },
    "Destination": {
        "LocationId": "loc-abcdef01234567890",
        "RelativePath": "encoding/content-null",
        "Metadata": {
            "Type": "Object",
            "ContentSize": 24,
            "LastModified": "2024-12-23T16:00:03Z",
            "S3": {
                "SystemMetadata": {
                    "ContentType": "application/octet-stream",
                    "ETag": "\"68b9c323bb846841ee491481f576ed4a\""
                },
                "UserMetadata": {
                    "file-mtime": "1734968895000"
                },
                "Tags": {}
            }
        }
    },
    "TransferType": "CONTENT_AND_METADATA",
    "ErrorCode": "MetadataDiffers",
    "ErrorDetail": "Verification failed due to a difference in metadata"
}
```

Action à exécuter

Pour éviter cette erreur, mettez à jour vos objets de localisation source afin d'inclure la propriété `Content-Type` des métadonnées.

Comprendre la durée de vérification des données

DataSync la vérification inclut une SHA256 somme de contrôle sur le contenu des fichiers et une comparaison exacte des métadonnées des fichiers entre les emplacements. La durée de la vérification dépend de plusieurs facteurs, notamment le nombre de fichiers ou d'objets concernés, la taille des données dans les systèmes de stockage et les performances de ces systèmes.

Action à exécuter

Compte tenu des facteurs qui peuvent affecter le délai de vérification, vous ne devriez rien avoir à faire. Toutefois, si l'exécution de votre tâche semble bloquée avec un statut de vérification, contactez le AWS Support Centre.

Résolution des problèmes liés aux coûts de stockage S3 plus élevés que prévu avec DataSync

Si les coûts de stockage de votre Amazon S3 sont supérieurs à ce que vous pensiez à la suite d'un AWS DataSync transfert, cela peut être dû à une ou plusieurs des raisons suivantes :

- Lors du transfert vers ou depuis des compartiments S3, vous encourez des coûts liés aux demandes d'API S3 effectuées par. DataSync
- DataSync utilise la fonctionnalité de téléchargement partitionné d'Amazon S3 pour charger des objets dans des compartiments S3. Cette approche peut entraîner des frais de stockage inattendus pour les téléchargements qui ne se terminent pas correctement.
- La gestion des versions d'objet peut être activée sur votre compartiment S3. Le versionnement des objets permet à Amazon S3 de stocker plusieurs copies d'objets portant le même nom.

Actions à exécuter

Dans ces cas, vous pouvez procéder comme suit :

- Assurez-vous de bien comprendre comment DataSync les requêtes S3 sont utilisées et comment elles peuvent affecter vos coûts de stockage. Pour de plus amples informations, veuillez consulter Évaluation des coûts des requêtes S3 lors de l'utilisation DataSync.
- Si le problème est lié aux téléchargements partitionnés, configurez une politique de téléchargement partitionné pour votre compartiment S3 afin de nettoyer les téléchargements partitionnés incomplets afin de réduire les coûts de stockage. Pour plus d'informations, consultez le billet de

AWS blog S3 Lifecycle Management Update - Support pour les téléchargements partitionnés et les marqueurs de suppression.

- Si le problème est lié à la gestion des versions d'objets, désactivez la gestion des versions d'objets dans votre compartiment S3.
- Si vous avez besoin d'aide supplémentaire, contactez le AWS Support centre.

AWS DataSync tutoriels

Ces didacticiels vous présentent des scénarios du monde réel avec AWS DataSync.

Rubriques

- Tutoriel : Transfert de données depuis le stockage sur site vers Amazon S3 via Comptes AWS
- Tutoriel : Transférer des données entre des compartiments Amazon S3 Comptes AWS

Tutoriel : Transfert de données depuis le stockage sur site vers Amazon S3 via Comptes AWS

Lorsque vous utilisez AWS DataSync le stockage sur site, vous transférez généralement les données vers un service AWS de stockage qui appartient au même Compte AWS que votre DataSync agent. Il existe toutefois des situations dans lesquelles vous devrez peut-être transférer des données vers un compartiment Amazon S3 associé à un autre compte.

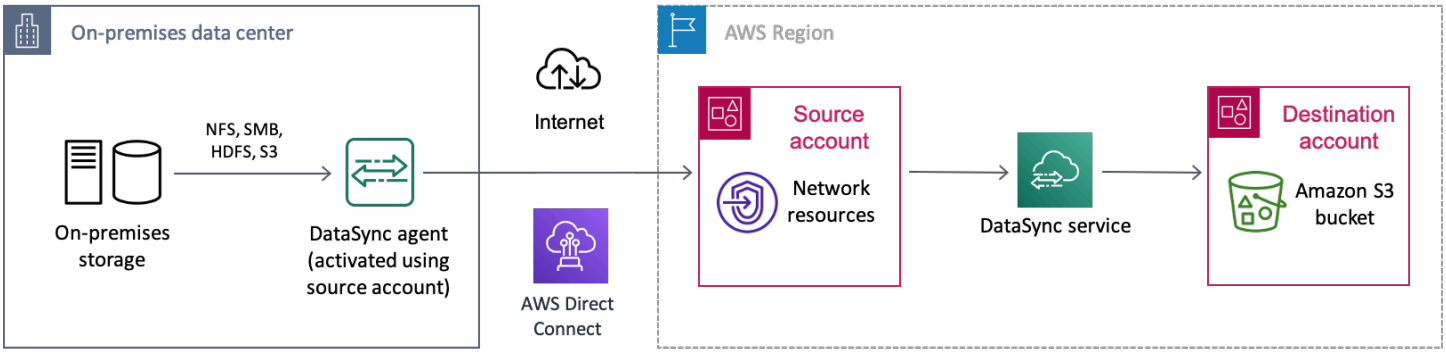
> **Important**
>
> Le transfert de données à Comptes AWS l'aide des méthodes décrites dans ce didacticiel ne fonctionne que lorsque Amazon S3 est l'un des sites de DataSync transfert.

Présentation

Il n'est pas rare de devoir transférer des données entre différents acteurs Comptes AWS, en particulier si vous avez des équipes distinctes qui gèrent les ressources de votre organisation. Voici à quoi DataSync peut ressembler un transfert entre comptes :

- Compte source : Compte AWS pour gérer les ressources du réseau. Il s'agit du compte avec lequel vous activez votre DataSync agent.
- Compte de destination : Compte AWS pour gérer le compartiment S3 vers lequel vous devez transférer des données.

Le schéma suivant illustre ce type de scénario.



Prérequis : autorisations de compte source requises

Pour votre source Compte AWS, deux ensembles d'autorisations doivent être pris en compte pour ce type de transfert entre comptes :

- Autorisations utilisateur qui permettent à un utilisateur de travailler avec DataSync (il peut s'agir de vous ou de votre administrateur de stockage). Ces autorisations vous permettent de créer des DataSync emplacements et des tâches.
- DataSync autorisations de service qui permettent DataSync de transférer des données vers le compartiment de votre compte de destination.

User permissions

Dans votre compte source, ajoutez au moins les autorisations suivantes à un rôle IAM pour créer vos DataSync emplacements et vos tâches. Pour plus d'informations sur la façon d'ajouter des autorisations à un rôle, consultez la section Création ou modification d'un rôle IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SourceUserRolePermissions",
            "Effect": "Allow",
            "Action": [
                "datasync:CreateLocationS3",
                "datasync:CreateTask",
                "datasync:DescribeLocation*",
                "datasync:DescribeTaskExecution",
                "datasync:ListLocations",
                "datasync:ListTaskExecutions",
```

```
                "datasync:DescribeTask",
                "datasync:CancelTaskExecution",
                "datasync:ListTasks",
                "datasync:StartTaskExecution",
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:AttachRolePolicy",
                "iam:ListRoles",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datasync.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

> **Tip**
>
> Pour configurer vos autorisations d'utilisateur, pensez à utiliser AWSDataSyncFullAccess. Il s'agit d'une politique AWS gérée qui fournit à l'utilisateur un accès complet DataSync et un accès minimal à ses dépendances.

DataSync service permissions

Le DataSync service a besoin des autorisations suivantes dans votre compte source pour transférer des données vers le compartiment de votre compte de destination.

Plus loin dans ce didacticiel, vous ajouterez ces autorisations lors de la création d'un rôle IAM pour DataSync. Vous spécifiez également ce rôle (*source-datasync-role*) dans votre politique de compartiment de destination et lors de la création de votre position de DataSync destination.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

Prérequis : autorisations requises pour le compte de destination

Dans votre compte de destination, vos autorisations utilisateur doivent vous permettre de mettre à jour la politique de votre compartiment de destination et de désactiver ses listes de contrôle d'accès (ACLs). Pour plus d'informations sur ces autorisations spécifiques, consultez le guide de l'utilisateur Amazon S3.

Étape 1 : Dans votre compte source, créez un DataSync agent

Pour commencer, vous devez créer un DataSync agent capable de lire depuis votre système de stockage sur site et de communiquer avec le DataSync service. Ce processus inclut le déploiement d'un agent dans votre environnement de stockage sur site et l'activation de l'agent dans votre source Compte AWS.

> **Note**
>
> Les étapes de ce didacticiel s'appliquent à tous les types d'agent et de point de terminaison de service que vous utilisez.

Pour créer un DataSync agent

1. Déployez un DataSync agent dans votre environnement de stockage sur site.
2. Choisissez un point de terminaison de service avec lequel l'agent communiquera AWS.
3. Activez votre agent dans votre compte source.

Étape 2 : dans votre compte source, créez un rôle DataSync IAM pour accéder au compartiment de destination

Dans votre compte source, vous avez besoin d'un rôle IAM qui autorise DataSync le transfert de données vers le compartiment de votre compte de destination.

Comme vous effectuez un transfert entre comptes, vous devez créer le rôle manuellement. (vous DataSync pouvez créer ce rôle dans la console lors du transfert vers le même compte.)

Création du rôle DataSync IAM

Créez un rôle IAM en DataSync tant qu'entité de confiance.

Pour créer le rôle IAM

1. Connectez-vous au AWS Management Console avec votre compte source.
2. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
3. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles, puis sélectionnez Créer un rôle.

4. Sur la page Sélectionner une entité de confiance, pour Type d'entité fiable, sélectionnez Service AWS.
5. Pour Cas d'utilisation, choisissez DataSyncdans la liste déroulante et sélectionnez DataSync. Choisissez Suivant.
6. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant).
7. Donnez un nom à votre rôle et choisissez Créer un rôle.

Pour plus d'informations, consultez la section Création d'un rôle pour une Service AWS (console) dans le guide de l'utilisateur IAM.

Ajouter des autorisations au rôle DataSync IAM

Le rôle IAM que vous venez de créer nécessite les autorisations permettant de transférer des données DataSync vers le compartiment S3 de votre compte de destination.

Pour ajouter des autorisations à votre rôle IAM

1. Sur la page Rôles de la console IAM, recherchez le rôle que vous venez de créer et choisissez son nom.
2. Sur la page de détails du rôle, choisissez l'onglet Autorisations. Choisissez Ajouter des autorisations, puis Créer une politique en ligne.
3. Choisissez l'onglet JSON et procédez comme suit :

   a. Collez le code JSON suivant dans l'éditeur de règles :

> **Note**
>
> La valeur de `aws:ResourceAccount` doit être l'ID de compte qui possède le compartiment Amazon S3 spécifié dans la politique.

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Action": [
             "s3:GetBucketLocation",
             "s3:ListBucket",
```

```
                "s3:ListBucketMultipartUploads"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            "Condition": {
                "StringEquals": {
                 "aws:ResourceAccount": "123456789012"
                }
            }
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectTagging"
              ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "123456789012"
                }
            }
        }
    ]
}
```

b. Remplacez chaque instance de *amzn-s3-demo-destination-bucket* par le nom du compartiment S3 dans votre compte de destination.

4. Choisissez Suivant. Donnez un nom à votre politique et choisissez Create policy.

Étape 3 : dans votre compte de destination, mettez à jour votre politique de compartiment S3

Dans votre compte de destination, modifiez la politique du compartiment S3 de destination pour inclure le rôle DataSync IAM que vous avez créé dans votre compte source.

Avant de commencer : assurez-vous que vous disposez des autorisations requises pour votre compte de destination.

Pour mettre à jour la politique du compartiment S3 de destination

1. Dans le AWS Management Console, passez à votre compte de destination.
2. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
3. Dans le panneau de navigation de gauche, choisissez Compartiments.
4. Dans la liste des compartiments, choisissez le compartiment S3 vers lequel vous transférez les données.
5. Sur la page détaillée du bucket, choisissez l'onglet Permissions.
6. Sous Politique de compartiment, choisissez Modifier et procédez comme suit pour modifier votre politique de compartiment S3 :

   a. Mettez à jour le contenu de l'éditeur pour inclure les déclarations de politique suivantes :

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source-account:role/source-datasync-role"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
```

```
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

b. Remplacez chaque instance de *source-account* par l' Compte AWS ID de votre compte source.

c. *source-datasync-role*Remplacez-le par le rôle IAM que vous avez créé DataSync dans votre compte source.

d. Remplacez chaque instance de *amzn-s3-demo-destination-bucket* par le nom du compartiment S3 dans votre compte de destination.

7. Sélectionnez Enregistrer les modifications.

Étape 4 : Dans votre compte de destination, ACLs désactivez-la pour votre compartiment S3

Il est important que toutes les données que vous copiez dans le compartiment S3 appartiennent à votre compte de destination. Pour vous assurer que ce compte possède les données, désactivez les listes de contrôle d'accès du bucket (ACLs). Pour plus d'informations, consultez la section Contrôle de la propriété des objets et désactivation ACLs de votre compartiment dans le guide de l'utilisateur Amazon S3.

Pour le désactiver ACLs pour votre compartiment de destination

1. Tout en restant connecté à la console S3 avec votre compte de destination, choisissez le compartiment S3 vers lequel vous souhaitez transférer les données.
2. Sur la page détaillée du bucket, choisissez l'onglet Permissions.
3. Sous Object Ownership (Propriétaire de l'objet), sélectionnez Edit (Modifier).
4. Si ce n'est pas déjà fait, choisissez l'option ACLs désactivée (recommandée).
5. Sélectionnez Enregistrer les modifications.

Étape 5 : Dans votre compte source, créez un emplacement DataSync source pour votre stockage sur site

Dans votre compte source, créez un emplacement DataSync source pour le système de stockage sur site à partir duquel vous transférez les données. Cet emplacement utilise l'agent que vous avez activé dans votre compte source.

Étape 6 : Dans votre compte source, créez un emplacement de DataSync destination pour votre compartiment S3

Pendant que vous êtes toujours dans votre compte source, créez un emplacement pour le compartiment S3 vers lequel vous transférez les données.

Avant de commencer : assurez-vous que vous disposez des autorisations requises pour votre compte source.

Comme vous ne pouvez pas créer d'emplacements entre comptes à l'aide de l'interface de DataSync console, ces instructions nécessitent que vous exécutiez une `create-location-s3` commande pour créer votre emplacement de destination. Nous vous recommandons d'exécuter la commande à l'aide AWS CloudShell d'un shell pré-authentifié basé sur un navigateur que vous lancez directement depuis la console. CloudShell vous permet d'exécuter AWS CLI des commandes `create-location-s3` sans télécharger ni installer d'outils de ligne de commande.

> **Note**
>
> Pour effectuer les étapes suivantes à l'aide d'un outil de ligne de commande autre que CloudShell, assurez-vous que votre AWS CLI profil utilise le même rôle IAM qui inclut les autorisations utilisateur requises pour être utilisé DataSync dans votre compte source.

Pour créer un lieu de DataSync destination en utilisant CloudShell

1. Lorsque vous êtes toujours dans votre compte source, effectuez l'une des opérations suivantes pour lancer CloudShell depuis la console :
   - Cliquez sur l' CloudShell icône dans la barre de navigation de la console. Il est situé à droite de la zone de recherche.
   - Utilisez le champ de recherche de la barre de navigation de la console pour rechercher, CloudShellpuis choisissez l'CloudShelloption.

2. Copiez la commande suivante :

```
aws datasync create-location-s3 \
  --s3-bucket-arn arn:aws:s3:::amzn-s3-demo-destination-bucket \
  --s3-config '{
    "BucketAccessRoleArn":"arn:aws:iam::source-user-account:role/source-datasync-role"
  }'
```

3. *amzn-s3-demo-destination-bucket*Remplacez-le par le nom du compartiment S3 dans votre compte de destination.
4. *source-user-account*Remplacez-le par l' Compte AWS identifiant de votre compte source.
5. *source-datasync-role*Remplacez-le par le rôle DataSync IAM que vous avez créé dans votre compte source.
6. Exécutez la commande dans CloudShell.

   Si la commande renvoie un ARN de DataSync localisation similaire à celui-ci, cela signifie que vous avez créé l'emplacement avec succès :

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-abcdef01234567890"
}
```

7. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.

Depuis votre compte source, vous pouvez voir l'emplacement S3 que vous venez de créer pour votre compartiment de comptes de destination.

Étape 7 : Dans votre compte source, créez et lancez votre DataSync tâche

Avant de commencer une DataSync tâche de transfert de vos données, récapitulons ce que vous avez fait jusqu'à présent :

- Dans votre compte source, vous avez créé votre DataSync agent. L'agent peut lire depuis votre système de stockage sur site et communiquer avec le DataSync service.
- Dans votre compte source, vous avez créé un rôle IAM qui permet de transférer des données DataSync vers le compartiment S3 de votre compte de destination.

- Dans votre compte de destination, vous avez configuré votre compartiment S3 afin de DataSync pouvoir y transférer des données.
- Dans votre compte source, vous avez créé les emplacements DataSync source et de destination de votre transfert.

Pour créer et démarrer la DataSync tâche

1. Tout en utilisant la DataSync console de votre compte source, développez Transfert de données dans le volet de navigation de gauche, puis choisissez Tâches et Créer une tâche.
2. Sur la page Configurer l'emplacement de la source, choisissez Choisir un emplacement existant. Choisissez l'emplacement source à partir duquel vous copiez les données (votre stockage sur site), puis Next.
3. Sur la page Configurer l'emplacement de destination, choisissez Choisir un emplacement existant. Choisissez l'emplacement de destination vers lequel vous copiez les données (le compartiment S3 de votre compte de destination), puis Next.
4. Sur la page Configurer les paramètres, nommez la tâche. Le cas échéant, configurez des paramètres supplémentaires, tels que la spécification d'un groupe de CloudWatch journaux Amazon. Choisissez Suivant.
5. Sur la page Révision, passez en revue vos paramètres et choisissez Créer une tâche.
6. Sur la page de détails de la tâche, choisissez Démarrer, puis choisissez l'une des options suivantes :
   - Pour exécuter la tâche sans modification, choisissez Démarrer avec les valeurs par défaut.
   - Pour modifier la tâche avant de l'exécuter, choisissez Démarrer avec des options de remplacement.

Lorsque votre tâche est terminée, vérifiez le compartiment S3 dans votre compte de destination. Vous devriez voir les données qui ont été déplacées depuis votre emplacement source.

Ressources connexes

Pour plus d'informations sur ce que vous avez fait dans ce didacticiel, consultez les rubriques suivantes :

- Création d'un rôle pour une Service AWS (console)
- Modifier une politique de confiance en matière de rôles (console)

- Ajouter une politique de compartiment à l'aide de la console Amazon S3
- Créez un emplacement S3 à l'aide du AWS CLI

Tutoriel : Transférer des données entre des compartiments Amazon S3 Comptes AWS

Avec AWS DataSync, vous pouvez transférer des données entre des compartiments Amazon S3 appartenant à des entités différentes Comptes AWS.

> **Important**
>
> Le transfert de données à Comptes AWS l'aide des méthodes décrites dans ce didacticiel ne fonctionne qu'avec Amazon S3. En outre, ce didacticiel peut vous aider à transférer des données entre des compartiments S3 qui se trouvent également dans des compartiments différents Régions AWS.

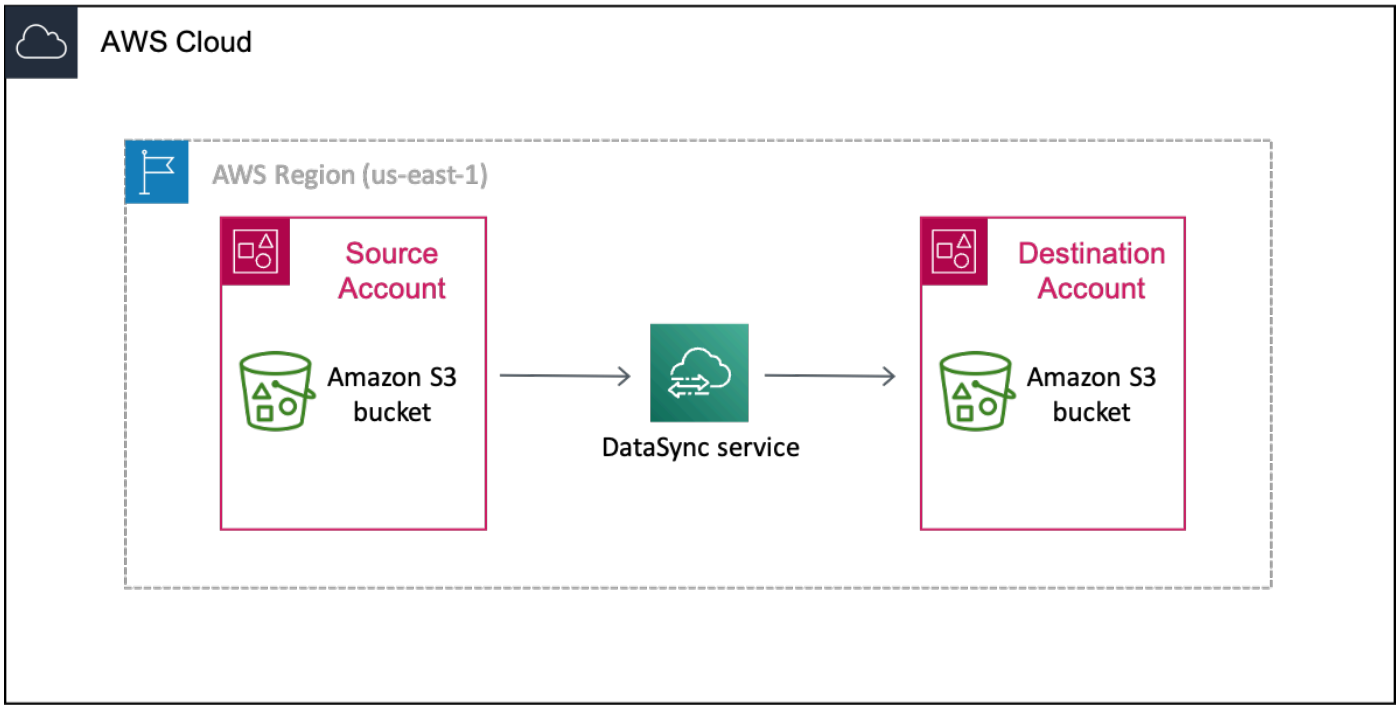
Présentation

Il n'est pas rare de transférer des données entre deux équipes Comptes AWS, en particulier si vous avez des équipes distinctes qui gèrent les ressources de votre organisation. Voici à quoi DataSync peut ressembler un transfert entre comptes :

- Compte source : Compte AWS pour gérer le compartiment S3 à partir duquel vous devez transférer des données.
- Compte de destination : Compte AWS pour gérer le compartiment S3 vers lequel vous devez transférer des données.

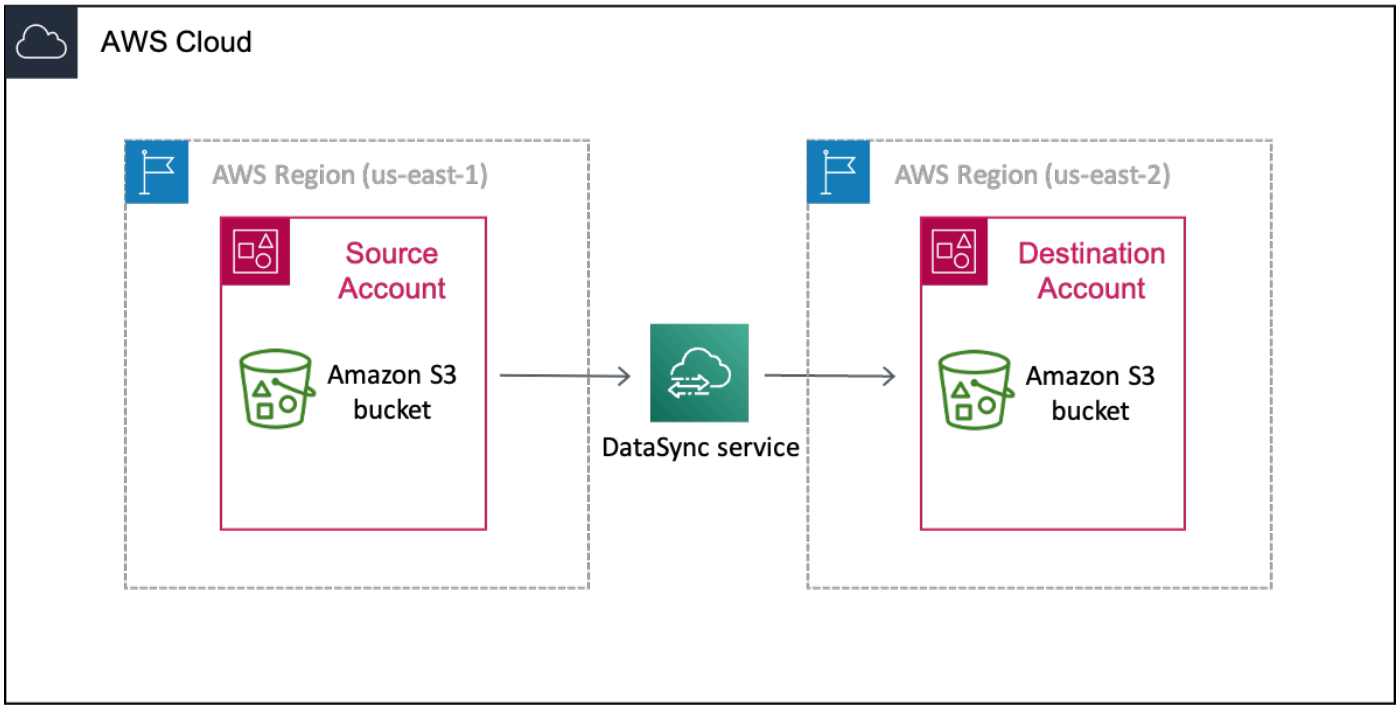
Transfers across accounts

Le schéma suivant illustre un scénario dans lequel vous transférez des données d'un compartiment S3 vers un autre compartiment S3 situé dans un autre Compte AWS.



Transfers across accounts and Regions

Le schéma suivant illustre un scénario dans lequel vous transférez des données d'un compartiment S3 vers un autre compartiment S3 situé dans une région Compte AWS et.



Prérequis : autorisations de compte source requises

Pour votre source Compte AWS, deux ensembles d'autorisations doivent être pris en compte pour ce type de transfert entre comptes :

- Autorisations utilisateur qui permettent à un utilisateur de travailler avec DataSync (il peut s'agir de vous ou de votre administrateur de stockage). Ces autorisations vous permettent de créer des DataSync emplacements et des tâches.
- DataSync autorisations de service qui permettent DataSync de transférer des données vers le compartiment de votre compte de destination.

Autorisations utilisateur pour votre compte source

Dans votre compte source, ajoutez au moins les autorisations suivantes à un rôle IAM pour créer vos DataSync emplacements et vos tâches. Pour plus d'informations sur la façon d'ajouter des autorisations à un rôle, consultez la section Création ou modification d'un rôle IAM.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SourceUserRolePermissions",
            "Effect": "Allow",
            "Action": [
                "datasync:CreateLocationS3",
                "datasync:CreateTask",
                "datasync:DescribeLocation*",
                "datasync:DescribeTaskExecution",
                "datasync:ListLocations",
                "datasync:ListTaskExecutions",
                "datasync:DescribeTask",
                "datasync:CancelTaskExecution",
                "datasync:ListTasks",
                "datasync:StartTaskExecution",
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:AttachRolePolicy",
                "iam:ListRoles",
```

```
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "datasync.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

> **Tip**
>
> Pour configurer vos autorisations d'utilisateur, pensez à utiliser AWSDataSyncFullAccess. Il s'agit d'une politique AWS gérée qui fournit à l'utilisateur un accès complet DataSync et un accès minimal à ses dépendances.

DataSync autorisations de service pour votre compte source

Le DataSync service a besoin des autorisations suivantes dans votre compte source pour transférer des données vers le compartiment de votre compte de destination.

Plus loin dans ce didacticiel, vous ajouterez ces autorisations lors de la création d'un rôle IAM pour DataSync. Vous spécifiez également ce rôle (`source-datasync-role`) dans votre politique de compartiment de destination et lors de la création de votre position de DataSync destination.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

Prérequis : autorisations requises pour le compte de destination

Dans votre compte de destination, vos autorisations utilisateur doivent vous permettre de mettre à jour la politique de votre compartiment de destination et de désactiver ses listes de contrôle d'accès (ACLs). Pour plus d'informations sur ces autorisations spécifiques, consultez le guide de l'utilisateur Amazon S3.

Étape 1 : dans votre compte source, créez un rôle DataSync IAM pour accéder au compartiment de destination

Dans votre source Compte AWS, vous avez besoin d'un rôle IAM qui autorise DataSync le transfert de données vers le bucket de votre compte de destination.

Comme vous effectuez un transfert entre comptes, vous devez créer le rôle manuellement. (vous DataSync pouvez créer ce rôle dans la console lors du transfert vers le même compte.)

Création du rôle DataSync IAM

Créez un rôle IAM en DataSync tant qu'entité de confiance.

1. Connectez-vous au AWS Management Console avec votre compte source.
2. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
3. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles, puis sélectionnez Créer un rôle.
4. Sur la page Sélectionner une entité de confiance, pour Type d'entité fiable, sélectionnez Service AWS.
5. Pour Cas d'utilisation, choisissez DataSyncdans la liste déroulante et sélectionnez DataSync. Choisissez Suivant.
6. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant).
7. Donnez un nom à votre rôle et choisissez Créer un rôle.

Pour plus d'informations, consultez la section Création d'un rôle pour une Service AWS (console) dans le guide de l'utilisateur IAM.

Ajouter des autorisations au rôle DataSync IAM

Le rôle IAM que vous venez de créer nécessite les autorisations permettant de transférer des données DataSync vers le compartiment S3 de votre compte de destination.

1. Sur la page Rôles de la console IAM, recherchez le rôle que vous venez de créer et choisissez son nom.
2. Sur la page de détails du rôle, choisissez l'onglet Autorisations. Choisissez Ajouter des autorisations, puis Créer une politique en ligne.
3. Choisissez l'onglet JSON et procédez comme suit :

a. Collez le code JSON suivant dans l'éditeur de règles :

> **Note**
>
> La valeur de `aws:ResourceAccount` doit être l'ID de compte qui possède le compartiment Amazon S3 spécifié dans la politique.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Action": [
             "s3:GetBucketLocation",
             "s3:ListBucket",
             "s3:ListBucketMultipartUploads"
         ],
         "Effect": "Allow",
         "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
         "Condition": {
             "StringEquals": {
              "aws:ResourceAccount": "123456789012"
             }
         }
     },
     {
         "Action": [
             "s3:AbortMultipartUpload",
             "s3:DeleteObject",
             "s3:GetObject",
             "s3:GetObjectTagging",
             "s3:GetObjectVersion",
             "s3:GetObjectVersionTagging",
             "s3:ListMultipartUploadParts",
             "s3:PutObject",
             "s3:PutObjectTagging"
           ],
         "Effect": "Allow",
         "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "123456789012"
                }
            }
        }
    ]
}
```

b. Remplacez chaque instance de *amzn-s3-demo-destination-bucket* par le nom du compartiment S3 dans votre compte de destination.

4. Choisissez Suivant. Donnez un nom à votre politique et choisissez Create policy.

Étape 2 : dans votre compte de destination, mettez à jour votre politique de compartiment S3

Dans votre compte de destination, modifiez la politique du compartiment S3 de destination pour inclure le rôle DataSync IAM que vous avez créé dans votre compte source.

Avant de commencer : assurez-vous que vous disposez des autorisations requises pour votre compte de destination.

Mettez à jour votre politique de compartiment S3 de destination

1. Dans le AWS Management Console, passez à votre compte de destination.
2. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
3. Dans le panneau de navigation de gauche, choisissez Compartiments.
4. Dans la liste des compartiments, choisissez le compartiment S3 vers lequel vous transférez les données.
5. Sur la page détaillée du bucket, choisissez l'onglet Permissions.
6. Sous Politique de compartiment, choisissez Modifier et procédez comme suit pour modifier votre politique de compartiment S3 :

   a. Mettez à jour le contenu de l'éditeur pour inclure les déclarations de politique suivantes :

```
{
  "Version": "2008-10-17",
  "Statement": [
```

```
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source-account:role/source-datasync-role"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

b. Remplacez chaque instance de *source-account* par l' Compte AWS ID de votre compte source.

c. *source-datasync-role*Remplacez-le par le rôle IAM que vous avez créé DataSync dans votre compte source.

d. Remplacez chaque instance de *amzn-s3-demo-destination-bucket* par le nom du compartiment S3 dans votre compte de destination.

7. Sélectionnez Enregistrer les modifications.

Étape 3 : dans votre compte de destination, ACLs désactivez-la pour votre compartiment S3

Il est important que toutes les données que vous transférez vers le compartiment S3 appartiennent à votre compte de destination. Pour vous assurer que ce compte possède les données, désactivez les listes de contrôle d'accès du bucket (ACLs). Pour plus d'informations, consultez la section Contrôle

de la propriété des objets et désactivation ACLs de votre compartiment dans le guide de l'utilisateur Amazon S3.

Avant de commencer : assurez-vous que vous disposez des autorisations requises pour votre compte de destination.

Désactivez votre compartiment S3 de destination ACLs

1. Tout en restant connecté à la console S3 avec votre compte de destination, choisissez le compartiment S3 vers lequel vous souhaitez transférer les données.
2. Sur la page détaillée du bucket, choisissez l'onglet Permissions.
3. Sous Object Ownership (Propriétaire de l'objet), sélectionnez Edit (Modifier).
4. Si ce n'est pas déjà fait, choisissez l'option ACLs désactivée (recommandée).
5. Sélectionnez Enregistrer les modifications.

Étape 4 : Dans votre compte source, créez vos DataSync emplacements

Dans votre compte source, créez les DataSync emplacements pour vos compartiments S3 source et de destination.

Avant de commencer : assurez-vous que vous disposez des autorisations requises pour votre compte source.

Créez votre emplacement DataSync source

- Dans votre compte source, créez un emplacement pour le compartiment S3 à partir duquel vous transférez les données.

Créez votre DataSync lieu de destination

Pendant que vous êtes toujours dans votre compte source, créez un emplacement pour le compartiment S3 vers lequel vous transférez les données.

Comme vous ne pouvez pas créer d'emplacements entre comptes à l'aide de l'interface de DataSync console, ces instructions nécessitent que vous exécutiez une `create-location-s3` commande pour créer votre emplacement de destination. Nous vous recommandons d'exécuter la commande à l'aide AWS CloudShell d'un shell pré-authentifié basé sur un navigateur que vous

lancez directement depuis la console. CloudShellvous permet d'exécuter AWS CLI des commandes `create-location-s3` sans télécharger ni installer d'outils de ligne de commande.

> **Note**
>
> Pour effectuer les étapes suivantes à l'aide d'un outil de ligne de commande autre que CloudShell, assurez-vous que votre AWS CLI profil utilise le même rôle IAM qui inclut les autorisations utilisateur requises pour être utilisé DataSync dans votre compte source.

Pour créer un lieu de DataSync destination en utilisant CloudShell

1. Lorsque vous êtes toujours dans votre compte source, effectuez l'une des opérations suivantes pour lancer CloudShell depuis la console :
   - Cliquez sur l' CloudShell icône dans la barre de navigation de la console. Il est situé à droite de la zone de recherche.
   - Utilisez le champ de recherche de la barre de navigation de la console pour rechercher, CloudShellpuis choisissez l'CloudShelloption.
2. Copiez la `create-location-s3` commande suivante :

```
aws datasync create-location-s3 \
  --s3-bucket-arn arn:aws:s3:::amzn-s3-demo-destination-bucket \
  --region amzn-s3-demo-destination-bucket-region \
  --s3-config '{
    "BucketAccessRoleArn":"arn:aws:iam::source-account-id:role/source-datasync-
role"
  }'
```

3. *`amzn-s3-demo-destination-bucket`*Remplacez-le par le nom du compartiment S3 dans votre compte de destination.
4. Si votre compartiment de destination se trouve dans une région différente de celle de votre compartiment source, remplacez-le *`amzn-s3-demo-destination-bucket-region`* par la région dans laquelle réside le compartiment de destination (par exemple,*`us-east-2`*). Supprimez cette option si vos buckets se trouvent dans la même région.
5. Remplacez *`source-account-id`* par l' Compte AWS ID source.
6. *`source-datasync-role`*Remplacez-le par le rôle DataSync IAM que vous avez créé dans votre compte source.

7. Exécutez la commande dans CloudShell.

   Si la commande renvoie un ARN de DataSync localisation similaire à celui-ci, cela signifie que vous avez créé l'emplacement avec succès :

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
abcdef01234567890"
}
```

8. Dans le volet de navigation de gauche, développez Transfert de données, puis choisissez Locations.
9. Si vous avez créé l'emplacement dans une autre région, sélectionnez cette région dans le volet de navigation.

Depuis votre compte source, vous pouvez voir l'emplacement S3 que vous venez de créer pour votre compartiment de comptes de destination.

Étape 5 : Dans votre compte source, créez et lancez votre DataSync tâche

Avant de commencer DataSync à transférer vos données, récapitulons ce que vous avez fait jusqu'à présent :

- Dans votre compte source, vous avez créé un rôle IAM qui permet de transférer des données DataSync vers le compartiment S3 de votre compte de destination.
- Dans votre compte de destination, vous avez configuré votre compartiment S3 afin de DataSync pouvoir y transférer des données.
- Dans votre compte source, vous avez créé les emplacements DataSync source et de destination de votre transfert.

Créez et lancez votre DataSync tâche

1. Tout en utilisant la DataSync console de votre compte source, développez Transfert de données dans le volet de navigation de gauche, puis choisissez Tâches et Créer une tâche.
2. Si le compartiment de votre compte de destination se trouve dans une région différente de celle du compartiment de votre compte source, choisissez la région du compartiment de destination dans le volet de navigation supérieur.

> **Important**
>
> Pour éviter une erreur de connexion réseau, vous devez créer votre DataSync tâche dans la même région que l'emplacement de destination.

3. Sur la page Configurer l'emplacement de la source, procédez comme suit :
   a. Sélectionnez Choisir un emplacement existant.
   b. (Pour les transferts entre régions) Dans le menu déroulant Région, choisissez la région dans laquelle réside le compartiment source.
   c. Pour les emplacements existants, choisissez l'emplacement source du compartiment S3 à partir duquel vous transférez les données, puis choisissez Next.
4. Sur la page Configurer l'emplacement de destination, procédez comme suit :
   a. Sélectionnez Choisir un emplacement existant.
   b. Pour les emplacements existants, choisissez l'emplacement de destination du compartiment S3 vers lequel vous transférez les données, puis choisissez Next.
5. Sur la page Configurer les paramètres, choisissez un mode Tâche.

> **Tip**
>
> Nous vous recommandons d'utiliser le mode amélioré. Pour de plus amples informations, veuillez consulter Choix d'un mode de tâche pour le transfert de données.

6. Donnez un nom à la tâche et configurez des paramètres supplémentaires, tels que la spécification d'un groupe de CloudWatch journaux Amazon. Choisissez Suivant.
7. Sur la page Révision, passez en revue vos paramètres et choisissez Créer une tâche.
8. Sur la page de détails de la tâche, choisissez Démarrer, puis choisissez l'une des options suivantes :
   - Pour exécuter la tâche sans modification, choisissez Démarrer avec les valeurs par défaut.
   - Pour modifier la tâche avant de l'exécuter, choisissez Démarrer avec des options de remplacement.

Lorsque votre tâche est terminée, vérifiez le compartiment S3 dans votre compte de destination. Vous devriez voir les données qui ont été déplacées depuis le compartiment de votre compte source.

Résolution des problèmes

Consultez les informations suivantes si vous rencontrez des problèmes lors de la tentative de transfert entre comptes.

Erreurs de connexion

Lors du transfert entre des buckets S3 situés dans différentes régions Comptes AWS et des tâches en mode Basic, il est possible que vous obteniez une erreur de connexion réseau au démarrage de votre DataSync tâche. Pour résoudre ce problème, utilisez une tâche en mode amélioré. Vous pouvez également créer une tâche en mode de base dans la même région que votre destination et essayer d'exécuter cette tâche.

Connexe : transferts entre comptes avec des compartiments S3 utilisant le chiffrement côté serveur

Si vous essayez d'effectuer ce transfert avec des compartiments S3 à l'aide du chiffrement côté serveur, consultez le blog sur le AWS stockage pour obtenir des instructions.

Effectuer une migration de données volumineuse avec AWS DataSync

Les migrations de données à grande échelle peuvent impliquer le transfert de volumes importants de données comprenant des millions de fichiers ou d'objets de différents formats. AWS DataSync simplifie ces transferts complexes en gérant la planification, la surveillance, le chiffrement et la vérification des données.

Qu'est-ce qu'une migration de données volumineuse ?

Une migration de données de grande envergure implique généralement le transfert de téraoctets ou plus de données réparties entre différentes sources vers un nouvel environnement de stockage de destination (dans ce cas, AWS). Ces migrations nécessitent une planification et une coordination minutieuses au sein de votre organisation afin de transférer les données avec succès tout en minimisant les interruptions d'activité.

DataSync peut simplifier ces migrations, qui sont généralement de nature complexe. Parmi les avantages de l'utilisation DataSync pour votre migration, citons :

- Gestion automatisée des processus de transfert de données et de l'infrastructure requise pour des transferts de données performants et sécurisés.
- End-to-end sécurité, y compris le chiffrement et la validation de l'intégrité des données, pour garantir que vos données arrivent en toute sécurité, intactes et prêtes à être utilisées.
- Un protocole réseau spécialement conçu et une architecture parallèle et multithread pour accélérer les migrations.

Les étapes clés d'une migration de données volumineuses

Vous pouvez généralement décomposer une migration de grande envergure selon les étapes suivantes :

- (Étape 1) Planification de la migration des données - À ce stade, vous essayez de comprendre pourquoi vous effectuez la migration et sur quel type de données vous travaillez. Les activités de planification incluent :
  - Comprendre pourquoi vous souhaitez effectuer une migration

  - Constituer une équipe pour vous aider dans tous les aspects de la migration.
  - Identification des emplacements, des formats et des modèles d'utilisation des données
  - Évaluation des ressources matérielles disponibles et des exigences réseau (si vous migrez depuis un centre de données sur site)
  - Exécution de tests de preuve de concept (POC) DataSync pour estimer les délais de migration, planifier les périodes de transition et avoir une idée de la manière dont vous devez configurer DataSync
- (Étape 2) Mise en œuvre de votre migration de données volumineuses - À ce stade, vous validez votre plan et commencez la migration. Les activités de mise en œuvre incluent :
  - Validation du plan de migration
  - Exécution de découpes progressives qui incluent la surveillance et la vérification de vos transferts de données comme prévu
  - Optimisation et ajustement selon les besoins entre chaque découpage
  - Nettoyer les ressources inutilisées une fois que vous avez terminé

Ressources supplémentaires

AWS Prescriptive Guidance propose les ressources suivantes qui peuvent vous aider à planifier et à mettre en œuvre une migration de grande envergure. Utilisez ce guide pour comprendre comment cela DataSync peut fonctionner dans le contexte de processus et d'activités de migration courants.

- Migrations importantes vers le AWS cloud
- Stratégie et meilleures pratiques pour les AWS grandes migrations
- Migrer des systèmes de fichiers partagés dans le cadre d'une migration de AWS grande envergure — Cette ressource inclut un classeur SFS-Discovery-Workbook que vous pouvez télécharger et utiliser pour planifier une migration au niveau du partage de fichiers.

Étape 1 : Planification de la migration de vos données volumineuses

La planification est essentielle lors de la migration d'un ensemble de données volumineux. Vous devez comprendre les données que vous migrez, les motivations qui ont motivé la migration et comment vous AWS DataSync pouvez les acheminer là où vous le souhaitez.

Rubriques

- Collecte des exigences relatives à votre migration
- Exécution d'une DataSync preuve de concept
- Estimation des délais de migration

Collecte des exigences relatives à votre migration

La première étape d'une migration de données à grande échelle nécessite la collecte de diverses informations au sein de votre organisation.

Ces informations vous aident à créer un processus de migration qui, pour les migrations de grande envergure, peut inclure plusieurs transferts et des procédures de découpage des opérations (effectuées par vagues) de votre stockage source vers votre stockage de destination.

Comprendre pourquoi vous souhaitez effectuer une migration

Avant de commencer à migrer vers AWS, vous devez clairement comprendre pourquoi vous migrez vos données. Cela permet de relever les défis courants liés à la migration, tels que le respect des délais, la gestion des ressources et la coordination entre les équipes.

Si vous avez besoin d'aide pour déterminer les motivations de votre migration, répondez aux questions suivantes :

- Libérez-vous de l'espace de stockage sur site ?
- Respectez-vous les délais des contrats de support matériel ?
- Est-ce pour une sortie de centre de données ?
- Quel est votre calendrier de migration ?
- Transférez-vous des données depuis un autre espace de stockage dans le cloud ?
- Vous migrez des ensembles de données partiels ou complets ?
- Est-ce pour l'archivage des données ?
- Les applications ou les utilisateurs ont-ils besoin d'un accès régulier à ces données ?

Comprendre la logistique

Répondez à certaines questions de logistique de base concernant votre environnement de stockage, la migration et votre organisation :

1. Obtenez une compréhension de base de votre infrastructure de stockage de données actuelle.
2. Vérifiez si vous avez besoin d'un DataSync agent. Par exemple, vous avez besoin d'un agent si vous effectuez un transfert depuis un stockage sur site.
3. Si vous avez besoin d'un agent, assurez-vous de bien comprendre les exigences de l'agent :
   - Un agent peut s'exécuter en tant que machine virtuelle (VM) VMware ESXi, machine virtuelle basée sur le noyau Linux (KVM) et hyperviseurs Microsoft Hyper-V. Vous pouvez également déployer un agent en tant qu' EC2 instance Amazon au sein de AWS.
   - Les migrations de grande envergure nécessitent généralement beaucoup de mémoire. Assurez-vous que votre agent dispose de suffisamment de RAM.
4. Identifiez les principales parties prenantes, issues de vos services de direction, de réseau, de stockage et informatiques, qui doivent participer à la migration. Cela peut inclure :
   - Trouvez un leader à fil unique qui se consacre au projet et à ses résultats.
   - Déterminez qui est responsable de la propriété et de la classification des données que vous migrez.
   - Identifiez qui gère votre source et qui, à terme, gérera le service AWS de stockage vers lequel vous migrez.
   - Découvrez qui créera et gérera tout autre processus pour vos données une fois qu'elles seront enregistrées AWS.
5. Établissez des canaux de communication interservices.
6. Créez un plan d'annulation pour les imprévus.
7. Documentez l'ensemble du processus de migration, y compris les procédures relatives aux vagues, à la validation et au transfert. Utilisez-le comme runbook pour l'ensemble de la migration. Vous mettrez à jour ce processus au fur et à mesure de la planification et de la mise en œuvre de la migration.

Révision des données que vous êtes en train de migrer

Collaborez avec vos équipes chargées du stockage et des applications pour analyser les caractéristiques des données que vous souhaitez migrer. Ces informations vous aident à déterminer une stratégie de migration que vous pouvez exécuter DataSync.

Table des matières

- Déterminer les modèles d'utilisation des données

- Identifier la structure et la mise en page des données
- Documenter les partages et les dossiers
- Analyse de la taille des fichiers

Déterminer les modèles d'utilisation des données

- Pour les données utilisées activement et fréquemment modifiées, planifiez plusieurs vagues de transferts incrémentiels afin de ne pas perturber les opérations commerciales.
- Pour les données en lecture seule qui peuvent être considérées comme archivistiques, vous n'avez peut-être pas besoin de planifier les vagues.
- Si vous avez plusieurs modèles d'utilisation des données, planifiez des vagues qui migrent ces différents ensembles de données séparément. Par exemple, vous pouvez avoir une vague pour les données d'archive, le reste étant dédié à la migration des données actives.

Identifier la structure et la mise en page des données

- Déterminez si les données sont organisées par périodes (année, mois, jour) ou par d'autres modèles.
- Utilisez cette structure organisationnelle pour planifier vos vagues de migration. Par exemple, vous pouvez migrer l'équivalent d'un an de données d'archives au cours d'une seule vague.

Documenter les partages et les dossiers

- Créez un inventaire des partages et des dossiers (y compris le nombre de fichiers ou d'objets pour chacun).
- Identifiez les partages et les dossiers contenant des ensembles de données actifs. Cela peut nécessiter des transferts progressifs lors de la migration.
- Passez en revue les DataSync quotas. Cela peut vous aider à planifier la manière de partitionner votre ensemble de données lors de la configuration DataSync.

Analyse de la taille des fichiers

- Attendez-vous à un débit de données plus élevé pour les transferts de fichiers volumineux (Mo ou Go) par rapport à des fichiers plus petits (Ko).

- Si vous travaillez avec de nombreux fichiers de petite taille, attendez-vous à davantage d'opérations de métadonnées sur votre système de stockage et à une baisse du débit de données. DataSynceffectue ces opérations lors de la comparaison et de la vérification de vos emplacements source et de destination.

Identification des besoins de stockage

Pour choisir un service AWS de stockage compatible pour migrer vos données, vous devez évaluer les caractéristiques et les performances de votre système de stockage source.

Ces informations peuvent également vous aider à planifier vos transferts afin de minimiser l'impact sur les opérations commerciales pendant la migration.

Table des matières

- Détermination de la prise en charge du stockage source
- Révision des exigences de conservation des métadonnées
- Collecte de mesures de performance à partir du stockage source
- Choix d'un service AWS de stockage de destination

Détermination de la prise en charge du stockage source

DataSync peut fonctionner avec divers systèmes de stockage qui autorisent l'accès via des clients de stockage d'objets compatibles NFS, SMB, HDFS et S3.

Si vous migrez depuis un autre espace de stockage dans le cloud, vérifiez que DataSync celui-ci peut fonctionner avec ce fournisseur. Pour obtenir la liste des emplacements sources pris en charge, voir Où puis-je transférer mes données AWS DataSync ?

Révision des exigences de conservation des métadonnées

DataSync peut conserver les métadonnées de votre fichier ou de votre objet lors d'un transfert. La façon dont vos métadonnées sont préservées dépend des lieux de transfert et de l'utilisation de types de métadonnées similaires par ces emplacements.

DataSync nécessite dans certains cas des autorisations supplémentaires pour préserver les métadonnées des fichiers, telles que les listes d'accès discrétionnaires NTFS ()DACLs.

Pour de plus amples informations, veuillez consulter Comprendre le mode de DataSync gestion des métadonnées des fichiers et des objets.

Collecte de mesures de performance à partir du stockage source

Mesurez les IOPS de référence et le débit du disque pendant les charges de travail moyennes et maximales de votre stockage source. Le transfert de données alourdit les E/S de vos systèmes de stockage source et de destination.

Comparez ces données de performances aux spécifications de votre système de stockage afin de déterminer les ressources de performance disponibles.

Choix d'un service AWS de stockage de destination

À ce stade, vous avez peut-être une idée du service AWS de stockage le plus adapté à vos données. Si ce n'est pas le cas, les modèles d'utilisation des données et les performances de stockage sont deux aspects à prendre en compte au moment de prendre une décision. Par exemple, vous pouvez envisager Amazon S3 si vous avez des données d'archives et Amazon FSx ou Amazon EFS pour les données actives.

Pour vous aider à choisir le stockage basé sur des objets ou des fichiers adapté à vos données, consultez la section Choix d'un service AWS de stockage.

Déterminer les exigences du réseau

Pour migrer vos données avec DataSync, vous devez établir des connexions réseau entre votre stockage source, votre agent et AWS. Vous devez également prévoir une bande passante et une infrastructure réseau suffisantes.

Collaborez avec vos ingénieurs réseau et vos administrateurs de stockage pour déterminer les exigences réseau suivantes.

Table des matières

- Évaluation de la bande passante réseau disponible
- Examen des options pour connecter votre réseau à AWS
- Choix d'un point de terminaison de service pour la communication entre agents
- Planification d'une infrastructure réseau suffisante

Évaluation de la bande passante réseau disponible

La bande passante réseau disponible influe sur les vitesses de transfert et le temps de migration global. Si vous effectuez un transfert depuis un système de stockage sur site, procédez comme suit :

- Collaborez avec votre équipe réseau pour déterminer l'utilisation moyenne et maximale de la bande passante.
- Identifiez les fenêtres dans lesquelles vous pouvez transférer des données et évitez de perturber les opérations quotidiennes. Cela vous indiquera quand vos vagues de migration et vos ruptures se produiront.

Vous pouvez contrôler la quantité de bande passante DataSync utilisée. Pour de plus amples informations, veuillez consulter Définition des limites de bande passante pour votre AWS DataSync tâche.

Étant donné que les transferts depuis d'autres systèmes de stockage dans le cloud se font généralement via l'Internet public, ces transferts sont généralement moins soumis à des restrictions de bande passante et à des considérations moins importantes.

Examen des options pour connecter votre réseau à AWS

Envisagez les options suivantes pour établir une connectivité réseau pour votre DataSync transfert :

- AWS Direct Connect- Passez en revue l'architecture et les exemples de routage relatifs à l'utilisation de Direct Connect avec DataSync. Vous pouvez surveiller l'activité de Direct Connect à l'aide d'Amazon CloudWatch.
- VPN : AWS Site-to-Site VPNoffre un débit allant jusqu'à 1,25 Gbit/s par tunnel.
- Internet public : contactez votre fournisseur de services Internet pour obtenir des données sur l'utilisation du réseau.

Choix d'un point de terminaison de service pour la communication entre agents

DataSync les agents utilisent des points de terminaison de service pour communiquer avec le DataSync service. Le type de point de terminaison que vous utilisez dépend de la manière dont vous vous connectez à votre réseau AWS.

Planification d'une infrastructure réseau suffisante

Pour chaque tâche de transfert que vous créez, génère et gère DataSync automatiquement l'infrastructure réseau pour vos transferts de données. Cette infrastructure est connue sous le nom d'interfaces réseau ou interfaces réseau élastiques, qui sont des composants réseau logiques dans un cloud privé virtuel (VPC) Amazon qui représentent des cartes réseau virtuelles. Pour plus d'informations, consultez le guide de EC2 l'utilisateur Amazon.

Chaque interface réseau utilise une adresse IP unique dans votre sous-réseau VPC de destination. Pour vous assurer que vous disposez d'une infrastructure réseau suffisante pour effectuer votre migration, procédez comme suit :

- Notez le nombre d'interfaces réseau qui DataSync seront créées pour votre position de DataSync destination.
- Assurez-vous que votre sous-réseau possède suffisamment d'adresses IP pour vos DataSync tâches. Par exemple, une tâche qui utilise un agent nécessite quatre adresses IP. Si vous créez quatre tâches pour votre migration, cela signifie que vous avez besoin de 16 adresses IP disponibles dans votre sous-réseau.

Exécution d'une DataSync preuve de concept

L'exécution d'une preuve de concept (POC) vous AWS DataSync aide à valider les aspects suivants de la planification de votre migration de données :

- Vérifiez la connectivité réseau entre les emplacements source et de destination.
- Validez la configuration initiale de vos DataSync tâches.
- Mesurez les performances de transfert de données.
- Estimez les délais de migration.
- Définissez les critères de réussite avec les principales parties prenantes travaillant sur la migration.

Commencer avec votre preuve de concept

1. Créez votre DataSync agent :
    1. Déployez votre agent.
    2. Choisissez un point de terminaison de service pour votre agent.
    3. Activez votre agent.
    4. Vérifiez les connexions réseau de votre agent.
2. Sélectionnez un petit sous-ensemble de données représentant les données que vous êtes en train de migrer.

    Par exemple, si votre stockage source contient à la fois de gros et de petits fichiers, le sous-ensemble de données que vous transférez dans votre POC doit en tenir compte. Cela vous

donne une idée préliminaire des performances des systèmes de stockage, de votre réseau et DataSync.

3. Créez un emplacement DataSync source pour votre système de stockage sur site ou dans le cloud.
4. Créez un emplacement de DataSync destination pour votre service AWS de stockage.
5. Créez une tâche DataSync de transfert avec un filtre qui transfère uniquement votre sous-ensemble de données.
6. Commencez votre DataSync tâche.
7. Collectez les indicateurs de performance des transferts en surveillant les éléments suivants :
   - Débit de données et de fichiers liés à l'exécution de vos tâches. Vous pouvez le faire par le biais de la DataSync console ou de l'DescribeTaskExecutionopération. Si vous utilisez`DescribeTaskExecution`, voici comment vous calculez ces mesures :
     - Débit de données : Diviser `BytesWritten` par `TransferDuration`
     - Débit de fichiers : Diviser `FilesTransferred` par `TransferDuration`
   - Utilisation du stockage à la source et à la destination. Travaillez en étroite collaboration avec vos administrateurs de stockage pour obtenir ces informations.
   - Utilisation du réseau
8. Vérifiez les données transférées sur votre lieu de destination :
   - Consultez vos CloudWatch journaux pour détecter les erreurs d'exécution des tâches.
   - Vérifiez que les autorisations et les métadonnées sont préservées à l'emplacement de destination.
   - Vérifiez que les applications et les utilisateurs peuvent accéder aux données de destination comme prévu.
   - Résolvez tous les problèmes que vous rencontrez. Pour de plus amples informations, veuillez consulter AWS DataSync Problèmes de résolution des problèmes.
9. Exécutez votre tâche plusieurs fois pour avoir une idée du temps nécessaire à la préparation, DataSync au transfert et à la vérification de vos données. (Pour plus d'informations, consultez Statuts d'exécution des tâches.)

   Si vous exécutez une tâche plusieurs fois, effectue DataSync par défaut un transfert incrémentiel et copie uniquement les données modifiées par rapport à l'exécution de la tâche précédente.

Bien que le temps de transfert soit probablement plus court pour les transferts progressifs, DataSync nous préparerons toujours votre transfert de la même manière en scannant et en comparant vos emplacements pour identifier les éléments à transférer. Vous pouvez utiliser ces temps de préparation pour estimer les délais de transition de votre migration.

10. Si nécessaire, mettez à jour votre plan de migration en fonction de ce que vous avez appris au cours du POC.

Estimation des délais de migration

À l'aide des informations que vous avez collectées jusqu'à présent, vous pouvez estimer la durée de la migration AWS DataSync.

Estimation des délais de transfert de données

Vous pouvez estimer le temps nécessaire DataSync au transfert de vos données sur la base des informations suivantes que vous avez collectées lors de la collecte des exigences de migration et de votre DataSync preuve de concept (POC) :

- Votre bande passante réseau disponible
- Mesures d'utilisation du stockage source et de destination
- Indicateurs de performance issus de votre DataSync POC

Pour estimer un calendrier de transfert de données

1. Comparez le débit de données et de fichiers de votre POC avec la bande passante réseau disponible.
2. Si votre débit est inférieur à la bande passante disponible (par exemple 300 Mo/s pour le débit avec 10 Gbit/s de bande passante réseau), envisagez de partitionner votre ensemble de données en plusieurs tâches afin de maximiser l'utilisation de la bande passante.

   DataSync propose quelques options pour partitionner votre ensemble de données. Pour de plus amples informations, veuillez consulter Accélérer votre migration grâce au partitionnement des données.
3. Calculez le nombre de jours nécessaires à un transfert à l'aide de la formule suivante, qui fournit une durée de transfert minimale théorique :

```
(DATA_SIZE * 8 bits per byte)/(CIRCUIT * NETWORK_UTILIZATION percentage * 3600
 seconds per hour * AVAILABLE_HOURS) = Number of days
```

Lorsque vous utilisez cette formule, remplacez les valeurs suivantes par vos propres valeurs :

- `DATA_SIZE`: quantité de données que vous êtes en train de migrer (exprimée en octets).
- `CIRCUIT`: votre bande passante réseau disponible (exprimée en bits par seconde).
- `NETWORK_UTILIZATION`: quel est le pourcentage de votre réseau utilisé ?
- `AVAILABLE_HOURS`: Le nombre d'heures opérationnelles disponibles par jour.

Par exemple, vous pouvez calculer une migration avec 100 To de données, une connexion Internet de 1 Gbit/s, 80 % d'utilisation du réseau et une disponibilité 24 heures sur 24 comme suit :

```
(100,000,000,000,000 bytes * 8) / (1,000,000,000 bps * 0.80 * 3600 *
24) = 11.57 days
```

Dans ce cas, la migration prendrait près de 12 jours avant de prendre en compte les conditions réelles.

4. Ajustez la durée de transfert calculée pour tenir compte des conditions réelles :
   - Fluctuations des performances du réseau
   - Variations des performances de stockage
   - Temps d'arrêt entre les vagues de migration

Estimation des délais de transition

Si vous migrez des ensembles de données actifs, vous aurez probablement besoin de transferts afin de ne pas perturber les opérations commerciales.

Ne sous-estimez pas le temps que prennent les transferts. Dans le cas de migrations de grande envergure, il n'est pas rare que les activités de transition prennent jusqu'à 30 % du temps total de migration.

1. Déterminez si vous devez effectuer des découpes par vagues afin de réduire la quantité de données numérisées pour des modifications incrémentielles.

Pour ce faire, l'une des stratégies consiste à supprimer les ensembles de données que vous partitionnez en fonction de partages, de dossiers ou de systèmes de stockage.

2. Vérifiez le temps généralement nécessaire DataSync à la préparation, au transfert et à la vérification de vos données pendant le POC.

   Notez en particulier les durées de préparation des exécutions de vos tâches. Pour obtenir ces informations, exécutez l'DescribeTaskExecutionopération, puis vérifiez la valeur de PrepareDurationpendant la durée (en millisecondes).

3. Estimez le temps que peut prendre une transition en mesurant le delta temporel entre les tâches parallèles.

   Pour plus d'informations sur les tâches parallèles, consultezAccélérer votre migration grâce au partitionnement des données.

4. Utilisez votre estimation des ruptures pour planifier vos ruptures. Il s'agit essentiellement de fenêtres de maintenance pendant lesquelles vos données sources ne peuvent pas être modifiées.

Étapes suivantes

Après avoir estimé vos délais, vous êtes prêt à commencer à mettre en œuvre votre migration.

Étape 2 : Implémentation de votre migration de données volumineuses

Grâce aux informations que vous avez recueillies lors de la planification, vous pouvez commencer à les utiliser AWS DataSync pour effectuer la migration vers votre nouveau système de stockage. Si ce n'est pas déjà fait, nous vous recommandons de consulter les ressources d'orientation AWS prescriptive pour les migrations de grande envergure.

Rubriques

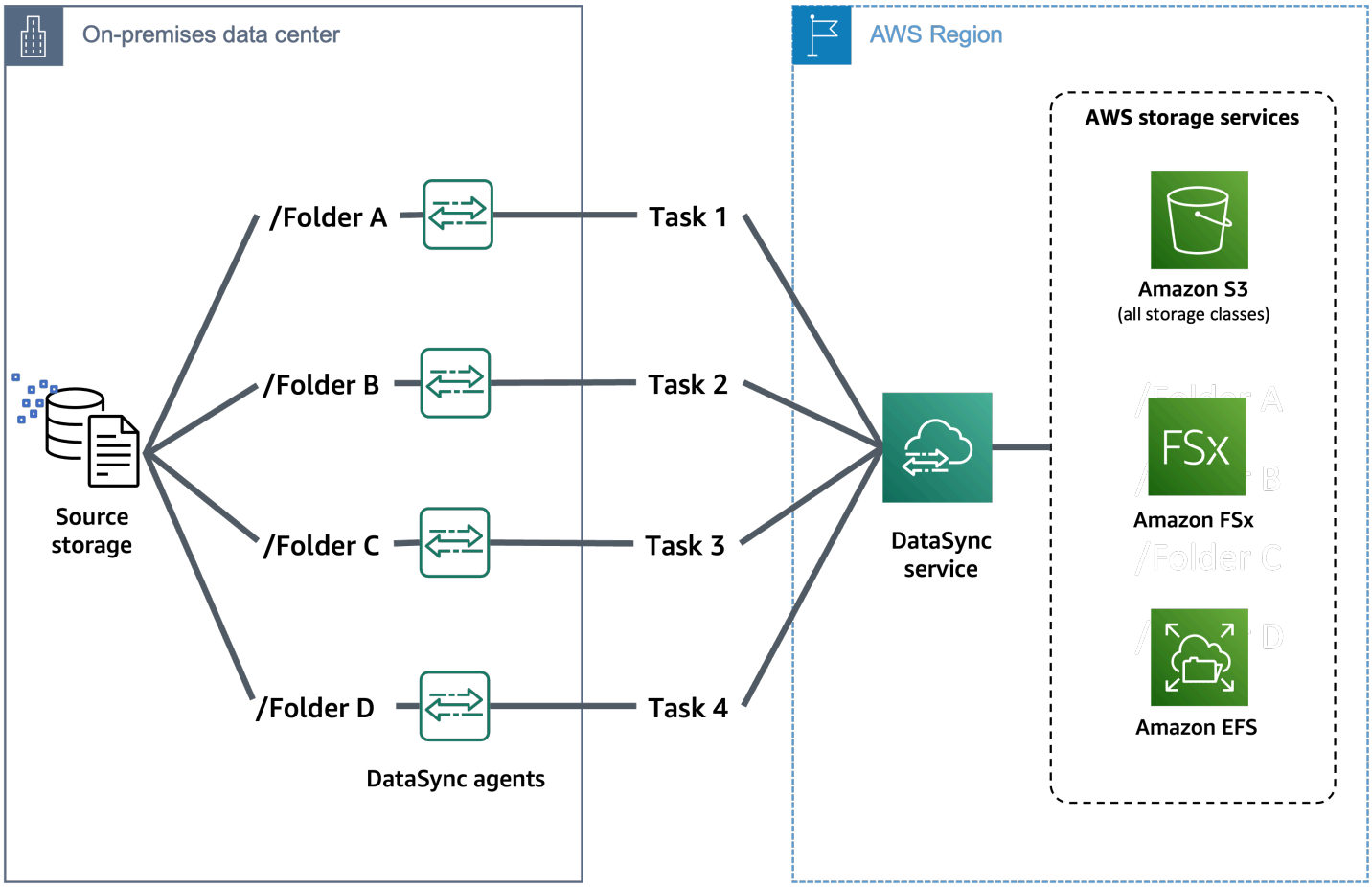
- Accélérer votre migration grâce au partitionnement des données
- Exécution de vos tâches DataSync de transfert
- Surveillance de vos transferts

Accélérer votre migration grâce au partitionnement des données

Dans le cas d'une migration importante, nous vous recommandons de partitionner votre ensemble de données en plusieurs DataSync tâches. Le partitionnement de vos données sources entre plusieurs tâches (et éventuellement des agents) vous permet de paralléliser vos transferts et de réduire le calendrier de migration.

Le partitionnement vous aide également à respecter les DataSync quotas et simplifie la surveillance et le débogage de vos tâches.

Le schéma suivant montre comment vous pouvez utiliser plusieurs DataSync tâches et agents pour transférer des données depuis le même emplacement de stockage source. Dans ce scénario, chaque tâche se concentre sur un dossier spécifique dans l'emplacement source. Pour plus d'informations et des exemples sur ces approches, consultez Comment accélérer vos transferts de données grâce à des architectures AWS DataSync évolutives.



Partitionnement de votre jeu de données par dossier ou par préfixe

Lorsque vous créez votre emplacement DataSync source, vous pouvez spécifier un dossier, un répertoire ou un préfixe dont la DataSync lecture est extraite. Par exemple, si vous migrez un partage de fichiers contenant des répertoires de premier niveau, vous pouvez créer plusieurs emplacements qui spécifient un chemin de répertoire différent. Vous pouvez ensuite utiliser ces emplacements pour exécuter plusieurs DataSync tâches au cours de votre migration.

Partitionnement de votre jeu de données à l'aide de filtres

Vous pouvez appliquer des filtres pour inclure ou exclure des données de votre emplacement source lors d'un transfert. Dans le contexte d'une migration de grande envergure, les filtres peuvent vous aider à étendre les tâches à des parties spécifiques de votre ensemble de données.

Par exemple, si vous migrez des données d'archives organisées par année, vous pouvez créer un filtre d'inclusion correspondant à une année spécifique ou à plusieurs années. Vous pouvez également modifier le filtre chaque fois que vous exécutez la tâche pour qu'il corresponde à une année différente.

Partitionnement de votre jeu de données avec des manifestes

Un manifeste est une liste de fichiers ou d'objets que vous DataSync souhaitez transférer. Avec un manifeste, DataSync il n'est pas nécessaire de tout lire dans un emplacement source pour déterminer ce qu'il faut transférer.

Vous pouvez créer des manifestes à partir des inventaires de votre stockage source ou à l'aide d'approches axées sur les événements (par exemple, voir Implémentation AWS DataSync avec des centaines de millions d'objets). Vous pouvez également utiliser un manifeste différent chaque fois que vous démarrez une tâche, ce qui vous permet de transférer différents ensembles de données avec la même tâche.

Exécution de vos tâches DataSync de transfert

Au cours de chacune de vos vagues de migration, le transfert de données suit généralement le même processus général :

1. Effectuez un premier transfert complet de vos données.
2. Vérifiez les données dans la destination.
3. Exécutez des transferts incrémentiels pour toutes les données susceptibles d'avoir changé depuis le transfert initial.

4. Réduisez les opérations jusqu'à votre destination.
5. Passez en revue les résultats de la transition.

Exécution de vos tâches

Vous devrez probablement exécuter vos tâches de DataSync transfert pendant les heures ouvrables afin de minimiser le temps total de migration. Dans ces situations, il est courant d'exécuter un transfert complet initial suivi de transferts incrémentiels qui tiennent compte des modifications apportées à votre emplacement source par les utilisateurs et les applications.

Pour éviter les problèmes liés au réseau pendant les heures de bureau, vous pouvez limiter la quantité de bande passante utilisée par vos tâches. Pour de plus amples informations, veuillez consulter Définition des limites de bande passante pour votre AWS DataSync tâche.

1. Exécutez un transfert complet initial :
   a. Démarrez votre DataSync tâche (ou vos tâches si vous les exécutez en parallèle).
   b. Surveillez la progression et les performances de l'exécution de vos tâches.
   c. Vérifiez que vos données ont été transférées comme prévu (par exemple, les métadonnées des fichiers sont préservées).
2. Exécutez des transferts incrémentiels :
   a. Planifiez vos tâches pour qu'elles s'exécutent régulièrement.
   b. Surveillez l'exécution de vos tâches et corrigez les erreurs éventuelles.

Exécution d'un cutover

Après vos transferts initiaux et progressifs, vous pouvez commencer le processus de transfert des opérations vers votre destination.

1. Démarrez la fenêtre de maintenance planifiée.
2. Mettez à jour votre système de stockage source pour qu'il soit en lecture seule pour les applications et les utilisateurs.
3. Exécutez les derniers transferts incrémentiels pour copier les deltas restants entre vos emplacements source et de destination.
4. Procédez à une validation approfondie des données (par exemple, en examinant CloudWatch les journaux et les rapports de tâches).

5. Basculez vos applications et vos utilisateurs vers le nouvel environnement de votre lieu de destination.
6. Testez les fonctionnalités de l'application et assurez-vous que les utilisateurs peuvent accéder aux données sur votre lieu de destination.
7. Planifiez une réunion rétrospective pour examiner le transfert avec les équipes de migration. Posez les exemples de questions exploratoires suivants :
   - La transition a-t-elle été un succès ? Si ce n'est pas le cas, quel était le problème ?
   - Avons-nous utilisé toute la bande passante disponible ?
   - Le stockage source et de destination a-t-il été pleinement utilisé ?
   - Pouvons-nous augmenter le débit de données grâce à des tâches supplémentaires ?
   - Devons-nous prévoir une période de maintenance plus longue ?
8. Si nécessaire, mettez à jour votre plan de migration avant de passer à la vague suivante.

Surveillance de vos transferts

AWS DataSync propose plusieurs options de surveillance pour vous aider à valider et à débuguer votre transfert.

Surveillance de vos transferts à l'aide de CloudWatch métriques

Vous pouvez créer des CloudWatch tableaux de bord personnalisés avec des indicateurs issus de l'exécution de vos DataSync tâches. Pour de plus amples informations, veuillez consulter Surveillance des transferts de données avec Amazon CloudWatch Metrics.

Surveillance de vos transferts à l'aide de rapports de tâches

Si vous transférez des millions de fichiers ou d'objets, envisagez d'utiliser des rapports de tâches. Les rapports de tâches fournissent des informations détaillées sur les DataSync tentatives de transfert, d'omission, de vérification et de suppression au cours de l'exécution d'une tâche. Pour de plus amples informations, veuillez consulter Surveillance de vos transferts de données à l'aide de rapports de tâches.

Vous pouvez également visualiser vos rapports de tâches à l'aide de AWS services tels qu' AWS Glue Amazon Athena et Amazon. QuickSight Pour plus d'informations, consultez le blog sur le AWS stockage.

Surveillance de vos transferts avec CloudWatch Logs

Nous vous recommandons au minimum de configurer votre tâche de manière à consigner les informations de base et les erreurs de transfert. Pour de plus amples informations, Surveillance des transferts de données avec Amazon CloudWatch Logsconsultez .

AWS DataSync API

Outre le AWS Management Console et AWS CLI, vous pouvez utiliser l' AWS DataSync API pour configurer et gérer DataSync avec le AWS SDKs.

Rubriques

- Actions
- Types de données
- Erreurs courantes
- Paramètres communs

Actions

Les actions suivantes sont prises en charge :

- CancelTaskExecution
- CreateAgent
- CreateLocationAzureBlob
- CreateLocationEfs
- CreateLocationFsxLustre
- CreateLocationFsxOntap
- CreateLocationFsxOpenZfs
- CreateLocationFsxWindows
- CreateLocationHdfs
- CreateLocationNfs
- CreateLocationObjectStorage
- CreateLocationS3
- CreateLocationSmb
- CreateTask
- DeleteAgent
- DeleteLocation
- DeleteTask

- DescribeAgent
- DescribeLocationAzureBlob
- DescribeLocationEfs
- DescribeLocationFsxLustre
- DescribeLocationFsxOntap
- DescribeLocationFsxOpenZfs
- DescribeLocationFsxWindows
- DescribeLocationHdfs
- DescribeLocationNfs
- DescribeLocationObjectStorage
- DescribeLocationS3
- DescribeLocationSmb
- DescribeTask
- DescribeTaskExecution
- ListAgents
- ListLocations
- ListTagsForResource
- ListTaskExecutions
- ListTasks
- StartTaskExecution
- TagResource
- UntagResource
- UpdateAgent
- UpdateLocationAzureBlob
- UpdateLocationEfs
- UpdateLocationFsxLustre
- UpdateLocationFsxOntap
- UpdateLocationFsxOpenZfs
- UpdateLocationFsxWindows
- UpdateLocationHdfs

- UpdateLocationNfs
- UpdateLocationObjectStorage
- UpdateLocationS3
- UpdateLocationSmb
- UpdateTask
- UpdateTaskExecution

CancelTaskExecution

Arrête l'exécution d'une AWS DataSync tâche en cours. Le transfert de certains fichiers est brusquement interrompu. Le contenu des fichiers transférés vers la destination peut être incomplet ou ne pas correspondre aux fichiers source.

Toutefois, si vous lancez l'exécution d'une nouvelle tâche en utilisant la même tâche et que vous la laissez se terminer, le contenu du fichier de destination sera complet et cohérent. Cela s'applique aux autres défaillances inattendues qui interrompent l'exécution d'une tâche. Dans tous ces cas, le transfert est terminé DataSync avec succès lorsque vous lancez l'exécution de la tâche suivante.

Syntaxe de la requête

```
{
   "TaskExecutionArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

TaskExecutionArn

Nom de ressource Amazon (ARN) de l'exécution de la tâche à arrêter.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateAgent

Active un AWS DataSync agent que vous déployez dans votre environnement de stockage. Le processus d'activation associe l'agent à votre Compte AWS.

Si vous n'avez pas encore déployé d'agent, consultez la section Ai-je besoin d'un DataSync agent ?

Syntaxe de la requête

```
{
   "ActivationKey": "string",
   "AgentName": "string",
   "SecurityGroupArns": [ "string" ],
   "SubnetArns": [ "string" ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "VpcEndpointId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

ActivationKey

Spécifie la clé d'activation de votre DataSync agent. Si vous n'avez pas de clé d'activation, consultez la section Activation de votre agent.

Type : String

Contraintes de longueur : longueur maximale de 29.

Modèle : `[A-Z0-9]{5}(-[A-Z0-9]{5}){4}`

Obligatoire : oui

AgentName

Spécifie le nom de votre agent. Nous vous recommandons de spécifier un nom dont vous vous souviendrez.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatoire : non

SecurityGroupArns

Spécifie le nom de ressource Amazon (ARN) du groupe de sécurité qui autorise le trafic entre votre agent et le point de terminaison du service VPC. Vous ne pouvez spécifier qu'un seul ARN.

Type : tableau de chaînes

Membres du tableau : nombre fixe de 1 élément.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obligatoire : non

SubnetArns

Spécifie l'ARN du sous-réseau où se trouve le point de terminaison de votre service VPC. Vous ne pouvez spécifier qu'un seul ARN.

Type : tableau de chaînes

Membres du tableau : nombre fixe de 1 élément.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/.*$`

Obligatoire : non

Tags

Spécifie des étiquettes qui vous aident à classer, filtrer et rechercher vos AWS ressources. Nous vous recommandons de créer au moins un tag pour votre agent.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

VpcEndpointId

Spécifie l'ID du point de terminaison du service VPC que vous utilisez. Par exemple, un identifiant de point de terminaison VPC ressemble à. `vpce-01234d5aff67890e1`

> **Important**
>
> Le point de terminaison du service VPC que vous utilisez doit inclure le nom du DataSync service (par exemple,`com.amazonaws.us-east-2.datasync`).

Type : String

Modèle : `^vpce-[0-9a-f]{17}$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "AgentArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AgentArn

L'ARN de l'agent que vous venez d'activer. Utilisez cette ListAgentsopération pour renvoyer une liste d'agents dans votre Compte AWS et Région AWS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande

L'exemple suivant active un DataSync agent.

```
{
    "ActivationKey": "AAAAA-1AAAA-BB1CC-33333-EEEEE",
    "AgentName": "MyAgent",
    "Tags": [{
        "Key": "Job",
        "Value": "TransferJob-1"
    }]
```

```
}
```

Exemple de réponse

La réponse renvoie l'ARN de l'agent activé.

```
{
    "AgentArn": "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44baca3"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationAzureBlob

Crée un emplacement de transfert pour un conteneur Microsoft Azure Blob Storage. AWS DataSync peut utiliser cet emplacement comme source ou destination de transfert. Vous pouvez effectuer des transferts avec ou sans DataSync agent connecté à votre conteneur.

Avant de commencer, assurez-vous de savoir comment DataSync accéder à Azure Blob Storage et comment utiliser les niveaux d'accès et les types de blob.

Syntaxe de la requête

```
{
   "AccessTier": "string",
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlobType": "string",
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "ContainerUrl": "string",
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "SasConfiguration": {
      "Token": "string"
   },
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AccessTier

Spécifie le niveau d'accès vers lequel vous souhaitez transférer vos objets ou fichiers. Cela s'applique uniquement lorsque l'emplacement est utilisé comme destination de transfert. Pour plus d'informations, consultez la section Niveaux d'accès.

Type : String

Valeurs valides : `HOT | COOL | ARCHIVE`

Obligatoire : non

AgentArns

(Facultatif) Spécifie le nom de ressource Amazon (ARN) de l' DataSync agent qui peut se connecter à votre conteneur Azure Blob Storage. Si vous configurez un transfert cross-cloud sans agent, il n'est pas nécessaire de spécifier une valeur pour ce paramètre.

Vous pouvez spécifier plusieurs agents. Pour plus d'informations, consultez la section Utilisation de plusieurs agents pour votre transfert.

> **Note**
>
> Assurez-vous de configurer correctement ce paramètre lorsque vous créez votre emplacement de stockage pour la première fois. Il est impossible d'ajouter ou de supprimer des agents d'un emplacement de stockage après l'avoir créé.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : non

AuthenticationType

Spécifie la méthode d'authentification DataSync utilisée pour accéder à votre Azure Blob Storage. DataSync peut accéder au stockage blob à l'aide d'une signature d'accès partagé (SAS).

Type : String

Valeurs valides : `SAS | NONE`

Obligatoire : oui

BlobType

Spécifie le type de blob que vous souhaitez attribuer à vos objets ou fichiers lorsque vous les transférez dans Azure Blob Storage. Actuellement, DataSync ne prend en charge le transfert de données vers Azure Blob Storage que sous forme de blobs de blocs. Pour plus d'informations sur les types de blob, consultez la documentation Azure Blob Storage.

Type : String

Valeurs valides : `BLOCK`

Obligatoire : non

CmkSecretConfig

Spécifie les informations de configuration pour un secret DataSync géré, qui inclut le jeton d'authentification DataSync utilisé pour accéder à un emplacement de AzureBlob stockage spécifique, avec un code géré par le client AWS KMS key.

Lorsque vous incluez ce paramètre dans le cadre d'une `CreateLocationAzureBlob` demande, vous ne fournissez que l'ARN de la clé KMS. DataSync utilise cette clé KMS avec le jeton d'authentification que vous spécifiez `SasConfiguration` pour créer un secret DataSync géré afin de stocker les informations d'accès à la localisation.

Assurez-vous qu' DataSync il est autorisé à accéder à la clé KMS que vous spécifiez.

> **Note**
>
> Vous pouvez utiliser `CmkSecretConfig` (avec`SasConfiguration`) ou `CustomSecretConfig` (sans`SasConfiguration`) pour fournir des informations d'identification pour une `CreateLocationAzureBlob` demande. Ne fournissez pas les deux paramètres pour la même demande.

Type : objet CmkSecretConfig

Obligatoire : non

ContainerUrl

Spécifie l'URL du conteneur Azure Blob Storage impliqué dans votre transfert.

Type : String

Contraintes de longueur : longueur maximale de 325.

Modèle : `^https:\/\/[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}\/[a-z0-9](-?[a-z0-9]){2,62}$`

Obligatoire : oui

CustomSecretConfig

Spécifie les informations de configuration d'un secret du Gestionnaire de Secrets Manager géré par le client dans lequel le jeton d'authentification d'un emplacement AzureBlob de stockage est stocké en texte brut. Cette configuration inclut l'ARN secret et l'ARN d'un rôle IAM qui donne accès au secret.

> **Note**
>
> Vous pouvez utiliser `CmkSecretConfig` (avec`SasConfiguration`) ou `CustomSecretConfig` (sans`SasConfiguration`) pour fournir des informations d'identification pour une `CreateLocationAzureBlob` demande. Ne fournissez pas les deux paramètres pour la même demande.

Type : objet CustomSecretConfig

Obligatoire : non

SasConfiguration

Spécifie la configuration SAS qui permet d'accéder DataSync à votre stockage Azure Blob.

> **Note**
>
> Si vous fournissez un jeton d'authentification en utilisant`SasConfiguration`, sans fournir de détails de configuration secrets, en utilisant `CmkSecretConfig`

ou`CustomSecretConfig`, puis que vous DataSync stockez le jeton en utilisant le secret du gestionnaire de secrets de votre AWS compte.

Type : objet AzureBlobSasConfiguration

Obligatoire : non

Subdirectory

Spécifie les segments de chemin si vous souhaitez limiter votre transfert vers un répertoire virtuel de votre conteneur (par exemple,`/my/images`).

Type : String

Contraintes de longueur : longueur maximum de 1 024.

Modèle : `^[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}\p{C}]*$`

Obligatoire : non

Tags

Spécifie des étiquettes qui vous aident à catégoriser, filtrer et rechercher vos ressources AWS . Nous vous recommandons de créer au moins une étiquette nominative pour votre lieu de transfert.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

L'ARN de l'emplacement de transfert Azure Blob Storage que vous avez créé.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2

- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationEfs

Crée un emplacement de transfert pour un système de fichiers Amazon EFS. AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Avant de commencer, assurez-vous de bien comprendre comment DataSync accéder aux systèmes de fichiers Amazon EFS.

Syntaxe de la requête

```
{
   "AccessPointArn": "string",
   "Ec2Config": {
      "SecurityGroupArns": [ "string" ],
      "SubnetArn": "string"
   },
   "EfsFilesystemArn": "string",
   "FileSystemAccessRoleArn": "string",
   "InTransitEncryption": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AccessPointArn

Spécifie le nom de ressource Amazon (ARN) du point d'accès DataSync utilisé pour monter votre système de fichiers Amazon EFS.

Pour plus d'informations, consultez la section Accès aux systèmes de fichiers restreints.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

Obligatoire : non

Ec2Config

Spécifie le sous-réseau et les groupes de sécurité DataSync utilisés pour se connecter à l'une des cibles de montage de votre système de fichiers Amazon EFS.

Type : objet Ec2Config

Obligatoire : oui

EfsFilesystemArn

Spécifie l'ARN de votre système de fichiers Amazon EFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

Obligatoire : oui

FileSystemAccessRoleArn

Spécifie un rôle AWS Identity and Access Management (IAM) qui permet d'accéder DataSync à votre système de fichiers Amazon EFS.

Pour plus d'informations sur la création de ce rôle, voir Création d'un rôle DataSync IAM pour l'accès au système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Obligatoire : non

InTransitEncryption

Spécifie si vous DataSync souhaitez utiliser le chiffrement TLS (Transport Layer Security) 1.2 lors du transfert de données vers ou depuis votre système de fichiers Amazon EFS.

Si vous spécifiez un point d'accès en utilisant `AccessPointArn` ou un rôle IAM avec `FileSystemAccessRoleArn`, vous devez définir ce paramètre sur `TLS1_2`.

Type : String

Valeurs valides : `NONE | TLS1_2`

Obligatoire : non

Subdirectory

Spécifie un chemin de montage pour votre système de fichiers Amazon EFS. C'est là que les données sont DataSync lues ou écrites sur votre système de fichiers (selon qu'il s'agit d'un emplacement source ou de destination).

Par défaut, DataSync utilise le répertoire racine (ou le point d'accès si vous en fournissez un en utilisant`AccessPointArn`). Vous pouvez également inclure des sous-répertoires à l'aide de barres obliques (par exemple,). `/path/to/folder`

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Obligatoire : non

Tags

Spécifie la paire clé-valeur qui représente une balise que vous souhaitez ajouter à la ressource. La valeur peut être une chaîne vide. Cette valeur vous aide à gérer, filtrer et rechercher vos ressources. Nous vous recommandons de créer une balise de nom pour votre emplacement.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

Le nom de ressource Amazon (ARN) de l'emplacement du système de fichiers Amazon EFS que vous créez.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande

L'exemple suivant crée un emplacement pour un système de fichiers Amazon EFS.

```
{
    "Ec2Config": {
        "SubnetArn": "arn:aws:ec2:us-east-2:11122233344:subnet/
subnet-1234567890abcdef1",
        "SecurityGroupArns": [
            "arn:aws:ec2:us-east-2:11122233344:security-group/sg-1234567890abcdef2"
        ]
    },
    "EfsFilesystemArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:file-system/
fs-021345abcdef6789",
    "Subdirectory": "/mount/path",
    "Tags": [{
        "Key": "Name",
        "Value": "ElasticFileSystem-1"
    }]
}
```

Exemple de demande : création d'un emplacement pour un système de fichiers Amazon EFS restreint

L'exemple suivant crée un emplacement pour un système de fichiers Amazon EFS à accès restreint. Dans ce type de scénario, vous devrez peut-être spécifier des valeurs pour `AccessPointArnFileSystemAccessRoleArn`, et `InTransitEncryption` dans votre demande.

```
{
    "AccessPointArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:access-point/
fsap-1234567890abcdef0",
    "Ec2Config": {
        "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/
subnet-1234567890abcdef1",
        "SecurityGroupArns": [
            "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
        ]
    },
    "FileSystemAccessRoleArn": "arn:aws:iam::111222333444:role/
AwsDataSyncFullAccessNew",
```

```
    "InTransitEncryption": "TLS1_2",
    "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-
abcdef01234567890",
    "LocationUri": "efs://us-east-2.fs-021345abcdef6789/",
    "Subdirectory": "/mount/path",
    "Tags": [{
        "Key": "Name",
        "Value": "ElasticFileSystem-1"
    }]
}
```

Exemple de réponse

Une réponse renvoie l'ARN d'emplacement du système de fichiers Amazon EFS.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-12abcdef012345678"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationFsxLustre

Crée un emplacement de transfert pour un système de fichiers Amazon FSx for Lustre. AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Avant de commencer, assurez-vous de bien comprendre le mode d' DataSyncaccès aux systèmes FSx de fichiers Lustre.

Syntaxe de la requête

```
{
   "FsxFilesystemArn": "string",
   "SecurityGroupArns": [ "string" ],
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

FsxFilesystemArn

Spécifie le nom de ressource Amazon (ARN) du système de fichiers FSx for Lustre.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

Obligatoire : oui

SecurityGroupArns

Spécifie les noms de ressources Amazon (ARNs) d'un maximum de cinq groupes de sécurité qui donnent accès à votre système de fichiers FSx for Lustre.

Les groupes de sécurité doivent pouvoir accéder aux ports du système de fichiers. Le système de fichiers doit également autoriser l'accès depuis les groupes de sécurité. Pour plus d'informations sur l'accès au système de fichiers, consultez le guide de l'utilisateur d'Amazon FSx for Lustre.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obligatoire : oui

Subdirectory

Spécifie un chemin de montage pour votre système de fichiers FSx for Lustre. Le chemin peut inclure des sous-répertoires.

Lorsque l'emplacement est utilisé comme source, DataSync lit les données depuis le chemin de montage. Lorsque l'emplacement est utilisé comme destination, DataSync écrit des données sur le chemin de montage. Si vous n'incluez pas ce paramètre, DataSync utilise le répertoire racine du système de fichiers (`/`).

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : non

Tags

Spécifie des étiquettes qui vous aident à catégoriser, filtrer et rechercher vos ressources AWS . Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

Le nom de ressource Amazon (ARN) de l'emplacement du système de fichiers FSx pour Lustre que vous avez créé.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationFsxOntap

Crée un emplacement de transfert pour un système de fichiers Amazon FSx for NetApp ONTAP. AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Avant de commencer, assurez-vous de bien comprendre le mode d' DataSyncaccès aux systèmes FSx de fichiers ONTAP.

Syntaxe de la requête

```
{
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "Domain": "string",
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "SecurityGroupArns": [ "string" ],
   "StorageVirtualMachineArn": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Protocol

Spécifie le protocole de transfert de données AWS DataSync utilisé pour accéder à votre système de FSx fichiers Amazon.

Type : objet FsxProtocol

Obligatoire : oui

SecurityGroupArns

Spécifie les groupes EC2 de sécurité Amazon qui fournissent l'accès au sous-réseau préféré de votre système de fichiers.

Les groupes de sécurité doivent autoriser le trafic sortant sur les ports suivants (selon le protocole que vous utilisez) :

- NFS (Network File System) : ports TCP 111, 635 et 2 049
- SMB (Server Message Block) : port TCP 445

Les groupes de sécurité de votre système de fichiers doivent également autoriser le trafic entrant sur les mêmes ports.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obligatoire : oui

StorageVirtualMachineArn

Spécifie l'ARN de la machine virtuelle de stockage (SVM) de votre système de fichiers vers ou depuis laquelle vous souhaitez copier des données.

Type : String

Contraintes de longueur : longueur maximale de 162.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:storage-virtual-machine/fs-[0-9a-f]+/svm-[0-9a-f]{17,}$`

Obligatoire : oui

Subdirectory

Spécifie le chemin d'accès au partage de fichiers de la SVM vers lequel vous souhaitez transférer des données ou à partir duquel vous souhaitez transférer des données.

Vous pouvez spécifier un chemin de jonction (également appelé point de montage), un chemin qtree (pour les partages de fichiers NFS) ou un nom de partage (pour les partages de fichiers SMB). Par exemple, votre chemin de montage peut être `/vol1`, `/vol1/tree1` ou `/share1`.

> **Note**
>
> Ne spécifiez pas de chemin de jonction dans le volume racine de la SVM. Pour plus d'informations, consultez la section Gestion FSx des machines virtuelles de stockage ONTAP dans le guide de l'utilisateur Amazon FSx pour NetApp ONTAP.

Type : String

Contraintes de longueur : longueur maximale de 255.

Modèle : `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

Obligatoire : non

Tags

Spécifie des étiquettes qui vous aident à catégoriser, filtrer et rechercher vos ressources AWS . Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
```

```
    "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

Spécifie l'ARN de l'emplacement du système de fichiers FSx pour ONTAP que vous créez.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationFsxOpenZfs

Crée un emplacement de transfert pour un système de fichiers Amazon FSx pour OpenZFS. AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Avant de commencer, assurez-vous de bien comprendre le mode d' DataSyncaccès aux systèmes FSx de fichiers OpenZFS.

> **Note**
>
> Les paramètres de demande associés à `SMB` ne sont pas pris en charge par l'`CreateLocationFsxOpenZfs`opération.

Syntaxe de la requête

```
{
   "FsxFilesystemArn": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "Domain": "string",
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "SecurityGroupArns": [ "string" ],
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
```

```
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

FsxFilesystemArn

Nom de ressource Amazon (ARN) du système de fichiers FSx pour OpenZFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

Obligatoire : oui

Protocol

Type de protocole AWS DataSync utilisé pour accéder à votre système de fichiers.

Type : objet FsxProtocol

Obligatoire : oui

SecurityGroupArns

Les groupes ARNs de sécurité utilisés pour configurer le système de fichiers FSx pour OpenZFS.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obligatoire : oui

Subdirectory

Un sous-répertoire dans le chemin de l'emplacement qui doit commencer `/fsx` par. DataSync utilise ce sous-répertoire pour lire ou écrire des données (selon que le système de fichiers est un emplacement source ou de destination).

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[^\u0000\u0085\u2028\u2029\r\n]{1,4096}$`

Obligatoire : non

Tags

Paire clé-valeur qui représente une balise que vous souhaitez ajouter à la ressource. La valeur peut être une chaîne vide. Cette valeur vous aide à gérer, filtrer et rechercher vos ressources. Nous vous recommandons de créer une balise de nom pour votre emplacement.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

L'ARN de l'emplacement du système FSx de fichiers OpenZFS que vous avez créé.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

CreateLocationFsxWindows

Crée un emplacement de transfert pour un système de fichiers Amazon FSx pour Windows File Server. AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Avant de commencer, assurez-vous de bien comprendre le mode d' DataSyncaccès FSx aux systèmes de fichiers Windows File Server.

Syntaxe de la requête

```
{
   "Domain": "string",
   "FsxFilesystemArn": "string",
   "Password": "string",
   "SecurityGroupArns": [ "string" ],
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "User": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Domain

Spécifie le nom du domaine Windows auquel appartient le système FSx de fichiers du serveur de fichiers Windows.

Si votre environnement comporte plusieurs domaines Active Directory, la configuration de ce paramètre garantit la DataSync connexion au bon système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 253.

Modèle : `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

Obligatoire : non

FsxFilesystemArn

Spécifie le nom de ressource Amazon (ARN) FSx pour le système de fichiers Windows File Server.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

Obligatoire : oui

Password

Spécifie le mot de passe de l'utilisateur autorisé à monter et à accéder aux fichiers, dossiers et métadonnées de fichiers dans votre système de fichiers FSx pour Windows File Server.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^.{0,104}$`

Obligatoire : oui

SecurityGroupArns

Spécifie les groupes ARNs de EC2 sécurité Amazon qui fournissent l'accès au sous-réseau préféré de votre système de fichiers.

Les groupes de sécurité que vous spécifiez doivent pouvoir communiquer avec les groupes de sécurité de votre système de fichiers. Pour plus d'informations sur la configuration des groupes de sécurité pour l'accès au système de fichiers, consultez le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

> **Note**
>
> Si vous choisissez un groupe de sécurité qui n'autorise pas les connexions internes, effectuez l'une des opérations suivantes :
>
> - Configurez le groupe de sécurité pour lui permettre de communiquer au sein de lui-même.
> - Choisissez un autre groupe de sécurité capable de communiquer avec le groupe de sécurité de la cible de montage.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obligatoire : oui

Subdirectory

Spécifie un chemin de montage pour votre système de fichiers en utilisant des barres obliques. C'est là que les données sont DataSync lues ou écrites (selon qu'il s'agit d'un emplacement source ou de destination).

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : non

Tags

Spécifie des étiquettes qui vous aident à catégoriser, filtrer et rechercher vos ressources AWS . Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

User

Spécifie l'utilisateur autorisé à monter et à accéder aux fichiers, dossiers et métadonnées de fichiers dans votre système de fichiers FSx pour Windows File Server.

Pour plus d'informations sur le choix d'un utilisateur disposant du niveau d'accès approprié pour votre transfert, consultez les autorisations requises FSx pour les emplacements des serveurs de fichiers Windows.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

L'ARN de l'emplacement du système de fichiers FSx pour Windows File Server que vous avez créé.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationHdfs

Crée un emplacement de transfert pour un système de fichiers distribué Hadoop (HDFS). AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Avant de commencer, assurez-vous de bien comprendre comment DataSync accéder aux clusters HDFS.

Syntaxe de la requête

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlockSize": number,
   "KerberosKeytab": blob,
   "KerberosKrb5Conf": blob,
   "KerberosPrincipal": "string",
   "KmsKeyProviderUri": "string",
   "NameNodes": [
      {
         "Hostname": "string",
         "Port": number
      }
   ],
   "QopConfiguration": {
      "DataTransferProtection": "string",
      "RpcProtection": "string"
   },
   "ReplicationFactor": number,
   "SimpleUser": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AgentArns

Les Amazon Resource Names (ARNs) des DataSync agents qui peuvent se connecter à votre cluster HDFS.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : oui

AuthenticationType

Type d'authentification utilisé pour déterminer l'identité de l'utilisateur.

Type : String

Valeurs valides : `SIMPLE | KERBEROS`

Obligatoire : oui

BlockSize

La taille des blocs de données à écrire dans le cluster HDFS. La taille des blocs doit être un multiple de 512 octets. La taille des blocs par défaut est de 128 mégaoctets (Mio).

Type : entier

Plage valide : valeur minimale de 1048576. Valeur maximale de 1073741824.

Obligatoire : non

KerberosKeytab

La table de clés Kerberos (keytab) qui contient les mappages entre le principal Kerberos défini et les clés chiffrées. Vous pouvez charger le keytab à partir d'un fichier en fournissant l'adresse du fichier.

> **Note**
>
> Ce paramètre est requis si `KERBEROS` est spécifié pour `AuthenticationType`.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 65536.

Obligatoire : non

KerberosKrb5Conf

Le fichier `krb5.conf` qui contient les informations de configuration Kerberos. Vous pouvez charger le `krb5.conf` fichier en fournissant son adresse. Si vous utilisez le AWS CLI, il exécute le codage base64 pour vous. Dans le cas contraire, fournissez le texte codé en base64.

> **Note**
>
> Ce paramètre est requis si `KERBEROS` est spécifié pour `AuthenticationType`.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 131072.

Obligatoire : non

KerberosPrincipal

Le principal Kerberos ayant accès aux fichiers et dossiers du cluster HDFS.

> **Note**
>
> Ce paramètre est requis si `KERBEROS` est spécifié pour `AuthenticationType`.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^.+$`

Obligatoire : non

KmsKeyProviderUri

L'URI du serveur de gestion de clés (KMS) du cluster HDFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Modèle : `^kms:\/\/http[s]?@(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9])(;(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9]))*:[0-9]{1,5}\/kms$`

Obligatoire : non

NameNodes

Celui NameNode qui gère l'espace de noms HDFS. Il NameNode effectue des opérations telles que l'ouverture, la fermeture et le changement de nom de fichiers et de répertoires. Le NameNode contient les informations permettant de mapper des blocs de données au DataNodes. Vous ne pouvez en utiliser qu'un seul NameNode.

Type : tableau d'objets HdfsNameNode

Membres du tableau : Nombre minimum de 1 élément.

Obligatoire : oui

QopConfiguration

La configuration de la qualité de protection (QOP) spécifie les paramètres RPC (Remote Procedure Call) et de protection du transfert de données configurés sur le cluster de système de fichiers distribué Hadoop (HDFS). Si la valeur `QopConfiguration` n'est pas spécifiée, les valeurs `RpcProtection` et `DataTransferProtection` par défaut sont `PRIVACY`. Si vous définissez `RpcProtection` ou `DataTransferProtection`, l'autre paramètre suppose la même valeur.

Type : objet QopConfiguration

Obligatoire : non

ReplicationFactor

Le nombre de DataNodes vers lesquels répliquer les données lors de l'écriture dans le cluster HDFS. Par défaut, les données sont répliquées sur trois DataNodes.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 512.

Obligatoire : non

SimpleUser

Le nom d'utilisateur servant à identifier le client sur le système d'exploitation hôte.

> **Note**
>
> Ce paramètre est requis si `SIMPLE` est spécifié pour `AuthenticationType`.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

Obligatoire : non

Subdirectory

Un sous-répertoire du cluster HDFS. Ce sous-répertoire est utilisé pour lire des données à partir du cluster HDFS ou y écrire des données. Si le sous-répertoire n'est pas spécifié, la valeur par défaut est `/`.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : non

Tags

Paire clé-valeur qui représente la balise que vous souhaitez ajouter à l'emplacement. La valeur peut être une chaîne vide. Nous vous recommandons d'utiliser des balises pour nommer vos ressources.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

L'ARN de l'emplacement du cluster HDFS source que vous créez.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationNfs

Crée un emplacement de transfert pour un serveur de fichiers NFS (Network File System). AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Avant de commencer, assurez-vous de bien comprendre comment DataSync accéder aux serveurs de fichiers NFS.

Syntaxe de la requête

```
{
   "MountOptions": {
      "Version": "string"
   },
   "OnPremConfig": {
      "AgentArns": [ "string" ]
   },
   "ServerHostname": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

MountOptions

Spécifie les options qui DataSync peuvent être utilisées pour monter votre serveur de fichiers NFS.

Type : objet NfsMountOptions

Obligatoire : non

OnPremConfig

Spécifie le nom de ressource Amazon (ARN) de l' DataSync agent qui peut se connecter à votre serveur de fichiers NFS.

Vous pouvez spécifier plusieurs agents. Pour plus d'informations, consultez la section Utilisation de plusieurs DataSync agents.

Type : objet OnPremConfig

Obligatoire : oui

ServerHostname

Spécifie le nom DNS ou l'adresse IP (IPv4 ou IPv6) du serveur de fichiers NFS auquel votre DataSync agent se connecte.

Type : String

Contraintes de longueur : longueur maximale de 255.

Modèle : `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Obligatoire : oui

Subdirectory

Spécifie le chemin d'exportation sur le serveur de fichiers NFS que vous DataSync souhaitez monter.

Ce chemin (ou un sous-répertoire du chemin) est l'endroit où les données sont DataSync transférées depuis ou vers. Pour plus d'informations sur la configuration d'une exportation pour DataSync, consultez la section Accès aux serveurs de fichiers NFS.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]+$`

Obligatoire : oui

Tags

Spécifie des étiquettes qui vous aident à classer, filtrer et rechercher vos AWS ressources. Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

L'ARN de l'emplacement de transfert que vous avez créé pour votre serveur de fichiers NFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

exemple

L'exemple suivant crée un emplacement DataSync de transfert pour un serveur de fichiers NFS.

Exemple de demande

```
{
  "MountOptions": {
     "Version": : "NFS4_0"
     },
  "OnPremConfig": {
    "AgentArn": [ "arn:aws:datasync:us-east-2:111222333444:agent/
agent-0b0addbeef44b3nfs" ]
          },

           "ServerHostname": "MyServer@amazon.com",
           "Subdirectory": "/MyFolder",
           "Tags": [
              {
                "Key": "Name",
                "Value": "FileSystem-1"
              }
           ]
}
```

exemple

La réponse renvoie l'ARN de l'emplacement NFS.

Exemple de réponse

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
```

```
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationObjectStorage

Crée un emplacement de transfert pour un système de stockage d'objets. AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données. Vous pouvez effectuer des virements avec ou sans DataSyncagent.

Avant de commencer, assurez-vous de connaître les prérequis pour travailler avec DataSync les systèmes de stockage d'objets.

Syntaxe de la requête

```
{
   "AccessKey": "string",
   "AgentArns": [ "string" ],
   "BucketName": "string",
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "SecretKey": "string",
   "ServerCertificate": blob,
   "ServerHostname": "string",
   "ServerPort": number,
   "ServerProtocol": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AccessKey

Spécifie la clé d'accès (par exemple, un nom d'utilisateur) si des informations d'identification sont requises pour s'authentifier auprès du serveur de stockage d'objets.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `^.*$`

Obligatoire : non

AgentArns

(Facultatif) Spécifie les Amazon Resource Names (ARNs) des DataSync agents qui peuvent se connecter à votre système de stockage d'objets. Si vous configurez un transfert cross-cloud sans agent, il n'est pas nécessaire de spécifier une valeur pour ce paramètre.

> **Note**
>
> Assurez-vous de configurer correctement ce paramètre lorsque vous créez votre emplacement de stockage pour la première fois. Il est impossible d'ajouter ou de supprimer des agents d'un emplacement de stockage après l'avoir créé.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : non

BucketName

Spécifie le nom du compartiment de stockage d'objets impliqué dans le transfert.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 63.

Modèle : `^[a-zA-Z0-9_\-\+\.\(\)\$\p{Zs}]+$`

Obligatoire : oui

CmkSecretConfig

Spécifie les informations de configuration pour un secret DataSync géré, notamment le `SecretKey` secret DataSync utilisé pour accéder à un emplacement de stockage d'objets spécifique, avec un secret géré par le client AWS KMS key.

Lorsque vous incluez ce paramètre dans le cadre d'une `CreateLocationObjectStorage` demande, vous ne fournissez que l'ARN de la clé KMS. DataSync utilise cette clé KMS avec la valeur que vous spécifiez pour le `SecretKey` paramètre afin de créer un secret DataSync géré afin de stocker les informations d'accès à la localisation.

Assurez-vous qu' DataSync il est autorisé à accéder à la clé KMS que vous spécifiez.

> **Note**
>
> Vous pouvez utiliser `CmkSecretConfig` (avec`SecretKey`) ou `CustomSecretConfig` (sans`SecretKey`) pour fournir des informations d'identification pour une `CreateLocationObjectStorage` demande. Ne fournissez pas les deux paramètres pour la même demande.

Type : objet CmkSecretConfig

Obligatoire : non

CustomSecretConfig

Spécifie les informations de configuration d'un secret Secrets Manager géré par le client dans lequel la clé secrète d'un emplacement de stockage d'objets spécifique est stockée en texte brut. Cette configuration inclut l'ARN secret et l'ARN d'un rôle IAM qui donne accès au secret.

> **Note**
>
> Vous pouvez utiliser `CmkSecretConfig` (avec`SecretKey`) ou `CustomSecretConfig` (sans`SecretKey`) pour fournir des informations d'identification pour une

`CreateLocationObjectStorage` demande. Ne fournissez pas les deux paramètres pour la même demande.

Type : objet CustomSecretConfig

Obligatoire : non

SecretKey

Spécifie la clé secrète (par exemple, un mot de passe) si des informations d'identification sont requises pour s'authentifier auprès du serveur de stockage d'objets.

> **Note**
>
> Si vous fournissez un code secret en utilisant `CmkSecretConfig` ou`SecretKey`, si vous ne fournissez pas de détails de configuration secrets`CustomSecretConfig`, vous DataSync stockez le jeton en utilisant le secret du Gestionnaire de Secrets Manager de votre AWS compte.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `^.*$`

Obligatoire : non

ServerCertificate

Spécifie une chaîne de certificats DataSync pour l'authentification auprès de votre système de stockage d'objets si celui-ci utilise une autorité de certification (CA) privée ou auto-signée. Vous devez spécifier un seul `.pem` fichier avec une chaîne de certificats complète (par exemple,`file:///home/user/.ssh/object_storage_certificates.pem`).

La chaîne de certificats peut inclure :

- Le certificat du système de stockage d'objets
- Tous les certificats intermédiaires (s'il y en a)
- Le certificat racine de l'autorité de certification signataire

Vous pouvez concaténer vos certificats dans un `.pem` fichier (dont la taille peut atteindre 32 768 octets avant le codage base64). L'exemple de `cat` commande suivant crée un `object_storage_certificates.pem` fichier contenant trois certificats :

```
cat object_server_certificate.pem intermediate_certificate.pem
ca_root_certificate.pem > object_storage_certificates.pem
```

Pour utiliser ce paramètre, configurez `ServerProtocol` sur`HTTPS`.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 32 768.

Obligatoire : non

ServerHostname

Spécifie le nom de domaine ou l'adresse IP (IPv4 ou IPv6) du serveur de stockage d'objets auquel votre DataSync agent se connecte.

Type : String

Contraintes de longueur : longueur maximale de 255.

Modèle : `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Obligatoire : oui

ServerPort

Spécifie le port sur lequel votre serveur de stockage d'objets accepte le trafic réseau entrant (par exemple, le port 443).

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 65536.

Obligatoire : non

ServerProtocol

Spécifie le protocole utilisé par votre serveur de stockage d'objets pour communiquer. L'échelle par défaut, si elle n'est pas spécifiée, est de `HTTPS`.

Type : String

Valeurs valides : `HTTPS | HTTP`

Obligatoire : non

Subdirectory

Spécifie le préfixe d'objet pour votre serveur de stockage d'objets. S'il s'agit d'un emplacement source, copie DataSync uniquement les objets portant ce préfixe. S'il s'agit d'un emplacement de destination, DataSync écrit tous les objets avec ce préfixe.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Obligatoire : non

Tags

Spécifie la paire clé-valeur qui représente une balise que vous souhaitez ajouter à la ressource. Les balises vous aident à gérer, filtrer et rechercher vos ressources. Nous vous recommandons de créer une balise de nom pour votre emplacement.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

Spécifie l'ARN de l'emplacement du système de stockage d'objets que vous créez.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationS3

Crée un emplacement de transfert pour un compartiment Amazon S3. AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

> **Important**
>
> Avant de commencer, assurez-vous de lire les rubriques suivantes :
>
> - Considérations relatives à la classe de stockage avec les sites Amazon S3
> - Évaluation des coûts des requêtes S3 lors de l'utilisation DataSync

Pour plus d'informations, consultez Configuration des transferts avec Amazon S3.

Syntaxe de la requête

```
{
   "AgentArns": [ "string" ],
   "S3BucketArn": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
   "S3StorageClass": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AgentArns

(Amazon S3 sur Outposts uniquement) Spécifie le nom de ressource Amazon (ARN) de l' DataSync agent sur votre Outpost.

Pour plus d'informations, consultez la section Déployer votre DataSync agent sur AWS Outposts.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : non

S3BucketArn

Spécifie l'ARN du compartiment S3 que vous souhaitez utiliser comme emplacement. (Lorsque vous créerez votre DataSync tâche ultérieurement, vous indiquerez si cet emplacement est une source ou une destination de transfert.)

Si votre compartiment S3 se trouve sur une AWS Outposts ressource, vous devez spécifier un point d'accès Amazon S3. Pour plus d'informations, consultez la section Gestion de l'accès aux données avec les points d'accès Amazon S3 dans le guide de l'utilisateur Amazon S3.

Type : String

Contraintes de longueur : longueur maximale de 268.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

Obligatoire : oui

S3Config

Spécifie le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) DataSync utilisé pour accéder à votre compartiment S3.

Pour plus d'informations, consultez la section Fournir DataSync un accès aux compartiments S3.

Type : objet S3Config

Obligatoire : oui

S3StorageClass

Spécifie la classe de stockage que vous souhaitez que vos objets utilisent lorsque Amazon S3 est une destination de transfert.

Pour les compartiments entrants Régions AWS, la classe de stockage par défaut est. `STANDARD` Pour les buckets activés AWS Outposts, la classe de stockage par défaut est. `OUTPOSTS`

Pour plus d'informations, consultez la section Considérations relatives aux classes de stockage associées aux transferts Amazon S3.

Type : String

Valeurs valides : `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

Obligatoire : non

Subdirectory

Spécifie un préfixe dans le compartiment S3 qui DataSync lit ou écrit vers (selon que le compartiment est un emplacement source ou de destination).

> **Note**
>
> DataSync Impossible de transférer des objets dont le préfixe commence par une barre oblique (/) ou inclut `///./`, ou `/../` des motifs. Par exemple :
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`
> - `photos/../2006/March`

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Obligatoire : non

Tags

Spécifie des étiquettes qui vous aident à classer, filtrer et rechercher vos AWS ressources. Nous vous recommandons de créer au moins une étiquette nominative pour votre lieu de transfert.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

L'ARN de l'emplacement S3 que vous avez créé.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Étape 1. Autoriser à assumer le rôle IAM requis pour écrire dans le compartiment

L'exemple suivant montre la politique la plus simple qui accorde les autorisations requises pour accéder AWS DataSync à un compartiment Amazon S3 de destination, suivie d'un rôle IAM auquel la `create-location-s3-iam-role` politique a été attachée.

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

```
"Role": {
        "Path": "/",
        "RoleName": "amzn-s3-demo-bucket-access-role",
        "RoleId": "role-id",
        "Arn": "arn:aws:iam::account-id:role/amzn-s3-demo-bucket-access-role",
        "CreateDate": "2018-07-27T02:49:23.117Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
```

```
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "datasync.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Étape 2. Autoriser le rôle IAM créé à écrire dans le bucket

Associez au rôle une politique disposant des autorisations suffisantes pour accéder au compartiment. La politique `AWSDataSyncFullAccess` gérée est un exemple d'une telle politique.

Pour plus d'informations, consultez AWSDataSyncFullAccessla console IAM.

Il n'est pas nécessaire de créer cette politique. Il est géré par AWS, il vous suffit donc de spécifier son ARN dans la `attach-role-policy` commande.

```
IAM_POLICY_ARN='arn:aws:iam::aws:policy/AWSDataSyncFullAccess'
```

Étape 3. Création d'un point de terminaison pour un compartiment Amazon S3

L'exemple suivant crée un point de terminaison pour un compartiment Amazon S3.

Lorsque le point de terminaison S3 est créé, une réponse similaire au deuxième exemple suivant renvoie le nom de ressource Amazon (ARN) du nouvel emplacement Amazon S3.

Exemple de demande

```
{
  "S3BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket",
  "S3Config": {
     "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/amzn-s3-demo-bucket-access-
role",
    },
    "S3StorageClass": "STANDARD",
    "Subdirectory": "/MyFolder",
    "Tags": [
```

```
        {
           "Key": "Name",
           "Value": "s3Bucket-1"
        }
      ]
}
```

Exemple de réponse

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLocationSmb

Crée un emplacement de transfert pour un serveur de fichiers SMB (Server Message Block). AWS DataSync peut utiliser cet emplacement comme source ou destination pour le transfert de données.

Avant de commencer, assurez-vous de bien comprendre comment DataSync accéder aux serveurs de fichiers SMB. Pour plus d'informations, consultez la section Fournir un DataSync accès aux serveurs de fichiers SMB.

Syntaxe de la requête

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "DnsIpAddresses": [ "string" ],
   "Domain": "string",
   "KerberosKeytab": blob,
   "KerberosKrb5Conf": blob,
   "KerberosPrincipal": "string",
   "MountOptions": {
      "Version": "string"
   },
   "Password": "string",
   "ServerHostname": "string",
   "Subdirectory": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "User": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AgentArns

Spécifie l' DataSync agent (ou les agents) qui peuvent se connecter à votre serveur de fichiers SMB. Vous spécifiez un agent en utilisant son Amazon Resource Name (ARN).

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : oui

AuthenticationType

Spécifie le protocole d'authentification DataSync utilisé pour se connecter à votre serveur de fichiers SMB. DataSync supports `NTLM` (par défaut) et `KERBEROS` authentification.

Pour plus d'informations, consultez la section Fournir un DataSync accès aux serveurs de fichiers SMB.

Type : String

Valeurs valides : `NTLM | KERBEROS`

Obligatoire : non

DnsIpAddresses

Spécifie les IPv6 adresses IPv4 ou les adresses des serveurs DNS auxquels appartient votre serveur de fichiers SMB. Ce paramètre ne s'applique que s'`AuthenticationType`il est défini sur`KERBEROS`.

Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion au bon serveur de fichiers SMB.

Type : tableau de chaînes

Membres du tableau : nombre maximum de 2 éléments.

Contraintes de longueur : longueur minimale de 7. Longueur maximale de 39

Modèle : `\A((25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d)){3}|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6}))\z`

Obligatoire : non

Domain

Spécifie le nom de domaine Windows auquel appartient votre serveur de fichiers SMB. Ce paramètre ne s'applique que s'`AuthenticationType`il est défini sur`NTLM`.

Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion au bon serveur de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 253.

Modèle : `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

Obligatoire : non

KerberosKeytab

Spécifie votre fichier de table de clés Kerberos (keytab), qui inclut les mappages entre votre clé principale Kerberos et vos clés de chiffrement.

Pour éviter les erreurs d'exécution des tâches, assurez-vous que le principal Kerberos que vous utilisez pour créer le fichier keytab correspond exactement à ce que vous spécifiez. `KerberosPrincipal`

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 65536.

Obligatoire : non

KerberosKrb5Conf

Spécifie un fichier de configuration Kerberos (`krb5.conf`) qui définit la configuration de votre domaine Kerberos.

Le fichier doit être codé en base64. Si vous utilisez le AWS CLI, le codage est fait pour vous.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 131072.

Obligatoire : non

KerberosPrincipal

Spécifie un principal Kerberos, qui est une identité dans votre domaine Kerberos autorisée à accéder aux fichiers, aux dossiers et aux métadonnées des fichiers sur votre serveur de fichiers SMB.

Un principal Kerberos peut ressembler à. `HOST/kerberosuser@MYDOMAIN.ORG`

Les noms principaux distinguent les majuscules et minuscules. L'exécution de votre DataSync tâche échouera si le principal que vous spécifiez pour ce paramètre ne correspond pas exactement au principal que vous avez utilisé pour créer le fichier keytab.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^.+$`

Obligatoire : non

MountOptions

Spécifie la version du protocole SMB DataSync utilisée pour accéder à votre serveur de fichiers SMB.

Type : objet SmbMountOptions

Obligatoire : non

Password

Spécifie le mot de passe de l'utilisateur qui peut monter votre serveur de fichiers SMB et qui est autorisé à accéder aux fichiers et dossiers concernés par votre transfert. Ce paramètre ne s'applique que s'`AuthenticationType`il est défini sur`NTLM`.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^.{0,104}$`

Obligatoire : non

ServerHostname

Spécifie le nom de domaine ou l'adresse IP (IPv4 ou IPv6) du serveur de fichiers SMB auquel votre DataSync agent se connecte.

> **Note**
>
> Si vous utilisez l'authentification Kerberos, vous devez spécifier un nom de domaine.

Type : String

Contraintes de longueur : longueur maximale de 255.

Modèle : `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Obligatoire : oui

Subdirectory

Spécifie le nom du partage exporté par votre serveur de fichiers SMB où les données DataSync seront lues ou écrites. Vous pouvez inclure un sous-répertoire dans le chemin de partage (par exemple,`/path/to/subdirectory`). Assurez-vous que les autres clients SMB de votre réseau peuvent également monter ce chemin.

Pour copier toutes les données du sous-répertoire, vous DataSync devez être en mesure de monter le partage SMB et d'accéder à toutes ses données. Pour plus d'informations, consultez la section Fournir un DataSync accès aux serveurs de fichiers SMB.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : oui

Tags

Spécifie des étiquettes qui vous aident à catégoriser, filtrer et rechercher vos ressources AWS . Nous vous recommandons de créer au moins une balise de nom pour votre emplacement.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

User

Spécifie l'utilisateur qui peut monter et accéder aux fichiers, aux dossiers et aux métadonnées des fichiers sur votre serveur de fichiers SMB. Ce paramètre ne s'applique que s'`AuthenticationType`il est défini sur`NTLM`.

Pour plus d'informations sur le choix d'un utilisateur disposant du niveau d'accès approprié pour votre transfert, consultez la section Fournir un DataSync accès aux serveurs de fichiers SMB.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "LocationArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LocationArn

L'ARN de l'emplacement SMB que vous avez créé.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande

L'exemple suivant crée un emplacement pour un serveur de fichiers SMB.

```
{
   "AgentArns":[
      "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44b3nfs",
      "arn:aws:datasync:us-east-2:111222333444:agent/agent-2345noo35nnee1123ovo3"
   ],
   "Domain":"AMAZON",
   "MountOptions":{
      "Version":"SMB3"
   },
   "Password":"string",
   "ServerHostname":"MyServer.amazon.com",
   "Subdirectory":"share",
```

```
   "Tags":[
      {
         "Key":"department",
         "Value":"finance"
      }
   ],
   "User":"user-1"
}
```

Exemple de réponse

Une réponse renvoie l'ARN de l'emplacement de votre serveur de fichiers SMB.

```
{
    "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0f01451b140b2af49"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateTask

Configure une tâche qui définit où et comment vos données sont AWS DataSync transférées.

Une tâche inclut un emplacement source, un emplacement de destination et des options de transfert (telles que les limites de bande passante, la planification, etc.).

> **Important**
>
> Si vous prévoyez de transférer des données depuis ou vers un site Amazon S3, examinez comment cela DataSync peut affecter les frais de votre demande S3 et la page de DataSync tarification avant de commencer.

Syntaxe de la requête

```
{
   "CloudWatchLogGroupArn": "string",
   "DestinationLocationArn": "string",
   "Excludes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "Includes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "ManifestConfig": {
      "Action": "string",
      "Format": "string",
      "Source": {
         "S3": {
            "BucketAccessRoleArn": "string",
            "ManifestObjectPath": "string",
            "ManifestObjectVersionId": "string",
            "S3BucketArn": "string"
         }
      }
```

```
    },
    "Name": "string",
    "Options": {
       "Atime": "string",
       "BytesPerSecond": number,
       "Gid": "string",
       "LogLevel": "string",
       "Mtime": "string",
       "ObjectTags": "string",
       "OverwriteMode": "string",
       "PosixPermissions": "string",
       "PreserveDeletedFiles": "string",
       "PreserveDevices": "string",
       "SecurityDescriptorCopyFlags": "string",
       "TaskQueueing": "string",
       "TransferMode": "string",
       "Uid": "string",
       "VerifyMode": "string"
    },
    "Schedule": {
       "ScheduleExpression": "string",
       "Status": "string"
    },
    "SourceLocationArn": "string",
    "Tags": [
       {
          "Key": "string",
          "Value": "string"
       }
    ],
    "TaskMode": "string",
    "TaskReportConfig": {
       "Destination": {
          "S3": {
             "BucketAccessRoleArn": "string",
             "S3BucketArn": "string",
             "Subdirectory": "string"
          }
       },
       "ObjectVersionIds": "string",
       "OutputType": "string",
       "Overrides": {
          "Deleted": {
             "ReportLevel": "string"
```

```
            },
            "Skipped": {
               "ReportLevel": "string"
            },
            "Transferred": {
               "ReportLevel": "string"
            },
            "Verified": {
               "ReportLevel": "string"
            }
         },
         "ReportLevel": "string"
      }
   }
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

CloudWatchLogGroupArn

Spécifie le nom de ressource Amazon (ARN) d'un groupe de CloudWatch journaux Amazon pour surveiller votre tâche.

Pour les tâches en mode amélioré, il n'est pas nécessaire de spécifier quoi que ce soit. DataSyncenvoie automatiquement les journaux à un groupe de CloudWatch journaux nommé`/aws/datasync`.

Pour plus d'informations, consultez la section Surveillance des transferts de données à l'aide CloudWatch des journaux.

Type : String

Contraintes de longueur : longueur maximale de 562.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

Obligatoire : non

DestinationLocationArn

Spécifie l'ARN de l'emplacement de destination de votre transfert.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Excludes

Spécifie les filtres d'exclusion qui définissent les fichiers, les objets et les dossiers de votre emplacement source que vous ne DataSync souhaitez pas transférer. Pour plus d'informations et des exemples, voir Spécifier les DataSync transferts à l'aide de filtres.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Obligatoire : non

Includes

Spécifie les filtres d'inclusion qui définissent les fichiers, les objets et les dossiers que vous souhaitez DataSync transférer dans votre emplacement source. Pour plus d'informations et des exemples, voir Spécifier les DataSync transferts à l'aide de filtres.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Obligatoire : non

ManifestConfig

Configure un manifeste, qui est une liste de fichiers ou d'objets que vous souhaitez DataSync transférer. Pour plus d'informations et des exemples de configuration, voir Spécifier les DataSync transferts à l'aide d'un manifeste.

Lorsque vous utilisez ce paramètre, l'identité de votre appelant (le rôle DataSync avec lequel vous utilisez) doit être `iam:PassRole` autorisée. La AWSDataSyncFullAccesspolitique inclut cette autorisation.

Type : objet ManifestConfig

Obligatoire : non

Name

Spécifie le nom de votre tâche.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatoire : non

Options

Spécifie les paramètres de votre tâche, tels que la préservation des métadonnées des fichiers, la vérification de l'intégrité des données, entre autres options.

Type : objet Options

Obligatoire : non

Schedule

Spécifie le calendrier d'exécution de la tâche. Pour plus d'informations, veuillez consulter la rubrique Planification de votre tâche.

Type : objet TaskSchedule

Obligatoire : non

SourceLocationArn

Spécifie l'ARN de l'emplacement source de votre transfert.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Tags

Spécifie les balises que vous souhaitez appliquer à votre tâche.

Les balises sont des paires clé-valeur qui vous permettent de gérer, de filtrer et de rechercher vos DataSync ressources.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

TaskMode

Spécifie l'un des modes de tâche suivants pour le transfert de données :

- `ENHANCED`- Transférez un nombre pratiquement illimité d'objets avec des performances supérieures à celles du mode Basic. Les tâches en mode amélioré optimisent le processus de transfert de données en listant, préparant, transférant et vérifiant les données en parallèle. Le mode amélioré est actuellement disponible pour les transferts entre les sites Amazon S3, les transferts entre Azure Blob et Amazon S3 sans agent, et les transferts entre d'autres clouds et Amazon S3 sans agent.

  > **Note**
  >
  > Pour créer une tâche en mode amélioré, le rôle IAM que vous utilisez pour appeler l'`CreateTask`opération doit disposer de l'`iam:CreateServiceLinkedRole`autorisation.

- `BASIC`(par défaut) - Transférez des fichiers ou des objets entre le AWS stockage et tous les autres DataSync emplacements pris en charge. Les tâches en mode de base sont soumises à des quotas sur le nombre de fichiers, d'objets et de répertoires dans un ensemble de données. Le mode de base prépare, transfère et vérifie les données de manière séquentielle, ce qui le rend plus lent que le mode amélioré pour la plupart des charges de travail.

Pour plus d'informations, voir Comprendre les différences entre les modes de tâche.

Type : String

Valeurs valides : `BASIC | ENHANCED`

Obligatoire : non

TaskReportConfig

Spécifie la manière dont vous souhaitez configurer un rapport de tâches, qui fournit des informations détaillées sur votre DataSync transfert. Pour plus d'informations, consultez la section Surveillance de vos DataSync transferts à l'aide de rapports de tâches.

Lorsque vous utilisez ce paramètre, l'identité de votre appelant (le rôle DataSync avec lequel vous utilisez) doit être `iam:PassRole` autorisée. La AWSDataSyncFullAccesspolitique inclut cette autorisation.

Type : objet TaskReportConfig

Obligatoire : non

Syntaxe de la réponse

```
{
   "TaskArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

TaskArn

Amazon Resource Name (ARN) de la tâche.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande pour une tâche en mode amélioré

L'exemple suivant crée une DataSync tâche qui utilise le mode amélioré.

Contrairement à la création de tâches en mode Basic, il n'est pas nécessaire de spécifier un groupe de CloudWatch journaux Amazon. Avec les tâches en mode amélioré, envoie DataSync automatiquement les journaux des tâches à un groupe de journaux nommé`/aws/datasync`. Si ce groupe de journaux n'existe pas dans votre Région AWS, DataSync crée le groupe de journaux en votre nom lorsque vous créez la tâche.

```
{
  "SourceLocationArn": "arn:aws:datasync:us-
east-1:111222333444:location/1111aaaa2222bbbb3",
  "DestinationLocationArn": "arn:aws:datasync:us-
east-1:111222333444:location/0000zzzz1111yyyy2",
  "Name": "My Enhanced mode task",
  "TaskMode": "ENHANCED",
  "Options": {
    "TransferMode": "CHANGED",
    "VerifyMode": "ONLY_FILES_TRANSFERRED",
    "ObjectTags": "PRESERVE",
    "LogLevel": "TRANSFER"
  }
}
```

Exemple de demande pour une tâche en mode de base

L'exemple suivant crée une DataSync tâche qui utilise le mode de base.

```
{
    "SourceLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-1111aaaa2222bbbb3",
    "DestinationLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-0000zzzz1111yyyy2",
    "Name": "My Basic mode task",
    "TaskMode": "BASIC",
    "Options": {
        "Atime": "BEST_EFFORT",
        "Gid": "NONE",
        "Mtime": "PRESERVE",
        "PosixPermissions": "PRESERVE",
        "PreserveDevices": "NONE",
        "PreserveDeletedFiles": "PRESERVE",
        "Uid": "NONE",
        "VerifyMode": "ONLY_FILES_TRANSFERRED"
    },
    "Schedule": {
        "ScheduleExpression": "0 12 ? * SUN,WED *"
    },
    "CloudWatchLogGroupArn": "arn:aws:logs:us-east-2:111222333444:log-group:/log-group-
name:*",
    "Tags": [
        {
            "Key": "Name",
            "Value": "Migration-wave-1"
        }
    ]
}
```

Exemple de réponse

La réponse suivante inclut l'ARN d'une tâche créée.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteAgent

Supprime une ressource d' AWS DataSync agent de votre Compte AWS.

N'oubliez pas que cette opération (irréversible) ne supprime pas la machine virtuelle (VM) ou l' EC2 instance Amazon de l'agent de votre environnement de stockage. Pour les étapes suivantes, vous pouvez supprimer la machine virtuelle ou l'instance de votre environnement de stockage ou la réutiliser pour activer un nouvel agent.

Syntaxe de la requête

```
{
   "AgentArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AgentArn

Le nom de ressource Amazon (ARN) de l'agent à supprimer. Utilisez cette `ListAgents` opération pour renvoyer une liste d'agents pour votre compte et Région AWS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteLocation

Supprime une ressource de lieu de transfert de AWS DataSync.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Le nom de ressource Amazon (ARN) de l'emplacement à supprimer.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteTask

Supprime une ressource de tâche de transfert de AWS DataSync.

Syntaxe de la requête

```
{
   "TaskArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

TaskArn

Spécifie le nom de ressource Amazon (ARN) de la tâche que vous souhaitez supprimer.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeAgent

Renvoie des informations sur un AWS DataSync agent, telles que son nom, son type de point de terminaison de service et son statut.

Syntaxe de la requête

```
{
   "AgentArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AgentArn

Spécifie le nom de ressource Amazon (ARN) de l' DataSync agent sur lequel vous souhaitez obtenir des informations.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "AgentArn": "string",
   "CreationTime": number,
   "EndpointType": "string",
   "LastConnectionTime": number,
   "Name": "string",
   "Platform": {
```

```
        "Version": "string"
    },
    "PrivateLinkConfig": {
        "PrivateLinkEndpoint": "string",
        "SecurityGroupArns": [ "string" ],
        "SubnetArns": [ "string" ],
        "VpcEndpointId": "string"
    },
    "Status": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AgentArn

L'ARN de l'agent.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

Heure à laquelle l'agent a été activé.

Type : Timestamp

EndpointType

Type de point de terminaison de service auquel votre agent est connecté.

Type : String

Valeurs valides : `PUBLIC | PRIVATE_LINK | FIPS`

LastConnectionTime

La dernière fois que l'agent a communiqué avec le DataSync service.

Type : Timestamp

Name

Le nom de l'agent.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Platform

Les informations relatives à la plate-forme concernant l'agent, telles que le numéro de version.

Type : objet Platform

PrivateLinkConfig

Configuration réseau utilisée par l'agent lors de la connexion à un point de terminaison de service VPC.

Type : objet PrivateLinkConfig

Status

Le statut de l'agent.

- Si le statut est défini`ONLINE`, l'agent est correctement configuré et prêt à être utilisé.
- Si le statut est le cas`OFFLINE`, l'agent a été hors de contact avec DataSync lui pendant cinq minutes ou plus. Cela peut se produire pour plusieurs raisons. Pour plus d'informations, voir Que dois-je faire si mon agent est hors ligne ?

Type : String

Valeurs valides : `ONLINE | OFFLINE`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande

L'exemple suivant renvoie des informations sur un agent spécifié dans une demande.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/agent-1234567890abcdef0"
}
```

Exemple de réponse

L'exemple de réponse suivant décrit un agent qui utilise un point de terminaison de service public.

```
{
    "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/
agent-1234567890abcdef0",
    "Name": "Data center migration agent",
    "Status": "ONLINE",
    "LastConnectionTime": "2022-10-17T17:21:35.540000+00:00",
    "CreationTime": "2022-10-05T20:52:29.499000+00:00",
    "EndpointType": "PUBLIC",
    "Platform": {
        "Version": "2"
    }
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationAzureBlob

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert pour Microsoft Azure Blob Storage.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de votre emplacement de transfert Azure Blob Storage.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "AccessTier": "string",
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlobType": "string",
   "CmkSecretConfig": {
```

```
        "KmsKeyArn": "string",
        "SecretArn": "string"
    },
    "CreationTime": number,
    "CustomSecretConfig": {
        "SecretAccessRoleArn": "string",
        "SecretArn": "string"
    },
    "LocationArn": "string",
    "LocationUri": "string",
    "ManagedSecretConfig": {
        "SecretArn": "string"
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AccessTier

Le niveau d'accès vers lequel vous souhaitez transférer vos objets ou fichiers. Cela s'applique uniquement lorsque l'emplacement est utilisé comme destination de transfert. Pour plus d'informations, consultez la section Niveaux d'accès.

Type : String

Valeurs valides : `HOT | COOL | ARCHIVE`

AgentArns

Les ARNs DataSync agents qui peuvent se connecter à votre conteneur Azure Blob Storage.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

La méthode d'authentification DataSync utilisée pour accéder à votre Azure Blob Storage. DataSync peut accéder au stockage blob à l'aide d'une signature d'accès partagé (SAS).

Type : String

Valeurs valides : `SAS | NONE`

BlobType

Type de blob que vous souhaitez attribuer à vos objets ou fichiers lorsque vous les transférez dans Azure Blob Storage. Actuellement, DataSync ne prend en charge le transfert de données vers Azure Blob Storage que sous forme de blobs de blocs. Pour plus d'informations sur les types de blob, consultez la documentation Azure Blob Storage.

Type : String

Valeurs valides : `BLOCK`

CmkSecretConfig

Décrit les informations de configuration d'un secret DataSync géré, tel qu'un jeton d'authentification DataSync utilisé pour accéder à un emplacement de stockage spécifique, avec un code géré par le client AWS KMS key.

Type : objet CmkSecretConfig

CreationTime

Heure à laquelle votre emplacement de transfert Azure Blob Storage a été créé.

Type : Timestamp

CustomSecretConfig

Décrit les informations de configuration d'un secret géré par le client, tel qu'un jeton d'authentification DataSync utilisé pour accéder à un emplacement de stockage spécifique, avec un secret géré par le client. AWS KMS key

Type : objet CustomSecretConfig

LocationArn

L'ARN de votre emplacement de transfert Azure Blob Storage.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

URL du conteneur Azure Blob Storage impliqué dans votre transfert.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

ManagedSecretConfig

Décrit les informations de configuration d'un secret DataSync géré, tel qu'un jeton d'authentification DataSync utilisé pour accéder à un emplacement de stockage spécifique. DataSync utilise la clé KMS AWS gérée par défaut pour chiffrer ce secret. AWS Secrets Manager

Type : objet ManagedSecretConfig

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationEfs

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert pour un système de fichiers Amazon EFS.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Le nom de ressource Amazon (ARN) de l'emplacement du système de fichiers Amazon EFS sur lequel vous souhaitez obtenir des informations.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "AccessPointArn": "string",
   "CreationTime": number,
   "Ec2Config": {
      "SecurityGroupArns": [ "string" ],
      "SubnetArn": "string"
```

```
    },
    "FileSystemAccessRoleArn": "string",
    "InTransitEncryption": "string",
    "LocationArn": "string",
    "LocationUri": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AccessPointArn

L'ARN du point d'accès DataSync utilisé pour accéder au système de fichiers Amazon EFS.

Pour plus d'informations, consultez la section Accès aux systèmes de fichiers restreints.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

CreationTime

Heure à laquelle le lieu a été créé.

Type : Timestamp

Ec2Config

Sous-réseau et groupes de sécurité AWS DataSync utilisés pour se connecter à l'une des cibles de montage de votre système de fichiers Amazon EFS.

Type : objet Ec2Config

FileSystemAccessRoleArn

Rôle AWS Identity and Access Management (IAM) qui permet d'accéder DataSync à votre système de fichiers Amazon EFS.

Pour plus d'informations, consultez la section Création d'un rôle DataSync IAM pour l'accès au système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

InTransitEncryption

Indique si le chiffrement TLS (Transport Layer Security) est DataSync utilisé lors du transfert de données vers ou depuis le système de fichiers Amazon EFS.

Type : String

Valeurs valides : `NONE | TLS1_2`

LocationArn

L'ARN de l'emplacement du système de fichiers Amazon EFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

URL de l'emplacement du système de fichiers Amazon EFS.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande

L'exemple suivant montre comment obtenir des informations sur l'emplacement d'un système de fichiers Amazon EFS spécifique.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-12abcdef012345678"
}
```

Exemple de réponse

L'exemple suivant renvoie les détails de localisation d'un système de fichiers Amazon EFS.

```
{
    "CreationTime": 1653319021.353,
    "Ec2Config": {
        "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/
subnet-1234567890abcdef1",
        "SecurityGroupArns": [
            "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
        ]
    },
    "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-
abcdef01234567890",
    "LocationUri": "efs://us-east-2.fs-021345abcdef6789/"
}
```

Exemple de réponse : description de l'emplacement d'un système de fichiers Amazon EFS restreint

L'exemple suivant renvoie les détails de localisation d'un système de fichiers Amazon EFS à accès restreint`AccessPointArn`, notamment les `InTransitEncryption` éléments`FileSystemAccessRoleArn`, et.

```
{
    "CreationTime": 1653319021.353,
    "AccessPointArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:access-point/
fsap-1234567890abcdef0",
    "Ec2Config": {
        "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/
subnet-1234567890abcdef1",
        "SecurityGroupArns": [
            "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
        ]
    },
    "FileSystemAccessRoleArn": "arn:aws:iam::111222333444:role/
AwsDataSyncFullAccessNew",
    "InTransitEncryption": "TLS1_2",
    "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-
abcdef01234567890",
    "LocationUri": "efs://us-east-2.fs-021345abcdef6789/",
    "Subdirectory": "/mount/path",
    "Tags": [{
        "Key": "Name",
        "Value": "ElasticFileSystem-1"
    }]
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2

- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationFsxLustre

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert FSx pour un système de fichiers Amazon for Lustre.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Le nom de ressource Amazon (ARN) de l'emplacement FSx pour Lustre à décrire.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "SecurityGroupArns": [ "string" ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Heure à laquelle l'emplacement FSx pour Lustre a été créé.

Type : Timestamp

LocationArn

Le nom de ressource Amazon (ARN) de l'emplacement FSx pour Lustre qui a été décrit.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI de l'emplacement FSx pour Lustre qui a été décrit.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

SecurityGroupArns

Les Amazon Resource Names (ARNs) des groupes de sécurité configurés pour le système de fichiers FSx for Lustre.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationFsxOntap

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert FSx pour un système de fichiers Amazon for NetApp ONTAP.

> **Note**
>
> Si votre position utilise le protocole SMB, l'`DescribeLocationFsxOntap`opération ne renvoie pas réellement un`Password`.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement du système FSx de fichiers ONTAP sur lequel vous souhaitez obtenir des informations.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
```

```
    "CreationTime": number,
    "FsxFilesystemArn": "string",
    "LocationArn": "string",
    "LocationUri": "string",
    "Protocol": {
       "NFS": {
          "MountOptions": {
             "Version": "string"
          }
       },
       "SMB": {
          "Domain": "string",
          "MountOptions": {
             "Version": "string"
          },
          "Password": "string",
          "User": "string"
       }
    },
    "SecurityGroupArns": [ "string" ],
    "StorageVirtualMachineArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Heure à laquelle le lieu a été créé.

Type : Timestamp

FsxFilesystemArn

L'ARN du système de fichiers FSx for ONTAP.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]*:[0-9]{12}:file-system/fs-.*$`

LocationArn

L'ARN de l'emplacement du système de fichiers FSx pour ONTAP.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'identifiant de ressource uniforme (URI) de l'emplacement du système FSx de fichiers ONTAP.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Protocol

Spécifie le protocole de transfert de données AWS DataSync utilisé pour accéder à votre système de FSx fichiers Amazon.

Type : objet FsxProtocol

SecurityGroupArns

Les groupes de sécurité DataSync utilisés pour accéder à votre système de fichiers FSx for ONTAP.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

StorageVirtualMachineArn

L'ARN de la machine virtuelle de stockage (SVM) de votre système de fichiers FSx for ONTAP vers ou depuis laquelle vous copiez des données.

Type : String

Contraintes de longueur : longueur maximale de 162.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-0-9]+:[0-9]{12}:storage-virtual-machine/fs-[0-9a-f]+/svm-[0-9a-f]{17,}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

DescribeLocationFsxOpenZfs

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert FSx pour un système de fichiers Amazon pour OpenZFS.

> **Note**
>
> Les éléments de réponse associés à `SMB` ne sont pas pris en charge par l'`DescribeLocationFsxOpenZfs`opération.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Nom de ressource Amazon (ARN) de l'emplacement FSx pour OpenZFS à décrire.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
```

```
    "CreationTime": number,
    "LocationArn": "string",
    "LocationUri": "string",
    "Protocol": {
       "NFS": {
          "MountOptions": {
             "Version": "string"
          }
       },
       "SMB": {
          "Domain": "string",
          "MountOptions": {
             "Version": "string"
          },
          "Password": "string",
          "User": "string"
       }
    },
    "SecurityGroupArns": [ "string" ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Heure à laquelle l'emplacement FSx pour OpenZFS a été créé.

Type : Timestamp

LocationArn

L'ARN de l'emplacement FSx pour OpenZFS décrit.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'identifiant de ressource uniforme (URI) de l'emplacement FSx pour OpenZFS décrit.

Exemple : `fsxz://us-west-2.fs-1234567890abcdef02/fsx/folderA/folder`

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Protocol

Type de protocole AWS DataSync utilisé pour accéder à votre système de fichiers.

Type : objet FsxProtocol

SecurityGroupArns

Les groupes ARNs de sécurité configurés FSx pour le système de fichiers OpenZFS.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationFsxWindows

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert FSx pour un système de fichiers Amazon pour Windows File Server.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement du serveur de fichiers FSx pour Windows.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "CreationTime": number,
   "Domain": "string",
   "LocationArn": "string",
   "LocationUri": "string",
   "SecurityGroupArns": [ "string" ],
   "User": "string"
```

```
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Heure à laquelle l'emplacement FSx du serveur de fichiers Windows a été créé.

Type : Timestamp

Domain

Nom du domaine Microsoft Active Directory auquel appartient le système de fichiers FSx pour Windows File Server.

Type : String

Contraintes de longueur : longueur maximale de 253.

Modèle : `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

LocationArn

L'ARN de l'emplacement du serveur de fichiers FSx pour Windows.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'identifiant de ressource uniforme (URI) de FSx l'emplacement du serveur de fichiers Windows.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

SecurityGroupArns

Les groupes ARNs de EC2 sécurité Amazon qui fournissent l'accès au sous-réseau préféré de votre système de fichiers.

Pour plus d'informations sur la configuration des groupes de sécurité pour l'accès au système de fichiers, consultez le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

User

Utilisateur autorisé à monter et à accéder au système de fichiers FSx for Windows File Server.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationHdfs

Fournit des détails sur la configuration d'un emplacement de AWS DataSync transfert pour un système de fichiers distribué Hadoop (HDFS).

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement HDFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlockSize": number,
   "CreationTime": number,
   "KerberosPrincipal": "string",
   "KmsKeyProviderUri": "string",
   "LocationArn": "string",
```

```
    "LocationUri": "string",
    "NameNodes": [
       {
          "Hostname": "string",
          "Port": number
       }
    ],
    "QopConfiguration": {
       "DataTransferProtection": "string",
       "RpcProtection": "string"
    },
    "ReplicationFactor": number,
    "SimpleUser": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AgentArns

Les ARNs DataSync agents qui peuvent se connecter à votre cluster HDFS.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

Type d'authentification utilisé pour déterminer l'identité de l'utilisateur.

Type : String

Valeurs valides : `SIMPLE | KERBEROS`

BlockSize

Taille des blocs de données à écrire dans le cluster HDFS.

Type : entier

Plage valide : valeur minimale de 1048576. Valeur maximale de 1073741824.

CreationTime

Heure à laquelle l'emplacement HDFS a été créé.

Type : Timestamp

KerberosPrincipal

Le principal Kerberos ayant accès aux fichiers et dossiers du cluster HDFS. Ce paramètre est utilisé si le `AuthenticationType` est défini comme`KERBEROS`.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^.+$`

KmsKeyProviderUri

L'URI du serveur de gestion de clés (KMS) du cluster HDFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Modèle : `^kms:\/\/http[s]?@(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9])(;(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9]))*:[0-9]{1,5}\/kms$`

LocationArn

L'ARN de l'emplacement HDFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI de l'emplacement HDFS.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

NameNodes

Celui NameNode qui gère l'espace de noms HDFS.

Type : tableau d'objets HdfsNameNode

Membres du tableau : Nombre minimum de 1 élément.

QopConfiguration

La configuration de la qualité de protection (QOP), qui spécifie les paramètres d'appel de procédure à distance (RPC) et de protection contre le transfert de données configurés sur le cluster HDFS.

Type : objet QopConfiguration

ReplicationFactor

Le nombre de DataNodes vers lesquels répliquer les données lors de l'écriture dans le cluster HDFS.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 512.

SimpleUser

Nom d'utilisateur permettant d'identifier le client sur le système d'exploitation hôte. Ce paramètre est utilisé si le `AuthenticationType` est défini comme`SIMPLE`.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationNfs

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert pour un serveur de fichiers NFS (Network File System).

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement NFS sur lequel vous souhaitez obtenir des informations.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "MountOptions": {
      "Version": "string"
```

```
    },
    "OnPremConfig": {
       "AgentArns": [ "string" ]
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Heure à laquelle l'emplacement NFS a été créé.

Type : Timestamp

LocationArn

L'ARN de l'emplacement NFS.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI de l'emplacement NFS.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

MountOptions

Les options de montage DataSync utilisées pour monter votre serveur de fichiers NFS.

Type : objet NfsMountOptions

OnPremConfig

Les AWS DataSync agents qui peuvent se connecter à votre serveur de fichiers NFS (Network File System).

Type : objet OnPremConfig

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

exemple

L'exemple suivant renvoie des informations sur l'emplacement NFS spécifié dans l'exemple de demande.

Exemple de demande

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
}
```

exemple

Cet exemple illustre une utilisation de DescribeLocationNfs.

Exemple de réponse

```
{
   "CreationTime": 1532660733.39,
   "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa",
   "LocationUri": "hostname.amazon.com",
   "OnPremConfig": {
      "AgentArns": [ "arn:aws:datasync:us-east-2:111222333444:agent/
agent-0b0addbeef44b3nfs" ]
   }
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationObjectStorage

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert pour un système de stockage d'objets.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement du système de stockage d'objets.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "AccessKey": "string",
   "AgentArns": [ "string" ],
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CreationTime": number,
```

```
    "CustomSecretConfig": {
       "SecretAccessRoleArn": "string",
       "SecretArn": "string"
    },
    "LocationArn": "string",
    "LocationUri": "string",
    "ManagedSecretConfig": {
       "SecretArn": "string"
    },
    "ServerCertificate": blob,
    "ServerPort": number,
    "ServerProtocol": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AccessKey

La clé d'accès (par exemple, un nom d'utilisateur) requise pour s'authentifier auprès du système de stockage d'objets.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `^.*$`

AgentArns

Les ARNs DataSync agents qui peuvent se connecter à votre système de stockage d'objets.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CmkSecretConfig

Décrit les informations de configuration pour un secret DataSync géré, tel qu'un jeton d'authentification ou un ensemble d'informations d'identification DataSync utilisé pour accéder à un lieu de transfert spécifique, et un secret géré par le client AWS KMS key.

Type : objet CmkSecretConfig

CreationTime

Heure à laquelle le lieu a été créé.

Type : Timestamp

CustomSecretConfig

Décrit les informations de configuration d'un secret géré par le client, tel qu'un jeton d'authentification ou un ensemble d'informations d'identification DataSync utilisé pour accéder à un lieu de transfert spécifique, et d'un secret géré par le client. AWS KMS key

Type : objet CustomSecretConfig

LocationArn

L'ARN de l'emplacement du système de stockage d'objets.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI de l'emplacement du système de stockage d'objets.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

ManagedSecretConfig

Décrit les informations de configuration d'un secret DataSync géré, tel qu'un jeton d'authentification ou un ensemble d'informations d'identification permettant DataSync d'accéder à

un emplacement de transfert spécifique. DataSync utilise la clé KMS AWS gérée par défaut pour chiffrer ce secret. AWS Secrets Manager

Type : objet ManagedSecretConfig

ServerCertificate

Chaîne de certificats permettant DataSync de s'authentifier auprès de votre système de stockage d'objets si celui-ci utilise une autorité de certification (CA) privée ou autosignée.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 32 768.

ServerPort

Port sur lequel votre serveur de stockage d'objets accepte le trafic réseau entrant (par exemple, le port 443).

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 65536.

ServerProtocol

Protocole utilisé par votre système de stockage d'objets pour communiquer.

Type : String

Valeurs valides : `HTTPS` | `HTTP`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationS3

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert pour un compartiment S3.

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement Amazon S3.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "AgentArns": [ "string" ],
   "CreationTime": number,
   "LocationArn": "string",
   "LocationUri": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
```

```
    "S3StorageClass": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AgentArns

Le ARNs nombre d' DataSync agents déployés sur votre Outpost lorsque vous utilisez Amazon S3 on Outposts.

Pour plus d'informations, voir Déployer votre DataSync agent sur AWS Outposts.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

Heure à laquelle l'emplacement Amazon S3 a été créé.

Type : Timestamp

LocationArn

L'ARN de l'emplacement Amazon S3.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

URL de l'emplacement Amazon S3 décrit.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

S3Config

Spécifie le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) DataSync utilisé pour accéder à votre compartiment S3.

Pour plus d'informations, consultez la section Fournir DataSync un accès aux compartiments S3.

Type : objet S3Config

S3StorageClass

Lorsque Amazon S3 est un emplacement de destination, il s'agit de la classe de stockage que vous avez choisie pour vos objets.

Certaines classes de stockage ont des comportements qui peuvent affecter les coûts de stockage de votre Amazon S3. Pour plus d'informations, consultez la section Considérations relatives aux classes de stockage associées aux transferts Amazon S3.

Type : String

Valeurs valides : `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

exemple

L'exemple suivant renvoie des informations sur l'emplacement Amazon S3 spécifié dans l'exemple de demande.

Exemple de demande

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

exemple

Cet exemple illustre une utilisation de DescribeLocation S3.

Exemple de réponse

```
{
   "CreationTime": 1532660733.39,
   "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3",
   "LocationUri": "s3://amzn-s3-demo-bucket",
   "S3Config": {
      "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/amzn-s3-demo-bucket-
access-role",
   }
    "S3StorageClass": "STANDARD"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeLocationSmb

Fournit des informations sur la configuration d'un emplacement de AWS DataSync transfert pour un serveur de fichiers SMB (Server Message Block).

Syntaxe de la requête

```
{
   "LocationArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement SMB sur lequel vous souhaitez obtenir des informations.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "CreationTime": number,
   "DnsIpAddresses": [ "string" ],
   "Domain": "string",
   "KerberosPrincipal": "string",
```

```
    "LocationArn": "string",
    "LocationUri": "string",
    "MountOptions": {
       "Version": "string"
    },
    "User": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AgentArns

Les ARNs DataSync agents qui peuvent se connecter à votre serveur de fichiers SMB.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

Protocole d'authentification DataSync utilisé pour se connecter à votre serveur de fichiers SMB.

Type : String

Valeurs valides : `NTLM | KERBEROS`

CreationTime

Heure à laquelle l'emplacement SMB a été créé.

Type : Timestamp

DnsIpAddresses

Les IPv6 adresses IPv4 ou des serveurs DNS auxquels appartient votre serveur de fichiers SMB. Cet élément ne s'applique que s'`AuthenticationType`il est défini sur`KERBEROS`.

Type : tableau de chaînes

Membres du tableau : nombre maximum de 2 éléments.

Contraintes de longueur : longueur minimale de 7. Longueur maximale de 39

Modèle : `\A((25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d)){3}|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6}))\z`

Domain

Nom du domaine Windows auquel appartient le serveur de fichiers SMB. Cet élément ne s'applique que s'`AuthenticationType`il est défini sur`NTLM`.

Type : String

Contraintes de longueur : longueur maximale de 253.

Modèle : `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

KerberosPrincipal

Le principal Kerberos autorisé à accéder aux fichiers, aux dossiers et aux métadonnées des fichiers sur votre serveur de fichiers SMB.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^.+$`

LocationArn

L'ARN de l'emplacement SMB.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

L'URI de l'emplacement SMB.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

MountOptions

Version du protocole SMB DataSync utilisée pour accéder à votre serveur de fichiers SMB.

Type : objet SmbMountOptions

User

L'utilisateur qui peut monter et accéder aux fichiers, aux dossiers et aux métadonnées des fichiers sur votre serveur de fichiers SMB. Cet élément ne s'applique que s'`AuthenticationType`il est défini sur`NTLM`.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

exemple

Cet exemple illustre une utilisation de DescribeLocationSmb.

Exemple de demande

```
{
  "arn:aws:datasync:us-east-1:111222333444:location/loc-0f01451b140b2af49"
}
```

exemple

Cet exemple illustre une utilisation de DescribeLocationSmb.

Exemple de réponse

```
{
   "AgentArns":[
      "arn:aws:datasync:us-east-2:111222333444:agent/agent-0bc3b3dc9bbc15145",
      "arn:aws:datasync:us-east-2:111222333444:agent/agent-04b3fe3d261a18c8f"
   ],
   "CreationTime":"1532660733.39",
   "Domain":"AMAZON",
   "LocationArn":"arn:aws:datasync:us-east-1:111222333444:location/
loc-0f01451b140b2af49",
   "LocationUri":"smb://hostname.amazon.com/share",
   "MountOptions":{
      "Version":"SMB3"
   },
   "User":"user-1"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS

- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeTask

Fournit des informations sur une tâche, qui définit où et comment AWS DataSync vos données sont transférées.

Syntaxe de la requête

```
{
   "TaskArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

TaskArn

Spécifie le nom de ressource Amazon (ARN) de la tâche de transfert sur laquelle vous souhaitez obtenir des informations.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "CloudWatchLogGroupArn": "string",
   "CreationTime": number,
   "CurrentTaskExecutionArn": "string",
   "DestinationLocationArn": "string",
   "DestinationNetworkInterfaceArns": [ "string" ],
   "ErrorCode": "string",
   "ErrorDetail": "string",
```

```
    "Excludes": [
       {
          "FilterType": "string",
          "Value": "string"
       }
    ],
    "Includes": [
       {
          "FilterType": "string",
          "Value": "string"
       }
    ],
    "ManifestConfig": {
       "Action": "string",
       "Format": "string",
       "Source": {
          "S3": {
             "BucketAccessRoleArn": "string",
             "ManifestObjectPath": "string",
             "ManifestObjectVersionId": "string",
             "S3BucketArn": "string"
          }
       }
    },
    "Name": "string",
    "Options": {
       "Atime": "string",
       "BytesPerSecond": number,
       "Gid": "string",
       "LogLevel": "string",
       "Mtime": "string",
       "ObjectTags": "string",
       "OverwriteMode": "string",
       "PosixPermissions": "string",
       "PreserveDeletedFiles": "string",
       "PreserveDevices": "string",
       "SecurityDescriptorCopyFlags": "string",
       "TaskQueueing": "string",
       "TransferMode": "string",
       "Uid": "string",
       "VerifyMode": "string"
    },
    "Schedule": {
       "ScheduleExpression": "string",
```

```
        "Status": "string"
    },
    "ScheduleDetails": {
        "DisabledBy": "string",
        "DisabledReason": "string",
        "StatusUpdateTime": number
    },
    "SourceLocationArn": "string",
    "SourceNetworkInterfaceArns": [ "string" ],
    "Status": "string",
    "TaskArn": "string",
    "TaskMode": "string",
    "TaskReportConfig": {
        "Destination": {
            "S3": {
                "BucketAccessRoleArn": "string",
                "S3BucketArn": "string",
                "Subdirectory": "string"
            }
        },
        "ObjectVersionIds": "string",
        "OutputType": "string",
        "Overrides": {
            "Deleted": {
                "ReportLevel": "string"
            },
            "Skipped": {
                "ReportLevel": "string"
            },
            "Transferred": {
                "ReportLevel": "string"
            },
            "Verified": {
                "ReportLevel": "string"
            }
        },
        "ReportLevel": "string"
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CloudWatchLogGroupArn

Le nom de ressource Amazon (ARN) d'un groupe de CloudWatch journaux Amazon pour surveiller votre tâche.

Pour plus d'informations, consultez la section Surveillance des transferts de données à l'aide CloudWatch des journaux.

Type : String

Contraintes de longueur : longueur maximale de 562.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

CreationTime

Heure à laquelle la tâche a été créée.

Type : Timestamp

CurrentTaskExecutionArn

L'ARN de la dernière exécution de tâche.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

DestinationLocationArn

L'ARN du lieu de destination de votre transfert.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

DestinationNetworkInterfaceArns

Les ARNs interfaces réseau DataSync créées pour votre emplacement de destination.

Type : tableau de chaînes

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:aws[\-a-z]{0,}:ec2:[a-z\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

ErrorCode

En cas de problème avec votre tâche, vous pouvez utiliser le code d'erreur pour résoudre le problème. Pour plus d'informations, consultez la section Résolution des problèmes liés aux DataSync transferts.

Type : String

ErrorDetail

En cas de problème avec votre tâche, vous pouvez utiliser les détails de l'erreur pour résoudre le problème. Pour plus d'informations, consultez la section Résolution des problèmes liés aux DataSync transferts.

Type : String

Excludes

Les filtres d'exclusion qui définissent les fichiers, les objets et les dossiers de votre emplacement source que vous ne DataSync souhaitez pas transférer. Pour plus d'informations et des exemples, voir Spécifier les DataSync transferts à l'aide de filtres.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Includes

Ils incluent des filtres qui définissent les fichiers, les objets et les dossiers que vous souhaitez DataSync transférer dans votre emplacement source. Pour plus d'informations et des exemples, voir Spécifier les DataSync transferts à l'aide de filtres.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

ManifestConfig

Configuration du manifeste qui répertorie les fichiers ou les objets que vous DataSync souhaitez transférer. Pour plus d'informations, voir Spécifier les DataSync transferts à l'aide d'un manifeste.

Type : objet ManifestConfig

Name

Le nom de votre tâche.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Options

Les paramètres de la tâche. Par exemple, quelles métadonnées de fichier sont préservées, comment l'intégrité des données est vérifiée à la fin du transfert, limites de bande passante, entre autres options.

Type : objet Options

Schedule

Le calendrier selon lequel vous souhaitez que votre tâche soit exécutée. Pour plus d'informations, veuillez consulter la rubrique Planification de votre tâche.

Type : objet TaskSchedule

ScheduleDetails

Les détails de votre planning de tâches.

Type : objet TaskScheduleDetails

SourceLocationArn

L'ARN de l'emplacement source de votre transfert.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

SourceNetworkInterfaceArns

Les ARNs interfaces réseau DataSync créées pour votre emplacement source.

Type : tableau de chaînes

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:aws[\-a-z]{0,}:ec2:[a-z\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

Status

État de votre tâche. Pour plus d'informations sur la signification de chaque statut, consultez la section Statuts des tâches.

Type : String

Valeurs valides : `AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE`

TaskArn

L'ARN de votre tâche.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

TaskMode

Le mode tâche que vous utilisez. Pour plus d'informations, voir Choisir un mode de tâche pour le transfert de données.

Type : String

Valeurs valides : `BASIC | ENHANCED`

TaskReportConfig

La configuration de votre rapport de tâches, qui fournit des informations détaillées sur votre DataSync transfert. Pour plus d'informations, consultez la section Surveillance de vos DataSync transferts à l'aide de rapports de tâches.

Type : objet TaskReportConfig

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande

L'exemple suivant indique l'ARN d'une DataSync tâche sur laquelle vous souhaitez obtenir des informations.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Exemple de réponse

L'exemple suivant montre une `DescribeTask` réponse.

```
{
```

```
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026",
  "Name": "MyTask",
  "TaskMode": "BASIC",
  "Status": "RUNNING",
  "SourceLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-1111aaaa2222bbbb3",
  "DestinationLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-0000zzzz1111yyyy2",
  "CurrentTaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f",
  "CreationTime": 1532660733.39,
  "Options": {
    "Atime": "BEST_EFFORT",
    "BytesPerSecond": 1000,
    "Gid": "NONE",
    "Mtime": "PRESERVE",
    "PosixPermissions": "PRESERVE",
    "PreserveDevices": "NONE",
    "PreserveDeletedFiles": "PRESERVE",
    "Uid": "NONE",
    "VerifyMode": "POINT_IN_TIME_CONSISTENT"
  },
  "CloudWatchLogGroupArn": "arn:aws:logs:us-east-2:111222333444:log-group:/log-group-
name:*"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

DescribeTaskExecution

Fournit des informations sur l'exécution de votre AWS DataSync tâche. Vous pouvez utiliser cette opération pour suivre la progression d'un transfert de données en cours ou vérifier les résultats du transfert.

> **Note**
>
> Certains éléments de `DescribeTaskExecution` réponse ne concernent qu'un mode de tâche spécifique. Pour plus d'informations, voir Comprendre les différences entre les modes de tâche et Comprendre les compteurs de performance du transfert de données.

Syntaxe de la requête

```
{
   "TaskExecutionArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

TaskExecutionArn

Spécifie le nom de ressource Amazon (ARN) de l'exécution de la tâche sur laquelle vous souhaitez obtenir des informations.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "BytesCompressed": number,
   "BytesTransferred": number,
   "BytesWritten": number,
   "EndTime": number,
   "EstimatedBytesToTransfer": number,
   "EstimatedFilesToDelete": number,
   "EstimatedFilesToTransfer": number,
   "Excludes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "FilesDeleted": number,
   "FilesFailed": {
      "Delete": number,
      "Prepare": number,
      "Transfer": number,
      "Verify": number
   },
   "FilesListed": {
      "AtDestinationForDelete": number,
      "AtSource": number
   },
   "FilesPrepared": number,
   "FilesSkipped": number,
   "FilesTransferred": number,
   "FilesVerified": number,
   "Includes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "LaunchTime": number,
   "ManifestConfig": {
      "Action": "string",
      "Format": "string",
      "Source": {
         "S3": {
```

```
            "BucketAccessRoleArn": "string",
            "ManifestObjectPath": "string",
            "ManifestObjectVersionId": "string",
            "S3BucketArn": "string"
         }
      }
   },
   "Options": {
      "Atime": "string",
      "BytesPerSecond": number,
      "Gid": "string",
      "LogLevel": "string",
      "Mtime": "string",
      "ObjectTags": "string",
      "OverwriteMode": "string",
      "PosixPermissions": "string",
      "PreserveDeletedFiles": "string",
      "PreserveDevices": "string",
      "SecurityDescriptorCopyFlags": "string",
      "TaskQueueing": "string",
      "TransferMode": "string",
      "Uid": "string",
      "VerifyMode": "string"
   },
   "ReportResult": {
      "ErrorCode": "string",
      "ErrorDetail": "string",
      "Status": "string"
   },
   "Result": {
      "ErrorCode": "string",
      "ErrorDetail": "string",
      "PrepareDuration": number,
      "PrepareStatus": "string",
      "TotalDuration": number,
      "TransferDuration": number,
      "TransferStatus": "string",
      "VerifyDuration": number,
      "VerifyStatus": "string"
   },
   "StartTime": number,
   "Status": "string",
   "TaskExecutionArn": "string",
   "TaskMode": "string",
```

```
    "TaskReportConfig": {
       "Destination": {
          "S3": {
             "BucketAccessRoleArn": "string",
             "S3BucketArn": "string",
             "Subdirectory": "string"
          }
       },
       "ObjectVersionIds": "string",
       "OutputType": "string",
       "Overrides": {
          "Deleted": {
             "ReportLevel": "string"
          },
          "Skipped": {
             "ReportLevel": "string"
          },
          "Transferred": {
             "ReportLevel": "string"
          },
          "Verified": {
             "ReportLevel": "string"
          }
       },
       "ReportLevel": "string"
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BytesCompressed

Nombre d'octets physiques DataSync transférés sur le réseau après compression (si la compression est possible). Ce nombre est généralement inférieur à BytesTransferredsauf si les données ne sont pas compressibles.

Type : long

BytesTransferred

Nombre d'octets DataSync envoyés au réseau avant la compression (si la compression est possible). Pour le nombre d'octets transférés sur le réseau, consultez BytesCompressed.

Type : long

BytesWritten

Le nombre d'octets logiques qui écrivent DataSync réellement sur l'emplacement de destination.

Type : long

EndTime

Heure de fin de la tâche de transfert.

Type : Timestamp

EstimatedBytesToTransfer

Le nombre d'octets logiques qui DataSync devraient écrire sur l'emplacement de destination.

Type : long

EstimatedFilesToDelete

Le nombre de fichiers, d'objets et de répertoires qui DataSync devraient être supprimés dans votre emplacement de destination. Si vous ne configurez pas votre tâche pour supprimer des données dans la destination qui ne figurent pas dans la source, la valeur est toujours`0`.

Type : long

EstimatedFilesToTransfer

Le nombre de fichiers, d'objets et de répertoires qui DataSync devraient être transférés sur le réseau. Cette valeur est calculée lors de la DataSync préparation du transfert.

La façon dont cela est calculé dépend principalement de la configuration du mode de transfert de votre tâche :

- Il `TranserMode` est défini sur `CHANGED` - Le calcul est basé sur la comparaison du contenu des emplacements source et de destination et sur la détermination de la différence à transférer. La différence peut inclure :

- Tout ce qui est ajouté ou modifié à l'emplacement source.
- Tout ce qui se trouve aux deux emplacements et qui est modifié à destination après un transfert initial (sauf s'OverwriteModeil est défini surNEVER).
- (Mode tâche de base uniquement) Nombre d'éléments qui devraient DataSync être supprimés (s'il PreserveDeletedFilesest défini surREMOVE).

- Si la valeur TranserMode est définie sur ALL - Le calcul est basé uniquement sur les éléments DataSync trouvés à l'emplacement source.

Type : long

Excludes

Liste de règles de filtrage qui excluent des données spécifiques lors de votre transfert. Pour plus d'informations et des exemples, voir Filtrer les données transférées par DataSync.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

FilesDeleted

Le nombre de fichiers, d'objets et de répertoires DataSync réellement supprimés dans votre emplacement de destination. Si vous ne configurez pas votre tâche pour supprimer des données dans la destination qui ne figurent pas dans la source, la valeur est toujours0.

Type : long

FilesFailed

Nombre d'objets dont la préparation, le transfert, la vérification et la suppression DataSync échouent lors de l'exécution de la tâche.

> **Note**
>
> S'applique uniquement aux tâches en mode amélioré.

Type : objet TaskExecutionFilesFailedDetail

FilesListed

Le nombre d'objets DataSync trouvés sur vos sites.

> **Note**
>
> S'applique uniquement aux tâches en mode amélioré.

Type : objet TaskExecutionFilesListedDetail

FilesPrepared

Le nombre d'objets qui DataSync tenteront d'être transférés après avoir comparé vos emplacements source et de destination.

> **Note**
>
> S'applique uniquement aux tâches en mode amélioré.

Ce compteur n'est pas applicable si vous configurez votre tâche pour transférer toutes les données. Dans ce scénario, DataSync copie tout de la source vers la destination sans comparer les différences entre les emplacements.

Type : long

FilesSkipped

Le nombre de fichiers, d'objets et de répertoires DataSync ignorés lors de votre transfert.

Type : long

FilesTransferred

Nombre de fichiers, d'objets et de répertoires DataSync réellement transférés sur le réseau. Cette valeur est mise à jour régulièrement pendant l'exécution de la tâche lorsqu'un élément est lu depuis la source et envoyé sur le réseau.

En cas d' DataSync échec du transfert, cette valeur peut être inférieure à`EstimatedFilesToTransfer`. Dans certains cas, cette valeur peut également être supérieure à`EstimatedFilesToTransfer`. Cet élément est spécifique à l'implémentation pour certains types d'emplacement. Ne l'utilisez donc pas comme une indication exacte de ce qui est transféré ou pour surveiller l'exécution de vos tâches.

Type : long

FilesVerified

Le nombre de fichiers, d'objets et de répertoires qui sont DataSync vérifiés lors de votre transfert.

> **Note**
>
> Lorsque vous configurez votre tâche pour vérifier uniquement les données transférées, DataSync elle ne vérifie pas les répertoires dans certains cas ni les fichiers qui ne parviennent pas à être transférés.

Type : long

Includes

Liste de règles de filtrage qui incluent des données spécifiques lors de votre transfert. Pour plus d'informations et des exemples, voir Filtrer les données transférées par DataSync.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

LaunchTime

Heure à laquelle l'exécution de la tâche commence réellement. Pour les tâches ne figurant pas dans la file d'attente, `LaunchTime` `StartTime` elles sont généralement identiques. Pour les tâches en file d'attente, `LaunchTime` c'est généralement plus tard que `StartTime` parce que les tâches précédemment mises en file d'attente doivent terminer leur exécution avant que les nouvelles tâches puissent commencer.

Type : Timestamp

ManifestConfig

Configuration du manifeste qui répertorie les fichiers ou les objets à transférer. Pour plus d'informations, voir Spécifier les DataSync transferts à l'aide d'un manifeste.

Type : objet ManifestConfig

Options

Indique comment votre tâche de transfert est configurée. Ces options incluent le mode DataSync de gestion des fichiers, des objets et des métadonnées associées lors de votre transfert. Vous

pouvez également spécifier comment vérifier l'intégrité des données, définir des limites de bande passante pour votre tâche, entre autres options.

Chaque option possède une valeur par défaut. À moins que vous n'en ayez besoin, vous n'avez pas à configurer d'option avant d'appeler StartTaskExecution.

Vous pouvez également remplacer vos options de tâche pour chaque exécution de tâche. Par exemple, vous souhaiterez peut-être ajuster le `LogLevel` pour une exécution individuelle.

Type : objet Options

ReportResult

Indique si un rapport de tâches complet a été DataSync généré pour votre transfert.

Type : objet ReportResult

Result

Résultat de l'exécution de la tâche.

Type : objet TaskExecutionResultDetail

StartTime

Heure à laquelle la DataSync demande est envoyée pour démarrer l'exécution de la tâche. Pour les tâches ne figurant pas dans la file d'attente, `LaunchTime` `StartTime` elles sont généralement identiques. Pour les tâches en file d'attente, `LaunchTime` c'est généralement plus tard que `StartTime` parce que les tâches précédemment mises en file d'attente doivent terminer leur exécution avant que les nouvelles tâches puissent commencer.

Type : Timestamp

Status

État de l'exécution de la tâche.

Pour des informations détaillées sur les états d'exécution des tâches, consultez la section Statuts d'exécution des tâches.

Type : String

Valeurs valides : `QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR`

TaskExecutionArn

L'ARN de l'exécution de la tâche sur laquelle vous vouliez obtenir des informations. `TaskExecutionArn`est hiérarchique et inclut `TaskArn` la tâche exécutée.

Par exemple, une `TaskExecution` valeur associée à l'ARN a `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2/execution/exec-08ef1e88ec491019b` exécuté la tâche à l'aide de l'ARN`arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2`.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

TaskMode

Le mode tâche que vous utilisez. Pour plus d'informations, consultez la section Choix d'un mode de tâche pour le transfert de données.

Type : String

Valeurs valides : `BASIC | ENHANCED`

TaskReportConfig

La configuration de votre rapport de tâches, qui fournit des informations détaillées sur votre DataSync transfert. Pour plus d'informations, consultez la section Création d'un rapport de tâches.

Type : objet TaskReportConfig

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande

Cet exemple illustre une `DescribeTaskExecution` demande.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/execution/exec-1234abcd1234abcd1"
}
```

Exemple de réponse 1 pour une exécution de tâche en mode amélioré

L'exemple suivant décrit une exécution de DataSync tâche qui utilise le mode amélioré. L'exécution consiste également à transférer des données spécifiques en utilisant des filtres d'exclusion et d'inclusion.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/execution/exec-1234abcd1234abcd1",
    "Status": "SUCCESS",
    "Options": {
        "VerifyMode": "ONLY_FILES_TRANSFERRED",
        "OverwriteMode": "ALWAYS",
        "Atime": "BEST_EFFORT",
        "Mtime": "PRESERVE",
        "Uid": "NONE",
        "Gid": "NONE",
        "PreserveDeletedFiles": "PRESERVE",
        "PreserveDevices": "NONE",
        "PosixPermissions": "NONE",
        "BytesPerSecond": -1,
        "TaskQueueing": "ENABLED",
        "LogLevel": "BASIC",
        "TransferMode": "CHANGED",
        "SecurityDescriptorCopyFlags": "NONE",
```

```
        "ObjectTags": "PRESERVE"
    },
    "Excludes": [{
        "FilterType": "SIMPLE_PATTERN",
        "Value": "/archive-files"
    }],
    "Includes": [{
        "FilterType": "SIMPLE_PATTERN",
        "Value": "/files"
    }],
    "StartTime": "2024-10-16T11:19:56.844000-04:00",
    "EstimatedFilesToTransfer": 7,
    "EstimatedBytesToTransfer": 30,
    "FilesTransferred": 7,
    "BytesWritten": 30,
    "BytesTransferred": 30,
    "BytesCompressed": 30,
    "Result": {
        "PrepareDuration": 0,
        "PrepareStatus": "SUCCESS",
        "TotalDuration": 3310,
        "TransferDuration": 0,
        "TransferStatus": "SUCCESS",
        "VerifyDuration": 0,
        "VerifyStatus": "SUCCESS"
    },
    "FilesDeleted": 0,
    "FilesSkipped": 0,
    "FilesVerified": 7,
    "EstimatedFilesToDelete": 0,
    "TaskMode": "ENHANCED",
    "FilesPrepared": 7,
    "FilesListed": {
        "AtSource": 7,
        "AtDestinationForDelete": 0
    },
    "FilesFailed": {
        "Prepare": 0,
        "Transfer": 0,
        "Verify": 0,
        "Delete": 0
    }
}
```

Exemple de réponse 2 pour une exécution de tâche en mode amélioré

L'exemple suivant décrit une autre exécution de DataSync tâche qui utilise le mode amélioré. Dans ce cas, l'exécution transfère des données spécifiques en utilisant un manifeste au lieu de filtres.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/execution/exec-1234abcd1234abcd1",
    "Status": "SUCCESS",
    "Options": {
        "VerifyMode": "ONLY_FILES_TRANSFERRED",
        "OverwriteMode": "ALWAYS",
        "Atime": "BEST_EFFORT",
        "Mtime": "PRESERVE",
        "Uid": "NONE",
        "Gid": "NONE",
        "PreserveDeletedFiles": "PRESERVE",
        "PreserveDevices": "NONE",
        "PosixPermissions": "NONE",
        "BytesPerSecond": -1,
        "TaskQueueing": "ENABLED",
        "LogLevel": "TRANSFER",
        "TransferMode": "CHANGED",
        "SecurityDescriptorCopyFlags": "NONE",
        "ObjectTags": "PRESERVE"
    },
    "Excludes": [],
    "Includes": [],
    "ManifestConfig": {
        "Action": "TRANSFER",
        "Format": "CSV",
        "S3AccessRoleArn": "arn:aws:iam::111222333444:role/service-role/
DataSyncS3ManifestAccess",
        "S3Bucket": "arn:aws:s3:::manifests-datasync",
        "VersionId": "Ixs7NQzEOj8BkL9r4ywX2FtDh_cPf3mG",
        "Source": {
            "S3": {
                "ManifestObjectPath": "manifest-folder/manifest-versioned-files",
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-manifest-
role/DataSyncS3ManifestAccess",
                "S3BucketArn": "arn:aws:s3:::manifests-datasync",
                "ManifestObjectVersionId": "Ixs7NQzEOj8BkL9r4ywX2FtDh_cPf3mG"
            }
        }
```

```
    },
    "StartTime": "2024-10-16T09:29:56.757000-04:00",
    "EstimatedFilesToTransfer": 1,
    "EstimatedBytesToTransfer": 6,
    "FilesTransferred": 1,
    "BytesWritten": 6,
    "BytesTransferred": 6,
    "BytesCompressed": 6,
    "Result": {
        "PrepareDuration": 0,
        "PrepareStatus": "SUCCESS",
        "TotalDuration": 3089,
        "TransferDuration": 0,
        "TransferStatus": "SUCCESS",
        "VerifyDuration": 0,
        "VerifyStatus": "SUCCESS"
    },
    "TaskReportConfig": {
        "Destination": {
            "S3": {
                "Subdirectory": "reports/",
                "S3BucketArn": "arn:aws:s3:::my-task-report",
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-task-report-
role/DataSyncTaskReportS3BucketAccess"
            }
        },
        "OutputType": "STANDARD",
        "ReportLevel": "SUCCESSES_AND_ERRORS",
        "ObjectVersionIds": "INCLUDE"
    },
    "FilesDeleted": 0,
    "FilesSkipped": 0,
    "FilesVerified": 1,
    "ReportResult": {
        "Status": "SUCCESS"
    },
    "EstimatedFilesToDelete": 0,
    "TaskMode": "ENHANCED",
    "FilesPrepared": 1,
    "FilesListed": {
        "AtSource": 1,
        "AtDestinationForDelete": 0
    },
    "FilesFailed": {
```

```
        "Prepare": 0,
        "Transfer": 0,
        "Verify": 0,
        "Delete": 0
    }
}
```

Exemple de réponse pour l'exécution d'une tâche en mode Basic

L'exemple suivant décrit une exécution de DataSync tâche qui utilise le mode de base.

```
{
    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/execution/exec-1234abcd1234abcd1",
    "BytesCompressed": 3500,
    "BytesTransferred": 5000,
    "BytesWritten": 5000,
    "EstimatedBytesToTransfer": 5000,
    "EstimatedFilesToDelete": 10,
    "EstimatedFilesToTransfer": 100,
    "FilesDeleted": 10,
    "FilesSkipped": 0,
    "FilesTransferred": 100,
    "FilesVerified": 100,
    "Result": {
        "PrepareDuration": 100,
        "PrepareStatus": "SUCCESS",
        "TransferDuration": 60,
        "TransferStatus": "SUCCESS",
        "VerifyDuration": 30,
        "VerifyStatus": "SUCCESS"
    },
    "StartTime": "2024-10-16T11:19:56.844000-04:00",
    "Status": "SUCCESS",
    "OverrideOptions": {
        "Atime": "BEST_EFFORT",
        "BytesPerSecond": "1000",
        "Gid": "NONE",
        "Mtime": "PRESERVE",
        "PosixPermissions": "PRESERVE",
        "PreserveDeletedFiles": "PRESERVE",
        "Uid": "NONE",
        "VerifyMode": "POINT_IN_TIME_CONSISTENT"
    },
```

```
    "TaskReportConfig": {
        "Destination": {
            "S3": {
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-datasync-
role",
                "S3BucketArn": "arn:aws:s3:::my-task-reports-bucket/*",
                "Subdirectory": "reports"
            }
        },
        "ObjectVersionIds": "INCLUDE",
        "OutputType": "STANDARD",
        "Overrides": {
            "Deleted": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Skipped": {
                "ReportLevel": "SUCCESSES_AND_ERRORS"
            },
            "Transferred": {
                "ReportLevel": "ERRORS_ONLY"
            },
            "Verified": {
                "ReportLevel": "ERRORS_ONLY"
            }
        },
        "ReportLevel": "ERRORS_ONLY"
    }
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListAgents

Renvoie une liste d' AWS DataSync agents appartenant à un Compte AWS in Région AWS spécifié dans la demande.

La pagination vous permet de réduire le nombre d'agents renvoyés dans une réponse. Si vous obtenez une liste tronquée d'agents dans une réponse, celle-ci contient un marqueur que vous pouvez spécifier dans votre prochaine demande pour récupérer la page d'agents suivante.

`ListAgentsest` finalement cohérent. Cela signifie que le résultat de l'exécution de l'opération peut ne pas refléter le fait que vous venez de créer ou de supprimer un agent. Par exemple, si vous créez un agent avec CreateAgentpuis que vous l'exécutez immédiatement`ListAgents`, cet agent risque de ne pas apparaître immédiatement dans la liste. Dans de telles situations, vous pouvez toujours vérifier si un agent a été créé (ou supprimé) en utilisant DescribeAgent.

Syntaxe de la requête

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

MaxResults

Spécifie le nombre maximum d' DataSync agents à répertorier dans une réponse. Par défaut, une réponse indique un maximum de 100 agents.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 100.

Obligatoire : non

NextToken

Spécifie une chaîne opaque qui indique le point de départ de la liste de résultats suivante dans la réponse.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Obligatoire : non

Syntaxe de la réponse

```
{
   "Agents": [
      {
         "AgentArn": "string",
         "Name": "string",
         "Platform": {
            "Version": "string"
         },
         "Status": "string"
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Agents

Une liste des DataSync agents figurant Compte AWS dans votre dossier, telle que Région AWS spécifiée dans la demande. La liste est triée selon les Amazon Resource Names (ARNs) des agents.

Type : tableau d'objets AgentListEntry

NextToken

Chaîne opaque qui indique le point de départ de la liste de résultats suivante dans la réponse.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListLocations

Renvoie une liste des emplacements source et de destination.

Si vous avez plus d'emplacements que ce qui est renvoyé dans une réponse (c'est-à-dire que la réponse ne renvoie qu'une liste tronquée de vos agents), la réponse contient un jeton que vous pouvez spécifier dans votre prochaine demande pour récupérer la page d'emplacements suivante.

Syntaxe de la requête

```
{
   "Filters": [
      {
         "Name": "string",
         "Operator": "string",
         "Values": [ "string" ]
      }
   ],
   "MaxResults": number,
   "NextToken": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Filters

Vous pouvez utiliser des filtres d'API pour affiner la liste des ressources renvoyées par`ListLocations`. Par exemple, pour récupérer toutes les tâches sur un emplacement source spécifique, vous pouvez utiliser `ListLocations` avec le nom du filtre `LocationType S3` et`Operator Equals`.

Type : tableau d'objets LocationFilter

Obligatoire : non

MaxResults

Le nombre maximum de sites à retourner.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 100.

Obligatoire : non

NextToken

Chaîne opaque qui indique la position à partir de laquelle commencer la prochaine liste d'emplacements.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Obligatoire : non

Syntaxe de la réponse

```
{
   "Locations": [
      {
         "LocationArn": "string",
         "LocationUri": "string"
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Locations

Tableau contenant une liste d'emplacements.

Type : tableau d'objets LocationListEntry

NextToken

Chaîne opaque qui indique la position à partir de laquelle commencer à renvoyer la liste d'emplacements suivante.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListTagsForResource

Renvoie toutes les balises associées à une AWS ressource.

Syntaxe de la requête

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ResourceArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

MaxResults

Spécifie le nombre de résultats que vous souhaitez voir apparaître dans la réponse.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 100.

Obligatoire : non

NextToken

Spécifie une chaîne opaque qui indique la position à partir de laquelle commencer la liste de résultats suivante dans la réponse.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Obligatoire : non

ResourceArn

Spécifie le nom de ressource Amazon (ARN) de la ressource pour laquelle vous souhaitez obtenir des informations de balise.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(agent|task|location|system)/((agent|task|loc)-[a-f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})(/execution/exec-[a-f0-9]{17})?$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

Chaîne opaque qui indique le point de départ de la liste de résultats suivante dans la réponse.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Tags

Un tableau de balises appliquées à la ressource spécifiée.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 55 articles.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListTaskExecutions

Renvoie la liste des exécutions pour une tâche AWS DataSync de transfert.

Syntaxe de la requête

```
{
   "MaxResults": number,
   "NextToken": "string",
   "TaskArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

MaxResults

Spécifie le nombre de résultats que vous souhaitez voir apparaître dans la réponse.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 100.

Obligatoire : non

NextToken

Spécifie une chaîne opaque qui indique la position à laquelle commencer la liste de résultats suivante dans la réponse.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Obligatoire : non

TaskArn

Spécifie le nom de ressource Amazon (ARN) de la tâche pour laquelle vous souhaitez obtenir des informations d'exécution.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "NextToken": "string",
   "TaskExecutions": [
      {
         "Status": "string",
         "TaskExecutionArn": "string",
         "TaskMode": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

Chaîne opaque qui indique le point de départ de la liste de résultats suivante dans la réponse.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

TaskExecutions

Liste des exécutions de la tâche.

Type : tableau d'objets TaskExecutionListEntry

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListTasks

Renvoie la liste des AWS DataSync tâches que vous avez créées.

Syntaxe de la requête

```
{
   "Filters": [
      {
         "Name": "string",
         "Operator": "string",
         "Values": [ "string" ]
      }
   ],
   "MaxResults": number,
   "NextToken": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Filters

Vous pouvez utiliser des filtres d'API pour affiner la liste des ressources renvoyées par`ListTasks`. Par exemple, pour récupérer toutes les tâches d'un emplacement source spécifique, vous pouvez les utiliser `ListTasks` avec le nom du filtre `LocationId` et `Operator` `Equals` avec l'ARN de l'emplacement.

Type : tableau d'objets TaskFilter

Obligatoire : non

MaxResults

Le nombre maximum de tâches à renvoyer.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 100.

Obligatoire : non

NextToken

Chaîne opaque qui indique la position à partir de laquelle commencer la liste de tâches suivante.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Obligatoire : non

Syntaxe de la réponse

```
{
   "NextToken": "string",
   "Tasks": [
      {
         "Name": "string",
         "Status": "string",
         "TaskArn": "string",
         "TaskMode": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

Chaîne opaque qui indique la position à partir de laquelle commencer à renvoyer la liste de tâches suivante.

Type : String

Contraintes de longueur : longueur maximale de 65535.

Modèle : `[a-zA-Z0-9=_-]+`

Tasks

Liste de toutes les tâches renvoyées.

Type : tableau d'objets TaskListEntry

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

StartTaskExecution

Démarre une tâche AWS DataSync de transfert. Pour chaque tâche, vous ne pouvez exécuter qu'une seule tâche à la fois.

L'exécution d'une tâche comporte plusieurs étapes. Pour plus d'informations, consultez la section Statuts d'exécution des tâches.

> **Important**
>
> Si vous prévoyez de transférer des données depuis ou vers un site Amazon S3, examinez comment cela DataSync peut affecter les frais de votre demande S3 et la page de DataSync tarification avant de commencer.

Syntaxe de la requête

```
{
   "Excludes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "Includes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "ManifestConfig": {
      "Action": "string",
      "Format": "string",
      "Source": {
         "S3": {
            "BucketAccessRoleArn": "string",
            "ManifestObjectPath": "string",
            "ManifestObjectVersionId": "string",
            "S3BucketArn": "string"
         }
      }
   },
```

```
    "OverrideOptions": {
       "Atime": "string",
       "BytesPerSecond": number,
       "Gid": "string",
       "LogLevel": "string",
       "Mtime": "string",
       "ObjectTags": "string",
       "OverwriteMode": "string",
       "PosixPermissions": "string",
       "PreserveDeletedFiles": "string",
       "PreserveDevices": "string",
       "SecurityDescriptorCopyFlags": "string",
       "TaskQueueing": "string",
       "TransferMode": "string",
       "Uid": "string",
       "VerifyMode": "string"
    },
    "Tags": [
       {
          "Key": "string",
          "Value": "string"
       }
    ],
    "TaskArn": "string",
    "TaskReportConfig": {
       "Destination": {
          "S3": {
             "BucketAccessRoleArn": "string",
             "S3BucketArn": "string",
             "Subdirectory": "string"
          }
       },
       "ObjectVersionIds": "string",
       "OutputType": "string",
       "Overrides": {
          "Deleted": {
             "ReportLevel": "string"
          },
          "Skipped": {
             "ReportLevel": "string"
          },
          "Transferred": {
             "ReportLevel": "string"
          },
```

```
            "Verified": {
                "ReportLevel": "string"
            }
        },
        "ReportLevel": "string"
    }
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Excludes

Spécifie une liste de règles de filtrage qui détermine les fichiers à exclure d'une tâche. La liste contient une chaîne de filtre unique qui contient les modèles à exclure. Les motifs sont délimités par « | » (c'est-à-dire une barre verticale), par exemple, `"/folder1|/folder2"`.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Obligatoire : non

Includes

Spécifie une liste de règles de filtrage qui détermine les fichiers à inclure lors de l'exécution d'une tâche. Le modèle doit contenir une seule chaîne de filtre composée des modèles à inclure. Les motifs sont délimités par « | » (c'est-à-dire une barre verticale), par exemple, `"/folder1|/folder2"`.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Obligatoire : non

ManifestConfig

Configure un manifeste, qui est une liste de fichiers ou d'objets que vous souhaitez DataSync transférer. Pour plus d'informations et des exemples de configuration, voir Spécifier les DataSync transferts à l'aide d'un manifeste.

Lorsque vous utilisez ce paramètre, l'identité de votre appelant (le rôle DataSync avec lequel vous utilisez) doit être `iam:PassRole` autorisée. La AWSDataSyncFullAccesspolitique inclut cette autorisation.

Pour supprimer une configuration de manifeste, spécifiez ce paramètre avec une valeur vide.

Type : objet ManifestConfig

Obligatoire : non

OverrideOptions

Indique comment votre tâche de transfert est configurée. Ces options incluent le mode DataSync de gestion des fichiers, des objets et des métadonnées associées lors de votre transfert. Vous pouvez également spécifier comment vérifier l'intégrité des données, définir des limites de bande passante pour votre tâche, entre autres options.

Chaque option possède une valeur par défaut. À moins que vous n'en ayez besoin, vous n'avez pas à configurer d'option avant d'appeler StartTaskExecution.

Vous pouvez également remplacer vos options de tâche pour chaque exécution de tâche. Par exemple, vous souhaiterez peut-être ajuster le `LogLevel` pour une exécution individuelle.

Type : objet Options

Obligatoire : non

Tags

Spécifie les balises que vous souhaitez appliquer à l'Amazon Resource Name (ARN) représentant l'exécution de la tâche.

Les balises sont des paires clé-valeur qui vous permettent de gérer, de filtrer et de rechercher vos DataSync ressources.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

TaskArn

Spécifie le nom de ressource Amazon (ARN) de la tâche que vous souhaitez démarrer.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Obligatoire : oui

TaskReportConfig

Spécifie la manière dont vous souhaitez configurer un rapport de tâches, qui fournit des informations détaillées sur votre DataSync transfert. Pour plus d'informations, consultez la section Surveillance de vos DataSync transferts à l'aide de rapports de tâches.

Lorsque vous utilisez ce paramètre, l'identité de votre appelant (le rôle DataSync avec lequel vous utilisez) doit être `iam:PassRole` autorisée. La AWSDataSyncFullAccesspolitique inclut cette autorisation.

Pour supprimer une configuration de rapport de tâches, spécifiez ce paramètre comme étant vide.

Type : objet TaskReportConfig

Obligatoire : non

Syntaxe de la réponse

```
{
   "TaskExecutionArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

TaskExecutionArn

L'ARN de l'exécution de la tâche en cours.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

Exemples

Exemple de demande

L'exemple suivant démarre l'exécution d'une tâche en utilisant les options par défaut pour la tâche spécifiée.

```
{
    "OverrideOptions": {
        "Atime": "BEST_EFFORT",
        "BytesPerSecond": 1000,
        "Gid": "NONE",
        "Mtime": "PRESERVE",
        "PosixPermissions": "PRESERVE",
        "PreserveDevices": "NONE",
        "PreserveDeletedFiles": "PRESERVE",
        "Uid": "NONE",
        "VerifyMode": "POINT_IN_TIME_CONSISTENT"
    },
    "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
```

```
}
```

Exemple de réponse

Cet exemple illustre une utilisation de StartTaskExecution.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"
}
```

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

TagResource

Applique une balise à une AWS ressource. Les balises sont des paires clé-valeur qui peuvent vous aider à gérer, filtrer et rechercher vos ressources.

Il s'agit notamment AWS DataSync des ressources, telles que les emplacements, les tâches et les exécutions de tâches.

Syntaxe de la requête

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

ResourceArn

Spécifie le nom de ressource Amazon (ARN) de la ressource à laquelle appliquer la balise.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(agent|task|location|system)/((agent|task|loc)-[a-f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})(/execution/exec-[a-f0-9]{17})?$`

Obligatoire : oui

Tags

Spécifie les balises que vous souhaitez appliquer à la ressource.

Type : tableau d'objets TagListEntry

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2

- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UntagResource

Supprime les balises d'une AWS ressource.

Syntaxe de la requête

```
{
   "Keys": [ "string" ],
   "ResourceArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Keys

Spécifie les clés des balises que vous souhaitez supprimer.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:/-]+$`

Obligatoire : oui

ResourceArn

Spécifie le nom de ressource Amazon (ARN) de la ressource dont les balises doivent être supprimées.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:(agent|task|location|system)/((agent|task|loc)-[a-`

```
f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]
{4}-[a-f0-9]{12})(/execution/exec-[a-f0-9]{17})?$
```

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateAgent

Met à jour le nom d'un AWS DataSync agent.

Syntaxe de la requête

```
{
   "AgentArn": "string",
   "Name": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AgentArn

Nom de ressource Amazon (ARN) de l'agent à mettre à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : oui

Name

Le nom que vous souhaitez utiliser pour configurer l'agent.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationAzureBlob

Modifie les configurations suivantes de l'emplacement de transfert Microsoft Azure Blob Storage que vous utilisez. AWS DataSync

Pour plus d'informations, consultez Configuration des DataSync transferts avec Azure Blob Storage.

Syntaxe de la requête

```
{
   "AccessTier": "string",
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlobType": "string",
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "LocationArn": "string",
   "SasConfiguration": {
      "Token": "string"
   },
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AccessTier

Spécifie le niveau d'accès vers lequel vous souhaitez transférer vos objets ou fichiers. Cela s'applique uniquement lorsque l'emplacement est utilisé comme destination de transfert. Pour plus d'informations, consultez la section Niveaux d'accès.

Type : String

Valeurs valides : `HOT | COOL | ARCHIVE`

Obligatoire : non

AgentArns

(Facultatif) Spécifie le nom de ressource Amazon (ARN) de l' DataSync agent qui peut se connecter à votre conteneur Azure Blob Storage. Si vous configurez un transfert cross-cloud sans agent, il n'est pas nécessaire de spécifier une valeur pour ce paramètre.

Vous pouvez spécifier plusieurs agents. Pour plus d'informations, consultez la section Utilisation de plusieurs agents pour votre transfert.

> **Note**
>
> Il est impossible d'ajouter ou de supprimer des agents d'un emplacement de stockage après l'avoir initialement créé.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : non

AuthenticationType

Spécifie la méthode d'authentification DataSync utilisée pour accéder à votre Azure Blob Storage. DataSync peut accéder au stockage blob à l'aide d'une signature d'accès partagé (SAS).

Type : String

Valeurs valides : `SAS | NONE`

Obligatoire : non

BlobType

Spécifie le type de blob que vous souhaitez attribuer à vos objets ou fichiers lorsque vous les transférez dans Azure Blob Storage. Actuellement, DataSync ne prend en charge le transfert de données vers Azure Blob Storage que sous forme de blobs de blocs. Pour plus d'informations sur les types de blob, consultez la documentation Azure Blob Storage.

Type : String

Valeurs valides : `BLOCK`

Obligatoire : non

CmkSecretConfig

Spécifie les informations de configuration pour un secret DataSync géré, tel qu'un jeton d'authentification ou un ensemble d'informations d'identification DataSync utilisé pour accéder à un lieu de transfert spécifique, et un secret géré par le client AWS KMS key.

Type : objet CmkSecretConfig

Obligatoire : non

CustomSecretConfig

Spécifie les informations de configuration pour un secret géré par le client, tel qu'un jeton d'authentification ou un ensemble d'informations d'identification DataSync utilisé pour accéder à un lieu de transfert spécifique, et un secret géré par le client. AWS KMS key

Type : objet CustomSecretConfig

Obligatoire : non

LocationArn

Spécifie l'ARN de l'emplacement de transfert Azure Blob Storage que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

SasConfiguration

Spécifie la configuration SAS qui permet d'accéder DataSync à votre Azure Blob Storage.

Type : objet AzureBlobSasConfiguration

Obligatoire : non

Subdirectory

Spécifie les segments de chemin si vous souhaitez limiter votre transfert vers un répertoire virtuel de votre conteneur (par exemple,`/my/images`).

Type : String

Contraintes de longueur : longueur maximum de 1 024.

Modèle : `^[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}\p{C}]*$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationEfs

Modifie les paramètres de configuration suivants du lieu de transfert Amazon EFS que vous utilisez. AWS DataSync

Pour plus d'informations, consultez Configuration des DataSync transferts avec Amazon EFS.

Syntaxe de la requête

```
{
   "AccessPointArn": "string",
   "FileSystemAccessRoleArn": "string",
   "InTransitEncryption": "string",
   "LocationArn": "string",
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AccessPointArn

Spécifie le nom de ressource Amazon (ARN) du point d'accès DataSync utilisé pour monter votre système de fichiers Amazon EFS.

Pour plus d'informations, consultez Accès aux systèmes de fichiers Amazon EFS restreints.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `(^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$)|(^$)`

Obligatoire : non

FileSystemAccessRoleArn

Spécifie un rôle AWS Identity and Access Management (IAM) qui permet d'accéder DataSync à votre système de fichiers Amazon EFS.

Pour plus d'informations sur la création de ce rôle, consultez Création d'un rôle DataSync IAM pour accéder au système de fichiers Amazon EFS.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `(^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$)|(^$)`

Obligatoire : non

InTransitEncryption

Spécifie si vous DataSync souhaitez utiliser le chiffrement TLS (Transport Layer Security) 1.2 lors du transfert de données vers ou depuis votre système de fichiers Amazon EFS.

Si vous spécifiez un point d'accès en utilisant `AccessPointArn` ou un rôle IAM avec `FileSystemAccessRoleArn`, vous devez définir ce paramètre sur `TLS1_2`.

Type : String

Valeurs valides : `NONE | TLS1_2`

Obligatoire : non

LocationArn

Spécifie le nom de ressource Amazon (ARN) du lieu de transfert Amazon EFS que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Subdirectory

Spécifie un chemin de montage pour votre système de fichiers Amazon EFS. C'est là que les données sont DataSync lues ou écrites sur votre système de fichiers (selon qu'il s'agit d'un emplacement source ou de destination).

Par défaut, DataSync utilise le répertoire racine (ou le point d'accès si vous en fournissez un en utilisant`AccessPointArn`). Vous pouvez également inclure des sous-répertoires à l'aide de barres obliques (par exemple,). `/path/to/folder`

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationFsxLustre

Modifie les paramètres de configuration suivants du lieu de transfert Amazon FSx for Lustre que vous utilisez. AWS DataSync

Pour plus d'informations, voir Configuration des DataSync transferts avec FSx pour Lustre.

Syntaxe de la requête

```
{
   "LocationArn": "string",
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) du lieu de transfert FSx pour Lustre que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Subdirectory

Spécifie un chemin de montage pour votre système de fichiers FSx for Lustre. Le chemin peut inclure des sous-répertoires.

Lorsque l'emplacement est utilisé comme source, DataSync lit les données depuis le chemin de montage. Lorsque l'emplacement est utilisé comme destination, DataSync écrit des données sur

le chemin de montage. Si vous n'incluez pas ce paramètre, DataSync utilise le répertoire racine du système de fichiers (/).

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2

- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationFsxOntap

Modifie les paramètres de configuration suivants du lieu de transfert Amazon FSx for NetApp ONTAP que vous utilisez. AWS DataSync

Pour plus d'informations, consultez Configuration des DataSync transferts avec FSx pour ONTAP.

Syntaxe de la requête

```
{
   "LocationArn": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "Domain": "string",
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) du lieu FSx de transfert ONTAP que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Protocol

Spécifie le protocole de transfert de données DataSync utilisé pour accéder à votre système de FSx fichiers Amazon.

Type : objet FsxUpdateProtocol

Obligatoire : non

Subdirectory

Spécifie le chemin d'accès au partage de fichiers sur la machine virtuelle de stockage (SVM) vers laquelle vous souhaitez transférer des données ou à partir de laquelle vous souhaitez transférer des données.

Vous pouvez spécifier un chemin de jonction (également appelé point de montage), un chemin qtree (pour les partages de fichiers NFS) ou un nom de partage (pour les partages de fichiers SMB). Par exemple, votre chemin de montage peut être `/vol1`, `/vol1/tree1` ou `/share1`.

> **Note**
>
> Ne spécifiez pas de chemin de jonction dans le volume racine de la SVM. Pour plus d'informations, consultez la section Gestion FSx des machines virtuelles de stockage ONTAP dans le guide de l'utilisateur Amazon FSx pour NetApp ONTAP.

Type : String

Contraintes de longueur : longueur maximale de 255.

Modèle : `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationFsxOpenZfs

Modifie les paramètres de configuration suivants du lieu de transfert Amazon FSx pour OpenZFS que vous utilisez. AWS DataSync

Pour plus d'informations, consultez Configuration des DataSync transferts avec FSx pour OpenZFS.

> **Note**
>
> Les paramètres de demande associés à `SMB` ne sont pas pris en charge par l'`UpdateLocationFsxOpenZfs`opération.

Syntaxe de la requête

```
{
   "LocationArn": "string",
   "Protocol": {
      "NFS": {
         "MountOptions": {
            "Version": "string"
         }
      },
      "SMB": {
         "Domain": "string",
         "MountOptions": {
            "Version": "string"
         },
         "Password": "string",
         "User": "string"
      }
   },
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement de transfert FSx pour OpenZFS que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Protocol

Spécifie le protocole de transfert de données AWS DataSync utilisé pour accéder à votre système de FSx fichiers Amazon.

Type : objet FsxProtocol

Obligatoire : non

Subdirectory

Spécifie un sous-répertoire dans le chemin de l'emplacement qui doit commencer `/fsx` par. DataSync utilise ce sous-répertoire pour lire ou écrire des données (selon que le système de fichiers est un emplacement source ou de destination).

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationFsxWindows

Modifie les paramètres de configuration suivants de l'emplacement de transfert du serveur de fichiers Amazon FSx pour Windows que vous utilisez. AWS DataSync

Pour plus d'informations, voir Configuration des DataSync transferts avec FSx pour Windows File Server.

Syntaxe de la requête

```
{
   "Domain": "string",
   "LocationArn": "string",
   "Password": "string",
   "Subdirectory": "string",
   "User": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Domain

Spécifie le nom du domaine Windows auquel appartient votre système de fichiers FSx pour Windows File Server.

Si votre environnement comporte plusieurs domaines Active Directory, la configuration de ce paramètre garantit la DataSync connexion au bon système de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 253.

Modèle : `^([A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252})?$`

Obligatoire : non

LocationArn

Spécifie l'ARN de l'emplacement FSx de transfert du serveur de fichiers Windows que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

Password

Spécifie le mot de passe de l'utilisateur autorisé à monter et à accéder aux fichiers, dossiers et métadonnées de fichiers de votre système de fichiers FSx pour Windows File Server.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^.{0,104}$`

Obligatoire : non

Subdirectory

Spécifie le chemin de montage de votre système de fichiers à l'aide de barres obliques. DataSync utilise ce sous-répertoire pour lire ou écrire des données (selon que le système de fichiers est un emplacement source ou de destination).

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : non

User

Spécifie l'utilisateur autorisé à monter et à accéder aux fichiers, dossiers et métadonnées de fichiers dans votre système de fichiers FSx pour Windows File Server.

Pour plus d'informations sur le choix d'un utilisateur disposant du niveau d'accès approprié pour votre transfert, consultez les autorisations requises FSx pour les emplacements des serveurs de fichiers Windows.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++

- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationHdfs

Modifie les paramètres de configuration suivants de l'emplacement de transfert du système de fichiers distribué Hadoop (HDFS) que vous utilisez avec. AWS DataSync

Pour plus d'informations, consultez la section Configuration des DataSync transferts avec un cluster HDFS.

Syntaxe de la requête

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "BlockSize": number,
   "KerberosKeytab": blob,
   "KerberosKrb5Conf": blob,
   "KerberosPrincipal": "string",
   "KmsKeyProviderUri": "string",
   "LocationArn": "string",
   "NameNodes": [
      {
         "Hostname": "string",
         "Port": number
      }
   ],
   "QopConfiguration": {
      "DataTransferProtection": "string",
      "RpcProtection": "string"
   },
   "ReplicationFactor": number,
   "SimpleUser": "string",
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AgentArns

Les Amazon Resource Names (ARNs) des DataSync agents qui peuvent se connecter à votre cluster HDFS.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : non

AuthenticationType

Type d'authentification utilisé pour déterminer l'identité de l'utilisateur.

Type : String

Valeurs valides : `SIMPLE | KERBEROS`

Obligatoire : non

BlockSize

Taille des blocs de données à écrire dans le cluster HDFS.

Type : entier

Plage valide : valeur minimale de 1048576. Valeur maximale de 1073741824.

Obligatoire : non

KerberosKeytab

La table de clés Kerberos (keytab) qui contient les mappages entre le principal Kerberos défini et les clés chiffrées. Vous pouvez charger le keytab à partir d'un fichier en fournissant l'adresse du fichier.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 65536.

Obligatoire : non

KerberosKrb5Conf

Le fichier `krb5.conf` qui contient les informations de configuration Kerberos. Vous pouvez charger le `krb5.conf` fichier en fournissant son adresse. Si vous utilisez le AWS CLI, il exécute le codage base64 pour vous. Dans le cas contraire, fournissez le texte codé en base64.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 131072.

Obligatoire : non

KerberosPrincipal

Le principal Kerberos ayant accès aux fichiers et dossiers du cluster HDFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^.+$`

Obligatoire : non

KmsKeyProviderUri

L'URI du serveur de gestion de clés (KMS) du cluster HDFS.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Modèle : `^kms:\/\/http[s]?@(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9])(;(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9]))*:[0-9]{1,5}\/kms$`

Obligatoire : non

LocationArn

Le nom de ressource Amazon (ARN) de l'emplacement du cluster HDFS source.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

NameNodes

Celui NameNode qui gère l'espace de noms HDFS. Il NameNode effectue des opérations telles que l'ouverture, la fermeture et le changement de nom de fichiers et de répertoires. Le NameNode contient les informations permettant de mapper des blocs de données au DataNodes. Vous ne pouvez en utiliser qu'un seul NameNode.

Type : tableau d'objets HdfsNameNode

Membres du tableau : Nombre minimum de 1 élément.

Obligatoire : non

QopConfiguration

La configuration de la qualité de protection (QOP) spécifie les paramètres RPC (Remote Procedure Call) et de confidentialité du transfert de données configurés sur le cluster de système de fichiers distribué Hadoop (HDFS).

Type : objet QopConfiguration

Obligatoire : non

ReplicationFactor

Le nombre de DataNodes vers lesquels répliquer les données lors de l'écriture dans le cluster HDFS.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 512.

Obligatoire : non

SimpleUser

Le nom d'utilisateur servant à identifier le client sur le système d'exploitation hôte.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^[_.A-Za-z0-9][-_.A-Za-z0-9]*$`

Obligatoire : non

Subdirectory

Un sous-répertoire du cluster HDFS. Ce sous-répertoire est utilisé pour lire des données à partir du cluster HDFS ou y écrire des données.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationNfs

Modifie les paramètres de configuration suivants de l'emplacement de transfert NFS (Network File System) que vous utilisez. AWS DataSync

Pour plus d'informations, consultez la section Configuration des transferts avec un serveur de fichiers NFS.

Syntaxe de la requête

```
{
   "LocationArn": "string",
   "MountOptions": {
      "Version": "string"
   },
   "OnPremConfig": {
      "AgentArns": [ "string" ]
   },
   "ServerHostname": "string",
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) de l'emplacement de transfert NFS que vous souhaitez mettre à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

MountOptions

Spécifie comment DataSync accéder à un emplacement à l'aide du protocole NFS.

Type : objet NfsMountOptions

Obligatoire : non

OnPremConfig

Les AWS DataSync agents qui peuvent se connecter à votre serveur de fichiers NFS (Network File System).

Type : objet OnPremConfig

Obligatoire : non

ServerHostname

Spécifie le nom DNS ou l'adresse IP (IPv4 ou IPv6) du serveur de fichiers NFS auquel votre DataSync agent se connecte.

Type : String

Contraintes de longueur : longueur maximale de 255.

Modèle : `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Obligatoire : non

Subdirectory

Spécifie le chemin d'exportation sur le serveur de fichiers NFS que vous DataSync souhaitez monter.

Ce chemin (ou un sous-répertoire du chemin) est l'endroit où les données sont DataSync transférées depuis ou vers. Pour plus d'informations sur la configuration d'une exportation pour DataSync, consultez la section Accès aux serveurs de fichiers NFS.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]+$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationObjectStorage

Modifie les paramètres de configuration suivants de l'emplacement de transfert du stockage d'objets que vous utilisez. AWS DataSync

Pour plus d'informations, consultez la section Configuration des DataSync transferts avec un système de stockage d'objets.

Syntaxe de la requête

```
{
   "AccessKey": "string",
   "AgentArns": [ "string" ],
   "CmkSecretConfig": {
      "KmsKeyArn": "string",
      "SecretArn": "string"
   },
   "CustomSecretConfig": {
      "SecretAccessRoleArn": "string",
      "SecretArn": "string"
   },
   "LocationArn": "string",
   "SecretKey": "string",
   "ServerCertificate": blob,
   "ServerHostname": "string",
   "ServerPort": number,
   "ServerProtocol": "string",
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AccessKey

Spécifie la clé d'accès (par exemple, un nom d'utilisateur) si des informations d'identification sont requises pour s'authentifier auprès du serveur de stockage d'objets.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `^.*$`

Obligatoire : non

AgentArns

(Facultatif) Spécifie les Amazon Resource Names (ARNs) des DataSync agents qui peuvent se connecter à votre système de stockage d'objets. Si vous configurez un transfert cross-cloud sans agent, il n'est pas nécessaire de spécifier une valeur pour ce paramètre.

> **Note**
>
> Il est impossible d'ajouter ou de supprimer des agents d'un emplacement de stockage après l'avoir initialement créé.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : non

CmkSecretConfig

Spécifie les informations de configuration pour un secret DataSync géré, tel qu'un jeton d'authentification ou un ensemble d'informations d'identification DataSync utilisé pour accéder à un lieu de transfert spécifique, et un secret géré par le client AWS KMS key.

Type : objet CmkSecretConfig

Obligatoire : non

CustomSecretConfig

Spécifie les informations de configuration pour un secret géré par le client, tel qu'un jeton d'authentification ou un ensemble d'informations d'identification DataSync utilisé pour accéder à un lieu de transfert spécifique, et un secret géré par le client. AWS KMS key

Type : objet CustomSecretConfig

Obligatoire : non

LocationArn

Spécifie l'ARN de l'emplacement du système de stockage d'objets que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

SecretKey

Spécifie la clé secrète (par exemple, un mot de passe) si des informations d'identification sont requises pour s'authentifier auprès du serveur de stockage d'objets.

> **Note**
>
> Si vous fournissez un code secret en utilisant `CmkSecretConfig` ou`SecretKey`, si vous ne fournissez pas de détails de configuration secrets`CustomSecretConfig`, vous DataSync stockez le jeton en utilisant le secret du Gestionnaire de Secrets Manager de votre AWS compte.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `^.*$`

Obligatoire : non

ServerCertificate

Spécifie une chaîne de certificats DataSync pour l'authentification auprès de votre système de stockage d'objets si celui-ci utilise une autorité de certification (CA) privée ou auto-signée. Vous devez spécifier un seul `.pem` fichier avec une chaîne de certificats complète (par exemple,`file:///home/user/.ssh/object_storage_certificates.pem`).

La chaîne de certificats peut inclure :

- Le certificat du système de stockage d'objets
- Tous les certificats intermédiaires (s'il y en a)
- Le certificat racine de l'autorité de certification signataire

Vous pouvez concaténer vos certificats dans un `.pem` fichier (dont la taille peut atteindre 32 768 octets avant le codage base64). L'exemple de `cat` commande suivant crée un `object_storage_certificates.pem` fichier contenant trois certificats :

```
cat object_server_certificate.pem intermediate_certificate.pem
ca_root_certificate.pem > object_storage_certificates.pem
```

Pour utiliser ce paramètre, configurez `ServerProtocol` sur`HTTPS`.

La mise à jour de ce paramètre n'interfère pas avec les tâches en cours.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 32 768.

Obligatoire : non

ServerHostname

Spécifie le nom de domaine ou l'adresse IP (IPv4 ou IPv6) du serveur de stockage d'objets auquel votre DataSync agent se connecte.

Type : String

Contraintes de longueur : longueur maximale de 255.

Modèle : `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Obligatoire : non

ServerPort

Spécifie le port sur lequel votre serveur de stockage d'objets accepte le trafic réseau entrant (par exemple, le port 443).

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 65536.

Obligatoire : non

ServerProtocol

Spécifie le protocole utilisé par votre serveur de stockage d'objets pour communiquer.

Type : String

Valeurs valides : `HTTPS | HTTP`

Obligatoire : non

Subdirectory

Spécifie le préfixe d'objet pour votre serveur de stockage d'objets. S'il s'agit d'un emplacement source, copie DataSync uniquement les objets portant ce préfixe. S'il s'agit d'un emplacement de destination, DataSync écrit tous les objets avec ce préfixe.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationS3

Modifie les paramètres de configuration suivants du lieu de transfert Amazon S3 que vous utilisez. AWS DataSync

> **Important**
>
> Avant de commencer, assurez-vous de lire les rubriques suivantes :
>
> - Considérations relatives à la classe de stockage avec les sites Amazon S3
> - Évaluation des coûts des requêtes S3 lors de l'utilisation DataSync

Syntaxe de la requête

```
{
   "LocationArn": "string",
   "S3Config": {
      "BucketAccessRoleArn": "string"
   },
   "S3StorageClass": "string",
   "Subdirectory": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

LocationArn

Spécifie le nom de ressource Amazon (ARN) du lieu de transfert Amazon S3 que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

S3Config

Spécifie le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) DataSync utilisé pour accéder à votre compartiment S3.

Pour plus d'informations, consultez la section Fournir DataSync un accès aux compartiments S3.

Type : objet S3Config

Obligatoire : non

S3StorageClass

Spécifie la classe de stockage que vous souhaitez que vos objets utilisent lorsque Amazon S3 est une destination de transfert.

Pour les compartiments entrants Régions AWS, la classe de stockage par défaut est. `STANDARD` Pour les buckets activés AWS Outposts, la classe de stockage par défaut est. `OUTPOSTS`

Pour plus d'informations, consultez la section Considérations relatives aux classes de stockage associées aux transferts Amazon S3.

Type : String

Valeurs valides : `STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL`

Obligatoire : non

Subdirectory

Spécifie un préfixe dans le compartiment S3 qui DataSync lit ou écrit vers (selon que le compartiment est un emplacement source ou de destination).

> **Note**
>
> DataSync Impossible de transférer des objets dont le préfixe commence par une barre oblique (/) ou inclut `///./`, ou `/../` des motifs. Par exemple :
>
> - `/photos`
> - `photos//2006/January`
> - `photos/./2006/February`

```
    • photos/../2006/March
```

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++

- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateLocationSmb

Modifie les paramètres de configuration suivants de l'emplacement de transfert SMB (Server Message Block) que vous utilisez. AWS DataSync

Pour plus d'informations, consultez la section Configuration des DataSync transferts avec un serveur de fichiers SMB.

Syntaxe de la requête

```
{
   "AgentArns": [ "string" ],
   "AuthenticationType": "string",
   "DnsIpAddresses": [ "string" ],
   "Domain": "string",
   "KerberosKeytab": blob,
   "KerberosKrb5Conf": blob,
   "KerberosPrincipal": "string",
   "LocationArn": "string",
   "MountOptions": {
      "Version": "string"
   },
   "Password": "string",
   "ServerHostname": "string",
   "Subdirectory": "string",
   "User": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

AgentArns

Spécifie l' DataSync agent (ou les agents) qui peuvent se connecter à votre serveur de fichiers SMB. Vous spécifiez un agent à l'aide de son Amazon Resource Name (ARN).

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : non

AuthenticationType

Spécifie le protocole d'authentification DataSync utilisé pour se connecter à votre serveur de fichiers SMB. DataSync supports `NTLM` (par défaut) et `KERBEROS` authentification.

Pour plus d'informations, consultez la section Fournir un DataSync accès aux serveurs de fichiers SMB.

Type : String

Valeurs valides : `NTLM | KERBEROS`

Obligatoire : non

DnsIpAddresses

Spécifie les adresses IP (IPv4 ou IPv6) des serveurs DNS auxquels appartient votre serveur de fichiers SMB. Ce paramètre ne s'applique que s'`AuthenticationType`il est défini sur`KERBEROS`.

Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion au bon serveur de fichiers SMB.

Type : tableau de chaînes

Membres du tableau : nombre maximum de 2 éléments.

Contraintes de longueur : longueur minimale de 7. Longueur maximale de 39

Modèle : `\A((25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d)){3}|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-`

`F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6}))\z`

Obligatoire : non

Domain

Spécifie le nom de domaine Windows auquel appartient votre serveur de fichiers SMB. Ce paramètre ne s'applique que s'`AuthenticationType`il est défini sur`NTLM`.

Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion au bon serveur de fichiers.

Type : String

Contraintes de longueur : longueur maximale de 253.

Modèle : `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

Obligatoire : non

KerberosKeytab

Spécifie votre fichier de table de clés Kerberos (keytab), qui inclut les mappages entre votre clé principale Kerberos et vos clés de chiffrement.

Pour éviter les erreurs d'exécution des tâches, assurez-vous que le principal Kerberos que vous utilisez pour créer le fichier keytab correspond exactement à ce que vous spécifiez. `KerberosPrincipal`

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 65536.

Obligatoire : non

KerberosKrb5Conf

Spécifie un fichier de configuration Kerberos (`krb5.conf`) qui définit la configuration de votre domaine Kerberos.

Le fichier doit être codé en base64. Si vous utilisez le AWS CLI, le codage est fait pour vous.

Type : objet de données binaires encodées en base64

Contraintes de longueur : longueur maximale de 131072.

Obligatoire : non

KerberosPrincipal

Spécifie un principal Kerberos, c'est-à-dire une identité dans votre domaine Kerberos autorisée à accéder aux fichiers, aux dossiers et aux métadonnées des fichiers sur votre serveur de fichiers SMB.

Cela pourrait ressembler à un Kerberos principal. `HOST/kerberosuser@MYDOMAIN.ORG`

Les noms principaux distinguent les majuscules et minuscules. L'exécution de votre DataSync tâche échouera si le principal que vous spécifiez pour ce paramètre ne correspond pas exactement au principal que vous avez utilisé pour créer le fichier keytab.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^.+$`

Obligatoire : non

LocationArn

Spécifie l'ARN de l'emplacement SMB que vous souhaitez mettre à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : oui

MountOptions

Spécifie la version du protocole SMB (Server Message Block) qui permet d'accéder AWS DataSync à un serveur de fichiers SMB.

Type : objet SmbMountOptions

Obligatoire : non

Password

Spécifie le mot de passe de l'utilisateur qui peut monter votre serveur de fichiers SMB et qui est autorisé à accéder aux fichiers et dossiers concernés par votre transfert. Ce paramètre ne s'applique que s'`AuthenticationType`il est défini sur`NTLM`.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^.{0,104}$`

Obligatoire : non

ServerHostname

Spécifie le nom de domaine ou l'adresse IP (IPv4 ou IPv6) du serveur de fichiers SMB auquel votre DataSync agent se connecte.

> **Note**
>
> Si vous utilisez l'authentification Kerberos, vous devez spécifier un nom de domaine.

Type : String

Contraintes de longueur : longueur maximale de 255.

Modèle : `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-:]*[A-Za-z0-9])$`

Obligatoire : non

Subdirectory

Spécifie le nom du partage exporté par votre serveur de fichiers SMB où les données DataSync seront lues ou écrites. Vous pouvez inclure un sous-répertoire dans le chemin de partage (par exemple,`/path/to/subdirectory`). Assurez-vous que les autres clients SMB de votre réseau peuvent également monter ce chemin.

Pour copier toutes les données du sous-répertoire spécifié, vous DataSync devez être en mesure de monter le partage SMB et d'accéder à toutes ses données. Pour plus d'informations, consultez la section Fournir un DataSync accès aux serveurs de fichiers SMB.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\$\p{Zs}]+$`

Obligatoire : non

User

Spécifie le nom d'utilisateur qui peut monter votre serveur de fichiers SMB et qui est autorisé à accéder aux fichiers et dossiers concernés par votre transfert. Ce paramètre ne s'applique que s'`AuthenticationType`il est défini sur`NTLM`.

Pour plus d'informations sur le choix d'un utilisateur disposant du niveau d'accès approprié pour votre transfert, consultez la section Fournir un DataSync accès aux serveurs de fichiers SMB.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateTask

Met à jour la configuration d'une tâche, qui définit où et comment AWS DataSync vos données sont transférées.

Syntaxe de la requête

```
{
   "CloudWatchLogGroupArn": "string",
   "Excludes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "Includes": [
      {
         "FilterType": "string",
         "Value": "string"
      }
   ],
   "ManifestConfig": {
      "Action": "string",
      "Format": "string",
      "Source": {
         "S3": {
            "BucketAccessRoleArn": "string",
            "ManifestObjectPath": "string",
            "ManifestObjectVersionId": "string",
            "S3BucketArn": "string"
         }
      }
   },
   "Name": "string",
   "Options": {
      "Atime": "string",
      "BytesPerSecond": number,
      "Gid": "string",
      "LogLevel": "string",
      "Mtime": "string",
      "ObjectTags": "string",
      "OverwriteMode": "string",
      "PosixPermissions": "string",
```

```
        "PreserveDeletedFiles": "string",
        "PreserveDevices": "string",
        "SecurityDescriptorCopyFlags": "string",
        "TaskQueueing": "string",
        "TransferMode": "string",
        "Uid": "string",
        "VerifyMode": "string"
    },
    "Schedule": {
        "ScheduleExpression": "string",
        "Status": "string"
    },
    "TaskArn": "string",
    "TaskReportConfig": {
        "Destination": {
            "S3": {
                "BucketAccessRoleArn": "string",
                "S3BucketArn": "string",
                "Subdirectory": "string"
            }
        },
        "ObjectVersionIds": "string",
        "OutputType": "string",
        "Overrides": {
            "Deleted": {
                "ReportLevel": "string"
            },
            "Skipped": {
                "ReportLevel": "string"
            },
            "Transferred": {
                "ReportLevel": "string"
            },
            "Verified": {
                "ReportLevel": "string"
            }
        },
        "ReportLevel": "string"
    }
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

CloudWatchLogGroupArn

Spécifie le nom de ressource Amazon (ARN) d'un groupe de CloudWatch journaux Amazon pour surveiller votre tâche.

Pour les tâches en mode amélioré, vous devez utiliser `/aws/datasync` comme nom de groupe de journaux. Par exemple :

```
arn:aws:logs:us-east-1:111222333444:log-group:/aws/datasync:*
```

Pour plus d'informations, consultez la section Surveillance des transferts de données à l'aide CloudWatch des journaux.

Type : String

Contraintes de longueur : longueur maximale de 562.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-0-9]+:[0-9]{12}:log-group:([^:\*]*)(:\*)?$`

Obligatoire : non

Excludes

Spécifie les filtres d'exclusion qui définissent les fichiers, les objets et les dossiers de votre emplacement source que vous ne DataSync souhaitez pas transférer. Pour plus d'informations et des exemples, voir Spécifier les DataSync transferts à l'aide de filtres.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Obligatoire : non

Includes

Spécifie que les filtres d'inclusion définissent les fichiers, les objets et les dossiers que vous souhaitez DataSync transférer dans votre emplacement source. Pour plus d'informations et des exemples, voir Spécifier les DataSync transferts à l'aide de filtres.

Type : tableau d'objets FilterRule

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Obligatoire : non

ManifestConfig

Configure un manifeste, qui est une liste de fichiers ou d'objets que vous souhaitez DataSync transférer. Pour plus d'informations et des exemples de configuration, voir Spécifier les DataSync transferts à l'aide d'un manifeste.

Lorsque vous utilisez ce paramètre, l'identité de votre appelant (le rôle IAM DataSync avec lequel vous utilisez) doit être autorisée. `iam:PassRole` La AWSDataSyncFullAccesspolitique inclut cette autorisation.

Pour supprimer une configuration de manifeste, spécifiez ce paramètre comme étant vide.

Type : objet ManifestConfig

Obligatoire : non

Name

Spécifie le nom de votre tâche.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatoire : non

Options

Indique comment votre tâche de transfert est configurée. Ces options incluent le mode DataSync de gestion des fichiers, des objets et des métadonnées associées lors de votre transfert. Vous

pouvez également spécifier comment vérifier l'intégrité des données, définir des limites de bande passante pour votre tâche, entre autres options.

Chaque option possède une valeur par défaut. À moins que vous n'en ayez besoin, vous n'avez pas besoin de configurer d'option avant d'appeler StartTaskExecution.

Vous pouvez également remplacer vos options de tâche pour chaque exécution de tâche. Par exemple, vous souhaiterez peut-être ajuster le `LogLevel` pour une exécution individuelle.

Type : objet Options

Obligatoire : non

Schedule

Spécifie le calendrier d'exécution de la tâche. Pour plus d'informations, veuillez consulter la rubrique Planification de votre tâche.

Type : objet TaskSchedule

Obligatoire : non

TaskArn

Spécifie l'ARN de la tâche que vous souhaitez mettre à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Obligatoire : oui

TaskReportConfig

Spécifie la manière dont vous souhaitez configurer un rapport de tâches, qui fournit des informations détaillées sur votre DataSync transfert. Pour plus d'informations, consultez la section Surveillance de vos DataSync transferts à l'aide de rapports de tâches.

Lorsque vous utilisez ce paramètre, l'identité de votre appelant (le rôle IAM DataSync avec lequel vous utilisez) doit être autorisée. `iam:PassRole` La AWSDataSyncFullAccesspolitique inclut cette autorisation.

Pour supprimer une configuration de rapport de tâches, spécifiez ce paramètre comme étant vide.

Type : objet TaskReportConfig

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateTaskExecution

Met à jour la configuration de l'exécution d'une AWS DataSync tâche en cours d'exécution.

> **Note**
>
> Actuellement, vous ne pouvez modifier `Option` que ce qui limite la bande passante pour l'exécution d'une tâche en cours ou en file d'attente. `UpdateTaskExecution` `BytesPerSecond`

Syntaxe de la requête

```
{
   "Options": {
      "Atime": "string",
      "BytesPerSecond": number,
      "Gid": "string",
      "LogLevel": "string",
      "Mtime": "string",
      "ObjectTags": "string",
      "OverwriteMode": "string",
      "PosixPermissions": "string",
      "PreserveDeletedFiles": "string",
      "PreserveDevices": "string",
      "SecurityDescriptorCopyFlags": "string",
      "TaskQueueing": "string",
      "TransferMode": "string",
      "Uid": "string",
      "VerifyMode": "string"
   },
   "TaskExecutionArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Options

Indique comment votre tâche de transfert est configurée. Ces options incluent le mode DataSync de gestion des fichiers, des objets et des métadonnées associées lors de votre transfert. Vous pouvez également spécifier comment vérifier l'intégrité des données, définir des limites de bande passante pour votre tâche, entre autres options.

Chaque option possède une valeur par défaut. À moins que vous n'en ayez besoin, vous n'avez pas besoin de configurer d'option avant d'appeler StartTaskExecution.

Vous pouvez également remplacer vos options de tâche pour chaque exécution de tâche. Par exemple, vous souhaiterez peut-être ajuster le `LogLevel` pour une exécution individuelle.

Type : objet Options

Obligatoire : oui

TaskExecutionArn

Spécifie le nom de ressource Amazon (ARN) de l'exécution de la tâche que vous mettez à jour.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalException

Cette exception est levée lorsqu'une erreur se produit dans le AWS DataSync service.

Code d'état HTTP : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour Kotlin
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

Types de données

Les types de données suivants sont pris en charge :

- AgentListEntry
- AzureBlobSasConfiguration
- CmkSecretConfig
- CustomSecretConfig
- Ec2Config
- FilterRule
- FsxProtocol

- FsxProtocolNfs
- FsxProtocolSmb
- FsxUpdateProtocol
- FsxUpdateProtocolSmb
- HdfsNameNode
- LocationFilter
- LocationListEntry
- ManagedSecretConfig
- ManifestConfig
- NfsMountOptions
- OnPremConfig
- Options
- Platform
- PrivateLinkConfig
- QopConfiguration
- ReportDestination
- ReportDestinationS3
- ReportOverride
- ReportOverrides
- ReportResult
- S3Config
- S3ManifestConfig
- SmbMountOptions
- SourceManifestConfig
- TagListEntry
- TaskExecutionFilesFailedDetail
- TaskExecutionFilesListedDetail
- TaskExecutionListEntry
- TaskExecutionResultDetail
- TaskFilter

- TaskListEntry
- TaskReportConfig
- TaskSchedule
- TaskScheduleDetails

AgentListEntry

Représente une seule entrée dans une liste (ou un tableau) d' AWS DataSync agents lorsque vous appelez l'ListAgentsopération.

Table des matières

AgentArn

Le nom de ressource Amazon (ARN) d'un DataSync agent.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : non

Name

Le nom d'un agent.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatoire : non

Platform

Les informations relatives à la plate-forme concernant l'agent, telles que le numéro de version.

Type : objet Platform

Obligatoire : non

Status

Le statut d'un agent.

- Si le statut est défini`ONLINE`, l'agent est correctement configuré et prêt à être utilisé.

- Si le statut est le cas`OFFLINE`, l'agent a été hors de contact avec DataSync lui pendant cinq minutes ou plus. Cela peut se produire pour plusieurs raisons. Pour plus d'informations, voir Que dois-je faire si mon agent est hors ligne ?

Type : String

Valeurs valides : `ONLINE | OFFLINE`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

AzureBlobSasConfiguration

Configuration de signature d'accès partagé (SAS) qui permet d'accéder AWS DataSync à votre Microsoft Azure Blob Storage.

Pour plus d'informations, consultez la section Jetons SAS pour accéder à votre stockage Azure Blob.

Table des matières

Token

Spécifie un jeton SAS qui fournit des autorisations pour accéder à votre stockage Azure Blob.

Le jeton fait partie de la chaîne d'URI SAS qui suit l'URI de la ressource de stockage et un point d'interrogation. Un jeton ressemble à ceci :

```
sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&s
%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Modèle : `^.+$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

CmkSecretConfig

Spécifie les informations de configuration pour un secret DataSync géré, tel qu'un jeton d'authentification ou une clé secrète qui permet d'accéder DataSync à un emplacement de stockage spécifique, avec un secret géré par le client AWS KMS key.

> **Note**
>
> Vous pouvez utiliser l'un ou l'autre `CmkSecretConfig` ou `CustomSecretConfig` fournir des informations d'identification pour une `CreateLocation` demande. Ne fournissez pas les deux paramètres pour la même demande.

Table des matières

KmsKeyArn

Spécifie l'ARN DataSync utilisé par le client AWS KMS key pour chiffrer le secret DataSync géré stocké pour. `SecretArn` DataSync fournit cette clé à AWS Secrets Manager.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):kms:[a-z\-0-9]+:[0-9]{12}:key/.*|)$`

Obligatoire : non

SecretArn

Spécifie l'ARN du AWS Secrets Manager secret DataSync géré utilisé pour accéder à un emplacement de stockage spécifique. Cette propriété est générée par DataSync et est en lecture seule. DataSync chiffre ce secret avec la clé KMS que vous spécifiez. `KmsKeyArn`

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

CustomSecretConfig

Spécifie les informations de configuration pour un secret Secrets Manager géré par le client dans lequel un jeton d'authentification ou une clé secrète de l'emplacement de stockage est stocké en texte brut. Cette configuration inclut l'ARN secret et l'ARN d'un rôle IAM qui donne accès au secret.

> **Note**
>
> Vous pouvez utiliser l'un ou l'autre `CmkSecretConfig` ou `CustomSecretConfig` fournir des informations d'identification pour une `CreateLocation` demande. Ne fournissez pas les deux paramètres pour la même demande.

Table des matières

SecretAccessRoleArn

Spécifie l'ARN du AWS Identity and Access Management rôle DataSync utilisé pour accéder au secret spécifié pour`SecretArn`.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/[a-zA-Z0-9+=,.@_-]+|)$`

Obligatoire : non

SecretArn

Spécifie l'ARN d'un AWS Secrets Manager secret.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Ec2Config

Sous-réseau et groupes de sécurité AWS DataSync utilisés pour se connecter à l'une des cibles de montage de votre système de fichiers Amazon EFS.

Table des matières

SecurityGroupArns

Spécifie les noms de ressources Amazon (ARNs) des groupes de sécurité associés à la cible de montage d'un système de fichiers Amazon EFS.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obligatoire : oui

SubnetArn

Spécifie l'ARN d'un sous-réseau où sont DataSync créées les interfaces réseau pour gérer le trafic pendant le transfert.

Le sous-réseau doit être situé :

- Dans le même cloud privé virtuel (VPC) que le système de fichiers Amazon EFS.
- Dans la même zone de disponibilité qu'au moins une cible de montage pour le système de fichiers Amazon EFS.

> **Note**
>
> Vous n'avez pas besoin de spécifier un sous-réseau incluant une cible de montage de système de fichiers.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/.*$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

FilterRule

Spécifie les fichiers, les dossiers et les objets à inclure ou à exclure lors du transfert de fichiers de la source vers la destination.

Table des matières

FilterType

Type de règle de filtre à appliquer. AWS DataSync ne prend en charge que le type de règle SIMPLE_PATTERN.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^[A-Z0-9_]+$`

Valeurs valides : `SIMPLE_PATTERN`

Obligatoire : non

Value

Une chaîne de filtre unique composée des modèles à inclure ou à exclure. Les modèles sont délimités par « | » (une barre verticale), par exemple : `/folder1|/folder2`

Type : String

Contraintes de longueur : longueur maximale de 102400.

Modèle : `^[^\x00]+$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++

- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

FsxProtocol

Spécifie le protocole de transfert de données AWS DataSync utilisé pour accéder à votre système de FSx fichiers Amazon.

Table des matières

NFS

Spécifie la configuration du protocole NFS (Network File System) à utiliser FSx pour accéder DataSync à votre système de fichiers OpenZFS ou FSx à la machine virtuelle de stockage (SVM) du système de fichiers ONTAP.

Type : objet FsxProtocolNfs

Obligatoire : non

SMB

Spécifie la configuration du protocole SMB (Server Message Block) à utiliser FSx pour DataSync accéder à votre SVM du système de fichiers ONTAP.

Type : objet FsxProtocolSmb

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

FsxProtocolNfs

Spécifie la configuration du protocole NFS (Network File System) à utiliser FSx pour accéder DataSync à votre système de fichiers OpenZFS ou FSx à la machine virtuelle de stockage (SVM) du système de fichiers ONTAP.

Table des matières

MountOptions

Spécifie comment DataSync accéder à un emplacement à l'aide du protocole NFS.

Type : objet NfsMountOptions

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

FsxProtocolSmb

Spécifie la configuration du protocole SMB (Server Message Block) qui permet d' AWS DataSync accéder à la machine virtuelle de stockage (SVM) de votre système de fichiers Amazon FSx for NetApp ONTAP. Pour plus d'informations, voir Fournir un DataSync accès aux systèmes FSx de fichiers ONTAP.

Table des matières

Password

Spécifie le mot de passe d'un utilisateur autorisé à accéder à votre SVM.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^.{0,104}$`

Obligatoire : oui

User

Spécifie un utilisateur qui peut monter et accéder aux fichiers, dossiers et métadonnées de votre SVM.

Pour plus d'informations sur le choix d'un utilisateur disposant du niveau d'accès approprié pour votre transfert, consultez la section Utilisation du protocole SMB.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Obligatoire : oui

Domain

Spécifie le nom du domaine Windows auquel appartient votre machine virtuelle de stockage (SVM).

Si votre environnement comporte plusieurs domaines, la configuration de ce paramètre garantit la DataSync connexion à la SVM appropriée.

Si votre environnement comporte plusieurs domaines Active Directory, la configuration de ce paramètre garantit la DataSync connexion à la SVM appropriée.

Type : String

Contraintes de longueur : longueur maximale de 253.

Modèle : `^[A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252}$`

Obligatoire : non

MountOptions

Spécifie la version du protocole SMB (Server Message Block) AWS DataSync utilisée pour accéder à un serveur de fichiers SMB.

Type : objet SmbMountOptions

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

FsxUpdateProtocol

Spécifie le protocole de transfert de données AWS DataSync utilisé pour accéder à votre système de FSx fichiers Amazon.

> **Note**
>
> Vous ne pouvez pas mettre à jour la configuration du protocole NFS (Network File System) FSx pour les emplacements ONTAP. DataSync ne prend actuellement en charge que la version 3 de NFS avec ce type d'emplacement.

Table des matières

NFS

Spécifie la configuration du protocole NFS (Network File System) à utiliser FSx pour accéder DataSync à votre système de fichiers OpenZFS ou FSx à la machine virtuelle de stockage (SVM) du système de fichiers ONTAP.

Type : objet FsxProtocolNfs

Obligatoire : non

SMB

Spécifie la configuration du protocole SMB (Server Message Block) à utiliser FSx pour DataSync accéder à la machine virtuelle de stockage (SVM) de votre système de fichiers ONTAP.

Type : objet FsxUpdateProtocolSmb

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2

- AWS SDK pour Ruby V3

FsxUpdateProtocolSmb

Spécifie la configuration du protocole SMB (Server Message Block) qui permet d' AWS DataSync accéder à la machine virtuelle de stockage (SVM) de votre système de fichiers Amazon FSx for NetApp ONTAP. Pour plus d'informations, consultez la section Fournir un DataSync accès FSx aux systèmes de fichiers ONTAP.

Table des matières

Domain

Spécifie le nom du domaine Windows auquel appartient votre machine virtuelle de stockage (SVM).

Si votre environnement comporte plusieurs domaines Active Directory, la configuration de ce paramètre garantit la DataSync connexion à la SVM appropriée.

Type : String

Contraintes de longueur : longueur maximale de 253.

Modèle : `^([A-Za-z0-9]((\.|-+)?[A-Za-z0-9]){0,252})?$`

Obligatoire : non

MountOptions

Spécifie la version du protocole SMB (Server Message Block) qui permet d'accéder AWS DataSync à un serveur de fichiers SMB.

Type : objet SmbMountOptions

Obligatoire : non

Password

Spécifie le mot de passe d'un utilisateur autorisé à accéder à votre SVM.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^.{0,104}$`

Obligatoire : non

User

Spécifie un utilisateur qui peut monter et accéder aux fichiers, dossiers et métadonnées de votre SVM.

Pour plus d'informations sur le choix d'un utilisateur disposant du niveau d'accès approprié pour votre transfert, consultez la section Utilisation du protocole SMB.

Type : String

Contraintes de longueur : longueur maximale de 104.

Modèle : `^[^\x22\x5B\x5D/\\:;|=,+*?\x3C\x3E]{1,104}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

HdfsNameNode

Le NameNode du système de fichiers distribué Hadoop (HDFS). NameNode Gère l'espace de noms du système de fichiers. Il NameNode effectue des opérations telles que l'ouverture, la fermeture et le changement de nom de fichiers et de répertoires. Le NameNode contient les informations permettant de mapper des blocs de données au DataNodes.

Table des matières

Hostname

Le nom d'hôte du NameNode dans le cluster HDFS. Cette valeur est l'adresse IP ou le nom DNS (Domain Name Service) du NameNode. Un agent installé sur site utilise ce nom d'hôte pour communiquer avec NameNode le réseau.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Modèle : `^(([a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-]*[A-Za-z0-9])$`

Obligatoire : oui

Port

Port NameNode utilisé pour écouter les demandes des clients.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 65536.

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

LocationFilter

Affinez la liste des ressources renvoyées par`ListLocations`. Par exemple, pour voir tous vos sites Amazon S3, créez un filtre à l'aide de `"Name": "LocationType""Operator": "Equals"`, et`"Values": "S3"`.

Pour plus d'informations, consultez la section Filtrage des ressources.

Table des matières

Name

Nom du filtre utilisé. Chaque appel d'API prend en charge une liste de filtres disponibles pour celui-ci (par exemple, `LocationType` pour`ListLocations`).

Type : String

Valeurs valides : `LocationUri | LocationType | CreationTime`

Obligatoire : oui

Operator

Opérateur utilisé pour comparer les valeurs des filtres (par exemple, `Equals` ou`Contains`).

Type : String

Valeurs valides : `Equals | NotEquals | In | LessThanOrEqual | LessThan | GreaterThanOrEqual | GreaterThan | Contains | NotContains | BeginsWith`

Obligatoire : oui

Values

Les valeurs que vous souhaitez filtrer. Par exemple, vous souhaiterez peut-être afficher uniquement les emplacements Amazon S3.

Type : tableau de chaînes

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Modèle : `^[0-9a-zA-Z_\ \-\:\*\.\\/\?-]*$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

LocationListEntry

Représente une entrée unique dans une liste d'emplacements. `LocationListEntry`renvoie un tableau contenant une liste d'emplacements lorsque l'ListLocationsopération est appelée.

Table des matières

LocationArn

Le nom de ressource Amazon (ARN) de l'emplacement. Pour le système de fichiers réseau (NFS) ou Amazon EFS, l'emplacement est le chemin d'exportation. Pour Amazon S3, l'emplacement est le chemin du préfixe que vous souhaitez monter et utiliser comme racine de l'emplacement.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obligatoire : non

LocationUri

Représente la liste URIs d'un emplacement. `LocationUri`renvoie un tableau contenant une liste d'emplacements lorsque l'ListLocationsopération est appelée.

Format :`TYPE://GLOBAL_ID/SUBDIR`.

TYPE désigne le type de lieu (par exemple, `nfs` ou`s3`).

GLOBAL_ID est l'identifiant unique au monde de la ressource qui soutient l'emplacement. Un exemple pour l'EFS est`us-east-2.fs-abcd1234`. Un exemple pour Amazon S3 est le nom du compartiment, tel que`myBucket`. Un exemple de NFS est une IPv6 adresse IPv4 ou un nom d'hôte valide conforme au DNS.

SUBDIR est un chemin de système de fichiers valide, délimité par des barres obliques, conformément à la convention *nix. Pour NFS et Amazon EFS, il s'agit du chemin d'exportation pour monter l'emplacement. Pour Amazon S3, il s'agit du chemin du préfixe vers lequel vous montez et que vous considérez comme la racine de l'emplacement.

Type : String

Contraintes de longueur : longueur maximale de 4360.

Modèle : `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ManagedSecretConfig

Spécifie les informations de configuration pour un secret DataSync géré, tel qu'un jeton d'authentification ou un ensemble d'informations d'identification permettant DataSync d'accéder à un emplacement de transfert spécifique. DataSync utilise la clé KMS AWS gérée par défaut pour chiffrer ce secret. AWS Secrets Manager

Table des matières

SecretArn

Spécifie l'ARN d'un AWS Secrets Manager secret.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-0-9]+:[0-9]{12}:secret:.*|)$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ManifestConfig

Configure un manifeste, qui est une liste de fichiers ou d'objets que vous souhaitez AWS DataSync transférer. Pour plus d'informations et des exemples de configuration, voir Spécifier les DataSync transferts à l'aide d'un manifeste.

Table des matières

Action

Spécifie à quoi DataSync sert le manifeste.

Type : String

Valeurs valides : `TRANSFER`

Obligatoire : non

Format

Spécifie le format de fichier de votre manifeste. Pour plus d'informations, consultez la section Création d'un manifeste.

Type : String

Valeurs valides : `CSV`

Obligatoire : non

Source

Spécifie le manifeste que vous souhaitez DataSync utiliser et l'endroit où il est hébergé.

> **Note**
>
> Vous devez spécifier ce paramètre si vous configurez un nouveau manifeste le 7 février 2024 ou après cette date.
> Si ce n'est pas le cas, vous recevrez un code d'état 400 et une `ValidationException` erreur indiquant qu'il vous manque le rôle IAM DataSync pour accéder au compartiment S3 dans lequel vous hébergez votre manifeste. Pour plus d'informations, consultez la section Fournir DataSync l'accès à votre manifeste.

Type : objet SourceManifestConfig

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

NfsMountOptions

Spécifie comment DataSync accéder à un emplacement à l'aide du protocole NFS.

Table des matières

Version

Spécifie la version NFS que vous DataSync souhaitez utiliser lors du montage de votre partage NFS. Si le serveur refuse d'utiliser la version spécifiée, la tâche échoue.

Vous pouvez spécifier les options suivantes :

- `AUTOMATIC`(par défaut) : DataSync choisit la version 4.1 de NFS.
- `NFS3` : version de protocole sans état qui permet des écritures asynchrones sur le serveur.
- `NFSv4_0` : version de protocole avec état et compatible avec le pare-feu qui prend en charge les délégations et les pseudo-systèmes de fichiers.
- `NFSv4_1` : version de protocole avec état qui prend en charge les sessions, les délégations de répertoires et le traitement parallèle des données. NFS version 4.1 inclut également toutes les fonctionnalités disponibles dans la version 4.0.

> **Note**
>
> DataSync ne prend actuellement en charge que la version 3 de NFS avec Amazon FSx pour les sites NetApp ONTAP.

Type : String

Valeurs valides : `AUTOMATIC | NFS3 | NFS4_0 | NFS4_1`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++

- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

OnPremConfig

Les AWS DataSync agents qui peuvent se connecter à votre serveur de fichiers NFS (Network File System).

Table des matières

AgentArns

Les Amazon Resource Names (ARNs) des DataSync agents qui peuvent se connecter à votre serveur de fichiers NFS.

Vous pouvez spécifier plusieurs agents. Pour plus d'informations, consultez la section Utilisation de plusieurs DataSync agents.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Options

Indique comment votre tâche de transfert est configurée. Ces options incluent le mode DataSync de gestion des fichiers, des objets et des métadonnées associées lors de votre transfert. Vous pouvez également spécifier comment vérifier l'intégrité des données, définir des limites de bande passante pour votre tâche, entre autres options.

Chaque option possède une valeur par défaut. À moins que vous n'en ayez besoin, vous n'avez pas à configurer d'option avant d'appeler StartTaskExecution.

Vous pouvez également remplacer vos options de tâche pour chaque exécution de tâche. Par exemple, vous souhaiterez peut-être ajuster le `LogLevel` pour une exécution individuelle.

Table des matières

Atime

Spécifie s'il faut conserver les métadonnées indiquant la dernière fois qu'un fichier a été lu ou écrit.

> **Note**
>
> Le comportement de `Atime` n'est pas entièrement standard sur toutes les plateformes. DataSync Vous ne pouvez donc le faire que dans la mesure du possible.

- `BEST_EFFORT`(par défaut) : DataSync tente de conserver l'`Atime`attribut d'origine sur tous les fichiers source (c'est-à-dire la version avant les `PREPARING` étapes d'exécution de la tâche). Cette option est recommandée.
- `NONE`- Ignore`Atime`.

> **Note**
>
> Si `Atime` est défini sur `BEST_EFFORT`, `Mtime` doit être défini sur `PRESERVE`.
> Si `Atime` est défini sur `NONE`, `Mtime` doit également être défini sur `NONE`.

Type : String

Valeurs valides : `NONE | BEST_EFFORT`

Obligatoire : non

BytesPerSecond

Limite la bande passante utilisée par une DataSync tâche. Par exemple, si vous DataSync souhaitez utiliser un maximum de 1 Mo, définissez cette valeur sur `1048576` (`=1024*1024`).

> **Note**
>
> Non applicable aux tâches en mode amélioré.

Type : long

Plage valide : Valeur minimum de -1.

Obligatoire : non

Gid

Spécifie l'ID de groupe POSIX (GID) des propriétaires du fichier.

- `INT_VALUE`(par défaut) - Préserve la valeur entière de l'ID utilisateur (UID) et du GID, ce qui est recommandé.
- `NONE`- Ignore l'UID et le GID.

Pour plus d'informations, voir Comprendre le mode de DataSync gestion des métadonnées des fichiers et des objets.

Type : String

Valeurs valides : `NONE | INT_VALUE | NAME | BOTH`

Obligatoire : non

LogLevel

Spécifie le type de journaux DataSync publiés dans un groupe de CloudWatch journaux Amazon Logs. Pour spécifier le groupe de journaux, consultez CloudWatchLogGroupArn.

- `BASIC`- Publie des journaux contenant uniquement des informations de base (telles que les erreurs de transfert).

- `TRANSFER`- Publie des journaux pour tous les fichiers ou objets transférés par votre DataSync tâche et vérifie l'intégrité des données.
- `OFF`- Aucun journal n'est publié.

Type : String

Valeurs valides : `OFF | BASIC | TRANSFER`

Obligatoire : non

Mtime

Spécifie s'il faut conserver les métadonnées indiquant la dernière fois qu'un fichier a été écrit avant l'`PREPARING`étape d'exécution de votre tâche. Cette option est requise lorsque vous devez exécuter une tâche plusieurs fois.

- `PRESERVE`(par défaut) - Préserve l'original`Mtime`, ce qui est recommandé.
- `NONE`- Ignore`Mtime`.

> **Note**
>
> Si `Mtime` est défini sur `PRESERVE`, `Atime` doit être défini sur `BEST_EFFORT`.
> Si `Mtime` est défini sur `NONE`, `Atime` doit également être défini sur `NONE`.

Type : String

Valeurs valides : `NONE | PRESERVE`

Obligatoire : non

ObjectTags

Spécifie si vous DataSync souhaitez utiliser des balises `PRESERVE` d'objet (comportement par défaut) lors du transfert entre systèmes de stockage d'objets. Si vous souhaitez que votre DataSync tâche ignore les balises d'objets, spécifiez la `NONE` valeur.

Type : String

Valeurs valides : `PRESERVE | NONE`

Obligatoire : non

OverwriteMode

Spécifie s'il DataSync faut modifier ou conserver les données à l'emplacement de destination.

- `ALWAYS`(par défaut) : DataSync modifie les données dans l'emplacement de destination lorsque les données source (y compris les métadonnées) ont changé.

  En cas de DataSync remplacement d'objets, des frais supplémentaires peuvent vous être facturés pour certaines classes de stockage Amazon S3 (par exemple, pour la récupération ou la suppression anticipée). Pour plus d'informations, consultez la section Considérations relatives aux classes de stockage associées aux transferts Amazon S3.
- `NEVER`- DataSync ne remplace pas les données dans l'emplacement de destination même si les données source ont changé. Vous pouvez utiliser cette option pour vous protéger contre le remplacement des modifications apportées aux fichiers ou aux objets dans la destination.

Type : String

Valeurs valides : `ALWAYS | NEVER`

Obligatoire : non

PosixPermissions

Spécifie quels utilisateurs ou groupes peuvent accéder à un fichier dans un but spécifique, tel que la lecture, l'écriture ou l'exécution du fichier.

Pour plus d'informations, voir Comprendre le mode de DataSync gestion des métadonnées des fichiers et des objets.

- `PRESERVE`(par défaut) - Préserve les autorisations de style POSIX, ce qui est recommandé.
- `NONE`- Ignore les autorisations de type POSIX.

> **Note**
>
> DataSync peut conserver les autorisations existantes d'un emplacement source.

Type : String

Valeurs valides : `NONE | PRESERVE`

Obligatoire : non

PreserveDeletedFiles

Spécifie si les fichiers de l'emplacement de destination qui n'existent pas dans la source doivent être conservés. Cette option peut avoir une incidence sur le coût de stockage de votre Amazon S3. Si votre tâche supprime des objets, des frais de stockage minimum peuvent vous être facturés pour certaines classes de stockage. Pour des informations détaillées, consultez la section Considérations relatives à l'utilisation des classes de stockage Amazon S3 dans DataSync.

- `PRESERVE`(par défaut) - Ignore ces fichiers de destination, ce qui est recommandé.
- `REMOVE`- Supprime les fichiers de destination absents de la source.

> **Note**
>
> Si vous définissez ce paramètre sur`REMOVE`, vous ne pouvez pas le `TransferMode` définir sur`ALL`. Lorsque vous transférez toutes les données, DataSync il ne scanne pas votre position de destination et ne sait pas quoi supprimer.

Type : String

Valeurs valides : `PRESERVE | REMOVE`

Obligatoire : non

PreserveDevices

Spécifie s'il DataSync convient de conserver les métadonnées des unités de blocs et de caractères dans l'emplacement source et de recréer les fichiers avec le nom et les métadonnées de ce périphérique sur la destination. DataSync copie uniquement le nom et les métadonnées de ces appareils.

> **Note**
>
> DataSync Impossible de copier le contenu réel de ces appareils car ils ne sont pas des terminaux et ne renvoient pas de marqueur end-of-file (EOF).

- `NONE`(par défaut) - Ignore les périphériques spéciaux (recommandé).
- `PRESERVE`- Préserve les métadonnées des caractères et des blocs du périphérique. Cette option n'est actuellement pas prise en charge pour Amazon EFS.

Type : String

Valeurs valides : `NONE | PRESERVE`

Obligatoire : non

SecurityDescriptorCopyFlags

Spécifie les composants du descripteur de sécurité SMB qui sont copiés des objets source vers les objets de destination.

Cette valeur est uniquement utilisée pour les transferts entre les sites SMB et Amazon FSx pour les serveurs de fichiers Windows ou entre deux FSx pour les emplacements de serveurs de fichiers Windows. Pour plus d'informations, voir Comprendre le mode de DataSync gestion des métadonnées des fichiers et des objets.

- `OWNER_DACL`(par défaut) - Pour chaque objet copié, DataSync copie les métadonnées suivantes :
  - Le propriétaire de l'objet.
  - Listes de contrôle d'accès discrétionnaires NTFS (DACLs), qui déterminent s'il faut accorder l'accès à un objet.

    DataSync ne copiera pas les listes de contrôle d'accès au système NTFS (SACLs) avec cette option.
- `OWNER_DACL_SACL`- Pour chaque objet copié, DataSync copie les métadonnées suivantes :
  - Le propriétaire de l'objet.
  - Listes de contrôle d'accès discrétionnaires NTFS (DACLs), qui déterminent s'il faut accorder l'accès à un objet.
  - SACLs, qui sont utilisés par les administrateurs pour consigner les tentatives d'accès à un objet sécurisé.

    La copie SACLs nécessite l'octroi d'autorisations supplémentaires à l'utilisateur Windows DataSync qui accède à votre site SMB. Pour plus d'informations sur le choix d'un utilisateur doté des autorisations appropriées, consultez les autorisations requises pour SMB, FSx pour Windows File Server ou FSx pour ONTAP (selon le type d'emplacement de votre transfert).
- `NONE`- Aucun des composants du descripteur de sécurité SMB n'est copié. Les objets de destination appartiennent à l'utilisateur qui a été indiqué pour accéder à l'emplacement de destination. DACLs et SACLs sont définis en fonction de la configuration du serveur de destination.

Type : String

Valeurs valides : `NONE | OWNER_DACL | OWNER_DACL_SACL`

Obligatoire : non

TaskQueueing

Spécifie si vos tâches de transfert doivent être placées dans une file d'attente dans certains scénarios lors de l'exécution de plusieurs tâches. C'est le `ENABLED` cas par défaut.

Type : String

Valeurs valides : `ENABLED | DISABLED`

Obligatoire : non

TransferMode

Spécifie s'il DataSync transfère uniquement les données (y compris les métadonnées) qui diffèrent d'un emplacement à l'autre après une copie initiale ou s'il transfère toutes les données à chaque fois que vous exécutez la tâche. Si vous prévoyez des transferts récurrents, vous souhaiterez peut-être uniquement transférer les modifications apportées depuis l'exécution de votre tâche précédente.

- `CHANGED`(par défaut) - Après votre transfert complet initial, DataSync copie uniquement les données et les métadonnées qui diffèrent entre l'emplacement source et l'emplacement de destination.
- `ALL`- DataSync copie tout le contenu de la source vers la destination sans comparer les différences entre les emplacements.

Type : String

Valeurs valides : `CHANGED | ALL`

Obligatoire : non

Uid

Spécifie l'ID utilisateur POSIX (UID) du propriétaire du fichier.

- `INT_VALUE`(par défaut) - Préserve la valeur entière de l'UID et de l'ID de groupe (GID), ce qui est recommandé.
- `NONE`- Ignore l'UID et le GID.

Pour plus d'informations, voir Métadonnées copiées par DataSync.

Type : String

Valeurs valides : `NONE | INT_VALUE | NAME | BOTH`

Obligatoire : non

VerifyMode

Spécifie si et comment DataSync vérifie l'intégrité de vos données à la fin de votre transfert.

- `ONLY_FILES_TRANSFERRED`(recommandé) : DataSync calcule la somme de contrôle des données transférées (y compris les métadonnées) à l'emplacement source. À la fin du transfert, compare DataSync ensuite cette somme de contrôle à la somme de contrôle calculée sur ces données à destination.

  > **Note**
  >
  > Il s'agit de l'option par défaut pour les tâches en mode amélioré.

  Nous recommandons cette option lors du transfert vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour plus d'informations, consultez la section Considérations relatives aux classes de stockage associées aux sites Amazon S3.

- `POINT_IN_TIME_CONSISTENT`- À la fin du transfert, DataSync vérifie l'intégralité de la source et de la destination pour vérifier que les deux emplacements sont parfaitement synchronisés.

  > **Note**
  >
  > Il s'agit de l'option par défaut pour les tâches en mode de base et n'est actuellement pas prise en charge avec les tâches en mode amélioré.

  Si vous utilisez un manifeste, il analyse et vérifie DataSync uniquement ce qui est répertorié dans le manifeste.

  Vous ne pouvez pas utiliser cette option lors du transfert vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour plus d'informations, consultez la section Considérations relatives aux classes de stockage associées aux sites Amazon S3.

- `NONE`- DataSync effectue des contrôles d'intégrité des données uniquement pendant votre transfert. Contrairement aux autres options, il n'y a aucune vérification supplémentaire à la fin de votre transfert.

Type : String

Valeurs valides : `POINT_IN_TIME_CONSISTENT | ONLY_FILES_TRANSFERRED | NONE`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Platform

Les informations relatives à la plate-forme concernant l' AWS DataSync agent, telles que le numéro de version.

Table des matières

Version

Version de l' DataSync agent.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

PrivateLinkConfig

Spécifie la manière dont votre AWS DataSync agent se connecte à AWS l'aide d'un point de terminaison de service de cloud privé virtuel (VPC). Un agent qui utilise un point de terminaison VPC n'est pas accessible via Internet public.

Table des matières

PrivateLinkEndpoint

Spécifie le point de terminaison VPC fourni par AWS PrivateLinklequel votre agent se connecte.

Type : String

Contraintes de longueur : longueur minimale de 7. Longueur maximale de 15.

Modèle : `\A(25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d)){3}\z`

Obligatoire : non

SecurityGroupArns

Spécifie les Amazon Resource Names (ARN) du groupe de sécurité qui fournit l' DataSync accès à votre point de terminaison VPC. Vous ne pouvez spécifier qu'un seul ARN.

Type : tableau de chaînes

Membres du tableau : nombre fixe de 1 élément.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obligatoire : non

SubnetArns

Spécifie l'ARN du sous-réseau où se trouve le point de terminaison de votre VPC. Vous ne pouvez spécifier qu'un seul ARN.

Type : tableau de chaînes

Membres du tableau : nombre fixe de 1 élément.

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-0-9]*:[0-9]{12}:subnet/.*$`

Obligatoire : non

VpcEndpointId

Spécifie l'ID du point de terminaison VPC auquel votre agent se connecte.

Type : String

Modèle : `^vpce-[0-9a-f]{17}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

QopConfiguration

La configuration de la qualité de protection (QOP) spécifie les paramètres RPC (Remote Procedure Call) et de confidentialité du transfert de données configurés sur le cluster de système de fichiers distribué Hadoop (HDFS).

Table des matières

DataTransferProtection

Le paramètre de protection du transfert de données configuré sur le cluster HDFS. Ce paramètre correspond à votre paramètre `dfs.data.transfer.protection` dans le fichier `hdfs-site.xml` sur votre cluster Hadoop.

Type : String

Valeurs valides : `DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY`

Obligatoire : non

RpcProtection

Le paramètre de protection RPC configuré sur le cluster HDFS. Ce paramètre correspond au paramètre `hadoop.rpc.protection` de votre fichier `core-site.xml` sur votre cluster Hadoop.

Type : String

Valeurs valides : `DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportDestination

Spécifie l'endroit DataSync où est chargé votre rapport de tâches.

Table des matières

S3

Spécifie le compartiment Amazon S3 dans lequel DataSync télécharge votre rapport de tâches.

Type : objet ReportDestinationS3

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportDestinationS3

Spécifie le compartiment Amazon S3 dans lequel DataSync télécharge votre rapport de tâches.

Table des matières

BucketAccessRoleArn

Spécifie le nom de ressource Amazon (ARN) de la politique IAM qui permet DataSync de télécharger un rapport de tâches dans votre compartiment S3. Pour plus d'informations, consultez DataSync Autoriser le chargement d'un rapport de tâches dans un compartiment Amazon S3.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Obligatoire : oui

S3BucketArn

Spécifie l'ARN du compartiment S3 dans lequel DataSync télécharge votre rapport.

Type : String

Contraintes de longueur : longueur maximale de 268.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

Obligatoire : oui

Subdirectory

Spécifie un préfixe de compartiment pour votre rapport.

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportOverride

Spécifie le niveau de détail d'un aspect particulier de votre rapport de DataSync tâches.

Table des matières

ReportLevel

Spécifie si votre rapport de tâches inclut uniquement les erreurs ou les réussites et les erreurs.

Par exemple, il se peut que votre rapport n'inclue généralement que les éléments qui ne se sont pas bien déroulés dans votre transfert (`ERRORS_ONLY`). Dans le même temps, vous souhaitez vérifier que votre filtre de tâches fonctionne correctement. Dans ce cas, vous pouvez obtenir une liste des fichiers ignorés DataSync avec succès et des fichiers transférés que vous n'avez pas dû transférer (`SUCCESSES_AND_ERRORS`).

Type : String

Valeurs valides : `ERRORS_ONLY | SUCCESSES_AND_ERRORS`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportOverrides

Le niveau de détail inclus dans chaque aspect de votre rapport de DataSync tâches.

Table des matières

Deleted

Spécifie le niveau de rapport pour les fichiers, les objets et les répertoires qui DataSync ont été tentés de supprimer dans votre emplacement de destination. Cela ne s'applique que si vous configurez votre tâche pour supprimer des données dans la destination qui ne figurent pas dans la source.

Type : objet ReportOverride

Obligatoire : non

Skipped

Spécifie le niveau de signalement pour les fichiers, les objets et les répertoires qui DataSync ont tenté d'être ignorés lors de votre transfert.

Type : objet ReportOverride

Obligatoire : non

Transferred

Spécifie le niveau de signalement des fichiers, objets et répertoires ayant fait l'objet d'une DataSync tentative de transfert.

Type : objet ReportOverride

Obligatoire : non

Verified

Spécifie le niveau de rapport pour les fichiers, les objets et les répertoires qui DataSync ont tenté de vérifier à la fin de votre transfert.

Type : objet ReportOverride

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportResult

Indique si un rapport de tâches complet DataSync a été créé pour votre transfert.

Table des matières

ErrorCode

Indique le code associé à l'erreur s'il n'est pas DataSync possible de créer un rapport complet.

Type : chaîne

Obligatoire : non

ErrorDetail

Fournit des informations sur les problèmes rencontrés lors de la création d'un rapport.

Type : chaîne

Obligatoire : non

Status

DataSync Indique si vous travaillez toujours sur votre rapport, si vous avez créé un rapport ou si vous ne pouvez pas créer un rapport complet.

Type : String

Valeurs valides : `PENDING | SUCCESS | ERROR`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

S3Config

Spécifie le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) DataSync utilisé pour accéder à votre compartiment S3.

Pour plus d'informations, consultez la section Fournir DataSync un accès aux compartiments S3.

Table des matières

BucketAccessRoleArn

Spécifie l'ARN du rôle IAM DataSync utilisé pour accéder à votre compartiment S3.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

S3ManifestConfig

Spécifie le compartiment S3 dans lequel vous hébergez le manifeste que vous AWS DataSync souhaitez utiliser. Pour plus d'informations et des exemples de configuration, voir Spécifier les DataSync transferts à l'aide d'un manifeste.

Table des matières

BucketAccessRoleArn

Spécifie le rôle AWS Identity and Access Management (IAM) qui permet d'accéder DataSync à votre manifeste. Pour plus d'informations, consultez la section Fournir DataSync l'accès à votre manifeste.

Type : String

Contraintes de longueur : longueur maximale de 2048.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Obligatoire : oui

ManifestObjectPath

Spécifie la clé d'objet Amazon S3 de votre manifeste. Cela peut inclure un préfixe (par exemple,`prefix/my-manifest.csv`).

Type : String

Contraintes de longueur : longueur maximale de 4096.

Modèle : `^[a-zA-Z0-9_\-\+\./\(\)\p{Zs}]*$`

Obligatoire : oui

S3BucketArn

Spécifie le nom de ressource Amazon (ARN) du compartiment S3 dans lequel vous hébergez votre manifeste.

Type : String

Contraintes de longueur : longueur maximale de 268.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\-0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\-0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_]{1,255}$`

Obligatoire : oui

ManifestObjectVersionId

Spécifie l'ID de version de l'objet du manifeste que vous DataSync souhaitez utiliser. Si ce n'est pas le cas, DataSync utilise la dernière version de l'objet.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^.+$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

SmbMountOptions

Spécifie la version du protocole SMB (Server Message Block) qui permet d'accéder AWS DataSync à un serveur de fichiers SMB.

Table des matières

Version

Par défaut, choisit DataSync automatiquement une version du protocole SMB en fonction de la négociation avec votre serveur de fichiers SMB. Vous pouvez également configurer DataSync pour utiliser une version SMB spécifique, mais nous vous recommandons de le faire uniquement si DataSync vous rencontrez des difficultés pour négocier automatiquement avec le serveur de fichiers SMB.

Les options de configuration de la version SMB sont les suivantes :

- `AUTOMATIC`(par défaut) : DataSync et le serveur de fichiers SMB négocient la version la plus élevée de SMB qu'ils supportent mutuellement entre 2.1 et 3.1.1.

  Il s'agit là de l'option recommandée. Si vous optez pour une version spécifique que votre serveur de fichiers ne prend pas en charge, vous risquez de recevoir une erreur `Operation Not Supported`.
- `SMB3` : restreint la négociation de protocole à la version SMB 3.0.2 uniquement.
- `SMB2`: Limite la négociation du protocole à la version 2.1 de SMB uniquement.
- `SMB2_0`: limite la négociation du protocole à la version 2.0 de SMB uniquement.
- `SMB1`: limite la négociation du protocole à la version 1.0 de SMB uniquement.

> **Note**
>
> L'`SMB1`option n'est pas disponible lors de la création d'un point de vente Amazon FSx pour NetApp ONTAP.

Type : String

Valeurs valides : `AUTOMATIC | SMB2 | SMB3 | SMB1 | SMB2_0`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

SourceManifestConfig

Spécifie le manifeste que vous souhaitez AWS DataSync utiliser et l'endroit où il est hébergé. Pour plus d'informations et des exemples de configuration, voir Spécifier les DataSync transferts à l'aide d'un manifeste.

Table des matières

S3

Spécifie le compartiment S3 dans lequel vous hébergez votre manifeste.

Type : objet S3ManifestConfig

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TagListEntry

Une paire clé-valeur représentant une balise unique appliquée à une AWS ressource.

Table des matières

Key

La clé d'une balise AWS de ressource.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:/-]+$`

Obligatoire : oui

Value

La valeur d'une balise AWS de ressource.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskExecutionFilesFailedDetail

Nombre d'objets dont la préparation, le transfert, la vérification et la suppression DataSync échouent lors de l'exécution de la tâche.

> **Note**
>
> S'applique uniquement aux tâches en mode amélioré.

Table des matières

Delete

Le nombre d'objets qui DataSync ne sont pas supprimés lors de l'exécution de la tâche.

Type : long

Obligatoire : non

Prepare

Le nombre d'objets dont la préparation DataSync échoue pendant l'exécution de la tâche.

Type : long

Obligatoire : non

Transfer

Le nombre d'objets qui DataSync ne parviennent pas à être transférés pendant l'exécution de la tâche.

Type : long

Obligatoire : non

Verify

Le nombre d'objets dont la vérification DataSync échoue pendant l'exécution de la tâche.

Type : long

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskExecutionFilesListedDetail

Le nombre d'objets DataSync trouvés sur vos sites.

> **Note**
>
> S'applique uniquement aux tâches en mode amélioré.

Table des matières

AtDestinationForDelete

Le nombre d'objets trouvés DataSync sur votre lieu de destination. Ce compteur n'est applicable que si vous configurez votre tâche pour supprimer des données dans la destination qui ne figurent pas dans la source.

Type : long

Obligatoire : non

AtSource

Le nombre d'objets DataSync trouvés à votre emplacement source.

- Dans le cas d'un manifeste, DataSync répertorie uniquement le contenu de votre manifeste (et non tout ce qui se trouve à votre emplacement source).
- Avec un filtre d'inclusion, DataSync répertorie uniquement ce qui correspond au filtre à votre emplacement source.
- Avec un filtre d'exclusion, DataSync répertorie tout ce qui se trouve à votre emplacement source avant d'appliquer le filtre.

Type : long

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskExecutionListEntry

Représente une entrée unique dans une liste d'exécutions de AWS DataSync tâches renvoyée avec l'ListTaskExecutionsopération.

Table des matières

Status

État de l'exécution d'une tâche. Pour plus d'informations, consultez la section Statuts d'exécution des tâches.

Type : String

Valeurs valides : `QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR`

Obligatoire : non

TaskExecutionArn

Le nom de ressource Amazon (ARN) d'une exécution de tâche.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Obligatoire : non

TaskMode

Le mode tâche que vous utilisez. Pour plus d'informations, consultez la section Choix d'un mode de tâche pour le transfert de données.

Type : String

Valeurs valides : `BASIC | ENHANCED`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskExecutionResultDetail

Fournit des informations détaillées sur le résultat de l'exécution de vos AWS DataSync tâches.

Table des matières

ErrorCode

Erreur DataSync survenue lors de l'exécution de votre tâche. Vous pouvez utiliser ces informations pour résoudre les problèmes.

Type : chaîne

Obligatoire : non

ErrorDetail

Description détaillée d'une erreur DataSync survenue lors de l'exécution de votre tâche. Vous pouvez utiliser ces informations pour résoudre les problèmes.

Type : chaîne

Obligatoire : non

PrepareDuration

Durée en millisecondes pendant laquelle votre tâche a été exécutée dans l'étape. `PREPARING` Pour plus d'informations, consultez la section Statuts d'exécution des tâches.

Pour les tâches en mode amélioré, la valeur est toujours`0`. Pour plus d'informations, consultez Comment DataSync prépare votre transfert de données.

Type : long

Plage valide : Valeur minimum de 0.

Obligatoire : non

PrepareStatus

État de l'`PREPARING`étape d'exécution de votre tâche. Pour plus d'informations, consultez la section Statuts d'exécution des tâches.

Type : String

Valeurs valides : `PENDING | SUCCESS | ERROR`

Obligatoire : non

TotalDuration

Durée en millisecondes pendant laquelle votre tâche a été exécutée.

Type : long

Plage valide : Valeur minimum de 0.

Obligatoire : non

TransferDuration

Durée en millisecondes pendant laquelle votre tâche a été exécutée dans l'étape. `TRANSFERRING` Pour plus d'informations, consultez la section Statuts d'exécution des tâches.

Pour les tâches en mode amélioré, la valeur est toujours`0`. Pour plus d'informations, consultez Comment DataSync transférer vos données.

Type : long

Plage valide : Valeur minimum de 0.

Obligatoire : non

TransferStatus

État de l'`TRANSFERRING`étape d'exécution de votre tâche. Pour plus d'informations, consultez la section Statuts d'exécution des tâches.

Type : String

Valeurs valides : `PENDING | SUCCESS | ERROR`

Obligatoire : non

VerifyDuration

Durée en millisecondes pendant laquelle votre tâche a été exécutée dans l'étape. `VERIFYING` Pour plus d'informations, consultez la section Statuts d'exécution des tâches.

Pour les tâches en mode amélioré, la valeur est toujours`0`. Pour plus d'informations, consultez Comment DataSync vérifier l'intégrité de vos données.

Type : long

Plage valide : Valeur minimum de 0.

Obligatoire : non

VerifyStatus

État de l'`VERIFYING`étape d'exécution de votre tâche. Pour plus d'informations, consultez la section Statuts d'exécution des tâches.

Type : String

Valeurs valides : `PENDING | SUCCESS | ERROR`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskFilter

Vous pouvez utiliser des filtres d'API pour affiner la liste des ressources renvoyées par`ListTasks`. Par exemple, pour récupérer toutes les tâches d'un emplacement source, vous pouvez les utiliser `ListTasks` avec le nom du filtre `LocationId` et `Operator Equals` avec l'ARN de l'emplacement.

Pour plus d'informations, consultez la section Filtrage DataSync des ressources.

Table des matières

Name

Nom du filtre utilisé. Chaque appel d'API prend en charge une liste de filtres disponibles pour celui-ci. Par exemple, `LocationId` ou `ListTasks`.

Type : String

Valeurs valides : `LocationId | CreationTime`

Obligatoire : oui

Operator

Opérateur utilisé pour comparer les valeurs des filtres (par exemple, `Equals` ou`Contains`).

Type : String

Valeurs valides : `Equals | NotEquals | In | LessThanOrEqual | LessThan | GreaterThanOrEqual | GreaterThan | Contains | NotContains | BeginsWith`

Obligatoire : oui

Values

Les valeurs que vous souhaitez filtrer. Par exemple, vous souhaiterez peut-être afficher uniquement les tâches relatives à un lieu de destination spécifique.

Type : tableau de chaînes

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Modèle : `^[0-9a-zA-Z_\ \-\:\*\.\\/\?-]*$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskListEntry

Représente une entrée unique dans une liste de tâches. `TaskListEntry`renvoie un tableau contenant une liste de tâches lorsque l'ListTasksopération est appelée. Une tâche inclut les systèmes de fichiers source et de destination à synchroniser ainsi que les options à utiliser pour les tâches.

Table des matières

Name

Nom de la tâche .

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatoire : non

Status

État de la tâche.

Type : String

Valeurs valides : `AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE`

Obligatoire : non

TaskArn

Amazon Resource Name (ARN) de la tâche.

Type : String

Contraintes de longueur : Longueur maximum de 128.

Modèle : `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Obligatoire : non

TaskMode

Le mode tâche que vous utilisez. Pour plus d'informations, consultez la section Choix d'un mode de tâche pour le transfert de données.

Type : String

Valeurs valides : `BASIC | ENHANCED`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskReportConfig

Spécifie la manière dont vous souhaitez configurer un rapport de tâches, qui fournit des informations détaillées sur votre AWS DataSync transfert.

Pour plus d'informations, consultez la section Rapports de tâches.

Table des matières

Destination

Spécifie le compartiment Amazon S3 dans lequel DataSync télécharge votre rapport de tâches. Pour plus d'informations, consultez la section Rapports de tâches.

Type : objet ReportDestination

Obligatoire : non

ObjectVersionIds

Spécifie si votre rapport de tâches inclut la nouvelle version de chaque objet transféré dans un compartiment S3. Cela ne s'applique que si vous activez le versionnement sur votre bucket. N'oubliez pas que définir cette valeur sur `INCLUDE` peut augmenter la durée d'exécution de vos tâches.

Type : String

Valeurs valides : `INCLUDE | NONE`

Obligatoire : non

OutputType

Spécifie le type de rapport de tâches que vous souhaitez :

- `SUMMARY_ONLY`: fournit les informations nécessaires sur votre tâche, notamment le nombre de fichiers, d'objets et de répertoires transférés et la durée du transfert.
- `STANDARD`: fournit des informations complètes sur votre tâche, notamment une liste complète des fichiers, objets et répertoires qui ont été transférés, ignorés, vérifiés, etc.

Type : String

Valeurs valides : `SUMMARY_ONLY | STANDARD`

Obligatoire : non

Overrides

Personnalise le niveau de reporting pour certains aspects de votre rapport de tâches. Par exemple, votre rapport peut généralement ne contenir que des erreurs, mais vous pouvez spécifier que vous souhaitez une liste des réussites et des erreurs uniquement pour les fichiers qui DataSync ont tenté de supprimer dans votre emplacement de destination.

Type : objet ReportOverrides

Obligatoire : non

ReportLevel

Spécifie si vous souhaitez que votre rapport de tâches inclue uniquement les problèmes rencontrés lors de votre transfert ou une liste de ce qui a réussi et de ce qui n'a pas été le cas.

- `ERRORS_ONLY`: un rapport indique ce qui n' DataSync a pas pu être transféré, ignoré, vérifié ou supprimé.
- `SUCCESSES_AND_ERRORS`: un rapport indique ce qui DataSync a pu ou non être transféré, ignoré, vérifié et supprimé.

Type : String

Valeurs valides : `ERRORS_ONLY | SUCCESSES_AND_ERRORS`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskSchedule

Configure votre AWS DataSync tâche pour qu'elle soit exécutée selon un calendrier (à un intervalle minimum d'une heure).

Table des matières

ScheduleExpression

Spécifie le planning de vos tâches à l'aide d'une expression cron ou rate.

Utilisez des expressions cron pour les plannings de tâches exécutés à une heure et à un jour spécifiques. Par exemple, l'expression cron suivante crée un planning de tâches qui s'exécute à 8 h le premier mercredi de chaque mois :

```
cron(0 8 * * 3#1)
```

Utilisez des expressions de taux pour les planifications de tâches exécutées à intervalles réguliers. Par exemple, l'expression de taux suivante crée un planning de tâches exécuté toutes les 12 heures :

```
rate(12 hours)
```

Pour plus d'informations sur la syntaxe des expressions cron et rate, consultez le guide de l' EventBridge utilisateur Amazon.

Type : String

Contraintes de longueur : longueur maximale de 256.

Modèle : `^[a-zA-Z0-9\ \_\*\?\,\|\^\-\/\#\s\(\)\+]*$`

Obligatoire : oui

Status

Spécifie s'il faut activer ou désactiver votre calendrier de tâches. Votre calendrier est activé par défaut, mais il peut arriver que vous deviez le désactiver. Par exemple, vous devrez peut-être suspendre un transfert récurrent pour résoudre un problème lié à votre tâche ou effectuer des opérations de maintenance sur votre système de stockage.

DataSync peut désactiver automatiquement votre planification si votre tâche échoue à plusieurs reprises avec la même erreur. Pour de plus amples informations, veuillez consulter TaskScheduleDetails.

Type : String

Valeurs valides : `ENABLED | DISABLED`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

TaskScheduleDetails

Fournit des informations sur le planning de vos AWS DataSync tâches.

Table des matières

DisabledBy

Indique la façon dont votre calendrier de tâches a été désactivé.

- `USER`- Votre planning a été désactivé manuellement à l'aide de l'UpdateTaskopération ou de DataSync la console.
- `SERVICE`- Votre planning a été automatiquement désactivé DataSync car la tâche a échoué à plusieurs reprises avec la même erreur.

Type : String

Valeurs valides : `USER | SERVICE`

Obligatoire : non

DisabledReason

Indique la raison pour laquelle le calendrier des tâches est désactivé.

Si votre emploi du temps est désactivé par`USER`, un `Manually disabled by user.` message s'affiche.

Si votre planification est désactivée par`SERVICE`, un message d'erreur s'affiche pour vous aider à comprendre pourquoi la tâche continue d'échouer. Pour plus d'informations sur la résolution DataSync des erreurs, consultez la section Résolution des problèmes liés aux DataSync transferts.

Type : String

Contraintes de longueur : longueur maximale de 8192.

Modèle : `^[\w\s.,'?!:;\/=|<>()-]*$`

Obligatoire : non

StatusUpdateTime

Indique la dernière fois que le statut de votre planning de tâches a été modifié. Par exemple, si vous désactivez DataSync automatiquement votre programme en raison d'une erreur répétée, vous pouvez voir à quel moment le calendrier a été désactivé.

Type : Timestamp

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Erreurs courantes

Cette section répertorie les erreurs communes aux actions d'API de tous les AWS services. Pour les erreurs spécifiques à une action d'API pour ce service, consultez la rubrique pour cette action d'API.

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 400

IncompleteSignature

La signature de la demande n'est pas conforme aux AWS normes.

Code d'état HTTP : 400

InternalFailure

Le traitement de la demande a échoué en raison d'une erreur, d'une exception ou d'un échec inconnu.

Code d'état HTTP : 500

InvalidAction

L'action ou l'opération demandée n'est pas valide. Vérifiez que l’action est entrée correctement.

Code d’état HTTP : 400

InvalidClientTokenId

Le certificat X.509 ou AWS l'ID de clé d'accès fourni n'existe pas dans nos archives.

Code d’état HTTP : 403

NotAuthorized

Vous ne disposez pas de l’autorisation nécessaire pour effectuer cette action.

Code d’état HTTP : 400

OptInRequired

L'ID de clé d' AWS accès nécessite un abonnement au service.

Code d’état HTTP : 403

RequestExpired

La demande est parvenue au service plus de 15 minutes après l'horodatage sur la demande ou plus de 15 minutes après la date d'expiration de la demande (par exemple pour les demandes pré-signées URLs), ou le horodatage sur la demande est daté dans plus de 15 minutes dans le futur.

Code d’état HTTP : 400

ServiceUnavailable

La requête a échoué en raison d’une défaillance temporaire du serveur.

HTTP Status Code: 503

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

Code d’état HTTP : 400

ValidationError

L'entrée ne satisfait pas les contraintes spécifiées par un AWS service.

Code d'état HTTP : 400

Paramètres communs

La liste suivante contient les paramètres que toutes les actions utilisent pour signer les demandes Signature Version 4 à l'aide d'une chaîne de requête. Tous les paramètres spécifiques d'une action particulière sont énumérées dans le sujet consacré à cette action. Pour plus d'informations sur la version 4 de Signature, consultez la section Signing AWS API du guide de l'utilisateur IAM.

Action

Action à effectuer.

Type : chaîne

Obligatoire : oui

Version

Version de l'API pour laquelle la demande est écrite, exprimée dans le format YYYY-MM-DD.

Type : chaîne

Obligatoire : oui

X-Amz-Algorithm

Algorithme de hachage que vous avez utilisé pour créer la signature de la demande.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Valeurs valides : `AWS4-HMAC-SHA256`

Obligatoire : Conditionnelle

X-Amz-Credential

Valeur de la portée des informations d'identification, qui est une chaîne incluant votre clé d'accès, la date, la région cible, le service demandé et une chaîne de terminaison (« aws4_request »). Spécifiez la valeur au format suivant : access_key/AAAAMMJJ/région/service/aws4_request.

Pour plus d'informations, consultez la section Création d'une demande d' AWS API signée dans le guide de l'utilisateur IAM.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Date

La date utilisée pour créer la signature. Le format doit être au format de base ISO 8601 (AAAAMMJJ'T'HHMMSS'Z'). Par exemple, la date et l'heure suivantes sont une X-Amz-Date valeur valide :`20120325T120000Z`.

Condition : X-Amz-Date est un en-tête facultatif pour toutes les demandes. Il peut être utilisé pour signer les demandes. Si l'en-tête Date est spécifié au format de base ISO 8601, X-Amz-Date il n'est pas obligatoire. Lorsqu'il X-Amz-Date est utilisé, il remplace toujours la valeur de l'en-tête Date. Pour plus d'informations, consultez la section Éléments d'une signature de demande d' AWS API dans le Guide de l'utilisateur IAM.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Security-Token

Le jeton de sécurité temporaire obtenu par un appel à AWS Security Token Service (AWS STS). Pour obtenir la liste des services prenant en charge les informations d'identification de sécurité temporaires d' AWS STS, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Condition : Si vous utilisez des informations d'identification de sécurité temporaires provenant de AWS STS, vous devez inclure le jeton de sécurité.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Signature

Spécifie la signature codée en hexadécimal qui a été calculée à partir de la chaîne à signer et de la clé de signature dérivée.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-SignedHeaders

Spécifie tous les en-têtes HTTP qui ont été inclus dans la demande canonique. Pour plus d'informations sur la spécification d'en-têtes signés, consultez la section Créer une demande d' AWS API signée dans le guide de l'utilisateur IAM.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

Historique du document

Le tableau suivant décrit les ajouts importants à la AWS DataSync documentation. Nous mettons également fréquemment à jour la documentation pour répondre aux commentaires que vous nous envoyez.

Pour être informé des mises à jour de cette documentation, abonnez-vous au flux RSS.

Modification	Description	Date
Support ajouté pour les IPv6 adresses	Vous pouvez désormais utiliser IPv4 les IPv6 adresses et pour vous connecter aux sources de données prises en charge DataSync et pour les transférer.	16 juillet 2025
Discovery n'est plus disponible	Depuis le 20 mai 2025, Discovery n'est plus une DataSync fonctionnalité disponible.	20 mai 2025
AWS mise à jour de stratégie gérée - Mise à jour de la politique existante	La `AWSDataSyncFullAccess` politique a mis à jour les déclarations d'autorisation qui suppriment les conditions de balisage des autorisations DataSync utilisées pour créer des secrets Secrets Manager.	13 mai 2025
AWS mise à jour de stratégie gérée - Mise à jour de la politique existante	La `AWSDataSyncFullAccess` politique comporte de nouvelles autorisations qui permettent DataSync de travailler avec AWS Secrets Manager.	7 mai 2025

AWS mise à jour de stratégie gérée - Mise à jour de la politique existante	La `AWSDataSyncFullAccess` politique comporte de nouvelles autorisations qui permettent DataSync de travailler avec AWS Secrets Manager.	23 avril 2025
AWS mise à jour de stratégie gérée - Mise à jour de la politique existante	La `AWSDataSyncFullAccess` politique comporte de nouvelles autorisations qui DataSync permettent de travailler avec AWS Secrets Manager et AWS Key Management Service.	23 avril 2025
AWS mise à jour de stratégie gérée - Mise à jour de la politique existante	`AWSDataSyncServiceRolePolicy` Il dispose de nouvelles autorisations qui permettent DataSync de travailler avec AWS Secrets Manager.	15 avril 2025
Réalisation de migrations de données volumineuses	Découvrez comment planifier des migrations de données à grande échelle DataSync pour transférer des fichiers ou des objets depuis un stockage sur site ou dans le cloud vers AWS.	19 février 2025
Support pour Kerberos avec des sites de PME	DataSync peut désormais utiliser l'authentification Kerberos lors de la connexion aux serveurs de fichiers SMB (Server Message Block).	28 janvier 2025

Nouvelle Région AWS	AWS DataSync est disponible pour les transferts de données dans la région du Mexique (centre).	14 janvier 2025
Nouvelle Région AWS	AWS DataSync est disponible pour les transferts de données dans la région Asie-Pacifique (Thaïlande).	7 janvier 2025
Mettre à jour les emplacements AWS de stockage	Vous pouvez désormais mettre à jour vos emplacements de FSx transfert Amazon S3, Amazon EFS et Amazon.	18 décembre 2024
Je ne suis plus compatible avec Snowball Edge	Depuis le 12 novembre 2024, il DataSync n'est plus pris en charge AWS Snowball Edge.	13 novembre 2024
Nouvelle politique AWS gérée	Le rôle DataSync lié au service nommé `AWSServiceRoleForDataSync` utilise une nouvelle politique gérée nommée. `AWSDataSyncServiceRolePolicy`	30 octobre 2024
Présentation du mode amélioré	Avec le mode amélioré, vous pouvez transférer un nombre pratiquement illimité d'objets entre les sites Amazon S3.	30 octobre 2024
AWS mises à jour de politiques gérées - Mise à jour d'une politique existante	La `AWSDataSyncFullAccess` politique prévoit une nouvelle autorisation pour les services compatibles avec DataSync.	30 octobre 2024

Support pour les comptes Azure de stockage à usage général v1	DataSync peut fonctionner avec des comptes Azure de stockage v1 à usage général lors d'un transfert vers ou depuis. Microsoft Azure Blob Storage	4 octobre 2024
Nouvelle méthode de configuration des plannings de tâches	Vous pouvez configurer vos plannings de DataSync tâches à l'aide d'expressions de taux.	22 août 2024
Nouvelle Région AWS	AWS DataSync est disponible pour les transferts de données dans la région Asie-Pacifique (Malaisie).	21 août 2024
Support pour les transferts interrégionaux sans agent incluant une région optionnelle	Vous n'avez plus besoin d'un DataSync agent pour les transferts entre les AWS services de stockage lorsqu'au moins un emplacement de stockage est inscrit. Région AWS	24 juillet 2024
AWS mises à jour de politiques gérées - Mise à jour d'une politique existante	La `AWSDataSyncFullAccess` politique prévoit une nouvelle autorisation pour les services compatibles avec DataSync.	22 juillet 2024
Tutoriel multi-comptes S3 mis à jour	Suppression de certaines autorisations d'utilisateur du compte source qui ne sont plus requises pour ce transfert.	10 juin 2024
Nouveau statut d'exécution des tâches	Le `CANCELLING` statut indique quand l'exécution d'une tâche est annulée.	15 mai 2024

Nouvelle option pour suspendre les plannings de tâches	Vous pouvez désactiver votre calendrier des AWS DataSync tâches lorsque vous devez résoudre des problèmes ou effectuer la maintenance du système de stockage.	24 avril 2024
Chiffrement TLS mis à jour pour les points de terminaison FIPS	AWS DataSync utilise le chiffrement TLS_AES_1 28_GCM_ SHA256 (secp256r 1) pour les points de terminais on du service FIPS (Federal Information Processing Standard).	22 avril 2024
AWS mises à jour de politique s gérées - Mise à jour d'une politique existante	La `AWSDataSyncFullAcc ess` politique prévoit une nouvelle autorisation pour les services compatibles avec DataSync.	16 février 2024
Transférer des fichiers ou des objets spécifiques à l'aide d'un manifeste	AWS DataSync peut transférer une liste de fichiers ou d'objets à l'aide d'un manifeste.	7 février 2024
Nouvelle Région AWS	AWS DataSync est désormais disponible pour les transferts de données dans la région de l'Ouest du Canada (Calgary).	20 décembre 2023
Support pour les transferts avec d'autres fournisseurs de cloud	AWS DataSync peut désormais transférer des données entre les services AWS de stockage IBM Cloud Object Storage et/ouSeagate Lyve Cloud.	7 novembre 2023

Support pour les transferts avec Alibaba Cloud Object Storage Service	AWS DataSync peut désormais transférer des données entre les services AWS de stockage etAlibaba Cloud Object Storage Service.	25 septembre 2023
Support pour les rapports de tâches	Surveillez vos AWS DataSync transferts à l'aide de rapports de tâches.	30 août 2023
Nouvelle Région AWS	AWS DataSync est désormais disponible pour les transfert s de données dans la région d'Israël (Tel Aviv).	23 août 2023
Support pour les transferts avec d'autres fournisseurs de cloud	AWS DataSync peut désormais transférer des données entre les services de AWS stockage et plusieurs autres fournisseurs de cloud (tels que Wasabi Cloud StorageDigitalOcean Spaces, etOracle Cloud Infrastructure Object Storage).	08 août 2023
Disponibilité générale du Microsoft Azure Blob Storage support	AWS DataSync peut désormais transférer des objets depuis et versMicrosoft Azure Blob Storage.	25 juillet 2023
Prise en charge du protocole TLS 1.3	Lors du transfert entre sites de stockage, l'ensemble du trafic réseau est AWS DataSync désormais chiffré avec le protocole TLS (Transport Layer Security) 1.3.	28 juin 2023

Nouvelles métriques DataSync de découverte	AWS DataSync Discovery peut désormais vous indiquer le nombre LUNs (numéros d'unités logiques) d'un cluster de ressources de stockage, d'une machine virtuelle de stockage (SVM) ou d'un volume.	28 juin 2023
Nouvelle Région AWS	AWS DataSync est désormais disponible pour les transfert s de données dans la région Asie-Pacifique (Melbourne).	24 mai 2023
Support pour le stockage compatible S3 sur Snowball Edge	Vous pouvez l'utiliser AWS DataSync pour transférer des données entre le stockage compatible Amazon S3 AWS Snowball Edge et les services AWS de stockage.	18 mai 2023
AWS mises à jour de politique s gérées - Mise à jour d'une politique existante	La `AWSDataSyncFullAccess` politique prévoit de nouvelles autorisations pour les services compatibles avec DataSync.	2 mai 2023
Disponibilité générale de AWS DataSync Discovery	Utilisez DataSync Discovery pour accélérer votre migration vers AWS.	25 avril 2023
Version préliminaire publique du support de Microsoft Azure Blob Storage	AWS DataSync peut désormais transférer des objets depuisMicrosoft Azure Blob Storage.	29 mars 2023

Nouvelle politique IAM	Pour prendre en charge la fonctionnalité DataSync Discovery, DataSync utilise le rôle lié au service nommé. `AWSServiceRoleForDataSyncDiscovery`	21 mars 2023
Nouvelle Régions AWS	AWS DataSync est désormais disponible dans les pays suivants Régions AWS : Asie-Pacifique (Hyderabad), Europe (Espagne) et Europe (Zurich).	6 février 2023
Utilisation de balises dans l'exécution des tâches	Vous pouvez désormais étiqueter les exécutions de vos AWS DataSync tâches.	16 décembre 2022
Support pour S3 Glacier Instant Retrieval	Vous pouvez désormais transférer des objets directement dans la classe de stockage S3 Glacier Instant Retrieval.	16 décembre 2022
Copier les métadonnées du système d'objets	AWS DataSync peut désormais copier les métadonnées du système lors du transfert entre un système de stockage d'objets et Amazon S3.	16 décembre 2022
Nouvelle Régions AWS	AWS DataSync est désormais disponible dans les régions de Chine (Pékin) et de Chine (Ningxia).	14 décembre 2022
Nouvelle Région AWS	AWS DataSync est désormais disponible dans la région Moyen-Orient (EAU).	16 novembre 2022

Support pour les certificats auto-signés avec des emplacements de stockage d'objets	AWS DataSync peut se connecter à des emplacements de stockage d'objets qui utilisent des certificats privés ou auto-signés.	25 octobre 2022
Obtenir des informations sur la compression des données	AWS DataSync peut fournir le nombre physique d'octets transférés sur le réseau après l'application de la compression.	25 octobre 2022
Version préliminaire publique de AWS DataSync Discovery	Utilisez DataSync Discovery pour accélérer votre migration vers AWS.	21 septembre 2022
Nouvelle option de migration des données vers ou depuis Google Cloud Storage	Vous pouvez transférer des données vers ou depuis Google Cloud Storage en déployant un AWS DataSync agent dans Google Cloud.	21 juillet 2022
Support d'Amazon FSx pour les systèmes de fichiers NetApp ONTAP	AWS DataSync peut désormais transférer des fichiers et des dossiers depuis et vers FSx les systèmes de fichiers ONTAP.	28 juin 2022
Nouvelles options de sécurité pour les sites Amazon EFS	AWS DataSync peut accéder aux systèmes de fichiers Amazon EFS à l'aide de TLS, de points d'accès et de rôles IAM.	31 mai 2022

Migration de données vers ou depuis Google Cloud Storage et Azure Files	Avec AWS DataSync, vous pouvez transférer des données vers ou depuis Google Cloud Storage et Azure Files. Pour plus d'informations, consultez les sections Création d'un emplacement pour le stockage d'objets et Création d'un emplacement pour les PME.	24 mai 2022
Nouveau paramètre AWS DataSync de tâche	Avec l'option Copier les balises d'objets, vous pouvez indiquer si vous souhaitez conserver les balises d'objet lors du transfert entre systèmes de stockage d'objets.	5 mai 2022
Nouvelle Région AWS	AWS DataSync est désormais disponible dans la région Asie-Pacifique (Jakarta).	19 avril 2022
Support d'Amazon FSx pour les systèmes de fichiers OpenZFS	AWS DataSync peut désormais transférer des fichiers et des dossiers vers et FSx depuis les systèmes de fichiers OpenZFS.	5 avril 2022
Support pour les systèmes de fichiers Amazon FSx for Lustre	AWS DataSync peut désormais transférer des fichiers et des dossiers vers et FSx depuis les systèmes de fichiers Lustre.	10 décembre 2021

Support pour les systèmes de fichiers distribués Hadoop (HDFS)	AWS DataSync prend désormais en charge le transfert de fichiers et de dossiers vers et depuis des clusters HDFS.	03 novembre 2021
Nouvelle Région AWS	AWS DataSync est désormais disponible dans la région Asie-Pacifique (Osaka).	28 juillet 2021
Transferts entièrement automatisés entre les services AWS de stockage	AWS DataSync peut désormais transférer des fichiers ou des objets entre Amazon S3, Amazon EFS ou FSx pour Windows File Server en quelques clics dans la DataSync console.	9 novembre 2020
Réglage de la bande passante réseau utilisée par une tâche en cours	AWS DataSync permet désormais aux clients d'ajuster la bande passante réseau utilisée par une DataSync tâche en cours d'exécution. Cela permet de minimiser l'impact sur les autres utilisate urs ou applications lorsqu'un e tâche s'étend sur plusieurs jours.	9 novembre 2020
Support amélioré pour les fonctions des machines DataSync virtuelles (VM) sur site	La console hôte de la machine virtuelle de l' AWS DataSync agent prend désormais en charge des fonctions améliorées, notamment l'activation d'un agent depuis la console locale.	19 octobre 2020

AWS DataSync peut désormais transférer des données depuis et vers AWS Outposts	DataSync prend désormais en charge le transfert d'objets depuis et vers Amazon S3 AWS Outposts.	30 septembre 2020
Support pour le filtrage des API	AWS DataSync prend désormais en charge le filtrage des appels d'`ListLocations` API `ListTasks` et d'API, ce qui vous permet de récupérer facilement la configuration des tâches de transfert de données en utilisant des filtres tels que la source ou la destination du transfert de données.	18 août 2020
Support pour la copie de données depuis votre stockage d'objets autogéré	AWS DataSync prend désormais en charge le transfert de données entre le stockage d'objets autogéré et Amazon S3, Amazon Elastic File System ou FSx Windows File Server.	27 juillet 2020
Support pour les machines virtuelles basées sur le noyau Linux (KVM) et les hyperviseurs Microsoft Hyper-V	AWS DataSync permet désormais de déployer des agents sur site sur les plateformes de virtualisation KVM et Microsoft Hyper-V, en plus des options existantes et VMware Amazon. EC2	1er juillet 2020

AWS DataSync peut désormais configurer automatiquement votre configuration Amazon CloudWatch Logs	Lors de l'utilisation DataSync, vous avez désormais la possibilité de générer automatiquement le groupe de CloudWatch journaux et la politique de ressources nécessaires pour publier les journaux pour votre transfert de données, simplifiant ainsi la création de tâches et la configuration de la surveilla nce.	1er juillet 2020
AWS DataSync peut désormais transférer des données depuis et vers AWS Snowball Edge	DataSync prend désormais en charge le transfert de fichiers vers et depuis AWS Snowball Edge, le plus petit élément de l'informatique AWS Snow Family de pointe et des dispositifs de transfert de données. Le Snowball Edge est portable, robuste et sûr. Il est suffisamment petit et léger pour tenir dans un sac à dos et peut résister à des environne ments difficiles.	17 juin 2020
Nouvelle Région AWS	AWS DataSync est désormais disponible dans la région Afrique (Le Cap) et dans la région Europe (Milan).	16 juin 2020

Capacités de surveillance améliorées avec journalisation au niveau des fichiers	Vous pouvez désormais activer la journalisation détaillée pour les fichiers et les objets copiés entre vos serveurs NFS, vos serveurs SMB, vos compartiments Amazon S3, vos systèmes de fichiers Amazon EFS et FSx pour les systèmes de fichiers Windows File Server.	24 avril 2020
Support pour la copie de données entre votre partage SMB et le serveur de fichiers Amazon FSx pour Windows	Vous pouvez désormais copier des données entre votre partage SMB et FSx pour Windows File Server.	24 janvier 2020
Support pour la planification des tâches	Vous pouvez désormais exécuter des tâches manuellement ou les planifier pour qu'elles s'exécutent en fonction d'une planification spécifiée.	20 novembre 2019
Nouvelle Région AWS	AWS DataSync est désormais disponible dans la région Asie-Pacifique (Hong Kong), la région Asie-Pacifique (Mumbai), la région Europe (Stockholm), la région Amérique du Sud (São Paulo) et la région AWS GovCloud (US-Est).	20 novembre 2019

Nouvelle Région AWS	AWS DataSync est désormais disponible dans la région Canada (Centre), la région Europe (Londres) et la région Europe (Paris).	2 octobre 2019
Support pour les classes de stockage Amazon S3	Vous pouvez désormais transférer des objets directement dans les classes de stockage Amazon S3.	24 septembre 2019
Nouvelle Région AWS	AWS DataSync est désormais disponible dans la région Moyen-Orient (Bahreïn).	28 août 2019
Support pour la copie de données entre votre partage SMB (Server Message Block) et Amazon S3 ou Amazon EFS	Vous pouvez désormais copier des données entre votre partage de fichiers SMB et Amazon S3 ou Amazon EFS.	22 août 2019
Support pour l'utilisation des points de terminaison du cloud privé virtuel (VPC)	Vous pouvez désormais créer une connexion privée entre votre agent et un réseau privé AWS et exécuter des tâches sur celui-ci. Ainsi, cela augmente la sécurité de vos données lorsqu'elles sont copiées sur le réseau.	5 août 2019
Prise en charge des points de terminaison FIPS (Federal Information Processing Standard)	Vous pouvez désormais utiliser des points de terminais on FIPS pour créer des agents et exécuter des tâches.	5 août 2019

Nouvelle Région AWS	AWS DataSync est désormais disponible dans la région AWS GovCloud (ouest des États-Unis).	11 juin 2019
Support pour le filtrage	Vous pouvez désormais appliquer des filtres pour transférer uniquement un sous-ensemble des fichiers figurant dans votre emplacement source lorsque vous transférez des données depuis votre emplacement source vers votre emplacement de destination.	22 mai 2019
Première version de AWS DataSync	Version générale du AWS DataSync service.	26 novembre 2018

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

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.